ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 04 No. 02. Oct-Dec 2025.Page#.240-262
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems
https://doi.org/10.5281/zenodo.17280432

Exploring the Role of Technologies in Building Organizational Resilience towards Organizational Stability: A Case of Kazakhstan

Gahwar Bhatti
SDU Business School, SDU University Kazakhstan
bhatti.gahwar@sdu.edu.kz
Izbassarova Aiaru
SDU Business School, SDU University Kazakhstan
Rakhim Dinara
SDU Business School, SDU University Kazakhstan
Qaswa Bint-e-Firdous Wani
SDU Business School, SDU University Kazakhstan
Nuri Gassanov
SDU Business School, SDU University Kazakhstan
Idris Musa Garba
SDU Business School, SDU University Kazakhstan

ABSTRACT

In the rapid technological developing world business and organizations must create robust strategies to adapt and withstand new disruptions. This study investigates the role of technologies in enhancing organizational resilience, eventually leading to organizational stability. The study employs qualitative research design by applying Gioia methodology to analyze semi-structured interviews with organizational leaders across various industries. Five principal types of disruption were discovered: geopolitical instability, pandemics, cybersecurity threats, natural disasters, and economic or trade disruptions. The results of the study reveal how organizations perceive and cope with such crises and illustrate the role of technological solutions in adaptation and recovery. The main contribution of this study is the development of a process model that clearly shows how organizations respond to certain disruptions with technology to get organizational stability. The data obtained represent both a theoretical contribution to research on sustainability and digital transformation, as well as a practical guide for managers interested in creating resilient and flexible organizations.

Keywords*: Organizational Resilience, Technology, Digital Technologies, Organizational Stability, Disruption*.

Introduction

In today's inconsistent and changing global environment, the most critical capabilities an organization can develop has become resilience. As the world encounters growing uncertainty due to economic turbulence, climate change, cybersecurity threats, political instability, and public health emergencies, organizations are being forced to adapt to disruptive conditions. These disruptions often happen unexpectedly and organizations never can be fully prepared for them, although consequences affect organizations on multiple levels starting from supply chain disturbances to employee displacement and revenue loss. In light of such challenges, organizational resilience, defined as the ability to prepare for, respond to, and recover from adverse events, is now viewed not only as a survival mechanism but as a competitive advantage (Duchek, 2020).

Technological development plays a crucial role in creating how organizations build and sustain their resilience proficiency. Compared to past decades where resilience was substantially based on strong leadership or risk management structure, today it is strongly tied to an organization's digital capacity. Tools such as cloud computing, big data analytics, artificial intelligence (AI), and collaborative platforms have enabled businesses to act swiftly in times of crisis, maintain operations, and support distributed teams in real time (Kitsios & Kamariotou, 2021). During disruptions such as the COVID-19 pandemic, these technologies helped firms to move the whole operations system online within days. Yet, such transformations also raised critical questions regarding digital inequality, technology readiness, and the uneven impact of disruptions across industries and regions.

In addition, there is no universal guideline on what technologies work best in specific disruption contexts. For instance, real-time inventory tracking and predictive analytics is required for supply chain disruptions, whereas internal crises such as employee burnout or cultural instability may need to solve this using communication platforms and mental health monitoring tools. For developing targeted and flexible resilience strategies understanding these details is fundamental.

While researchers have continuously studied both resilience and digital transformation, we still lack clear insights into how companies actually use technological solutions when facing different kinds of crises. Literature tends to examine either resilience or technology in isolation, missing the crucial ways they interact when organizations confront particular disruption scenarios (Sutcliffe & Vogus, 2003).

Research Questions

1. What disruptions organizations are facing and what strategies are they implementing to address them?
2. How technologies are helping the organizations to respond to these disruptions?
3. How organizational resilience creates organizational stability?

2. Literature Review

2.1. The concept of organizational resilience

According to Stoverink et al. (2020), the word "resilience" comes from the Latin word “resilire,” meaning “to bounce back.” Before it was used in organizations, the idea was initially developed in ecological sciences by Holling (1973) to characterize the shock absorption capability of environmental systems. Within the context of an organization, “resilience refers to a firm’s ability to anticipate, prepare for, respond to, and adapt to disruptions while maintaining its core functions, integrity, and purpose (Meena & Santhanalakshmi, 2023).” Recovery of operational performance after a disruption and proactive development of crucial capabilities are two essential skills that are combined to form organisational resilience (Holling, 1996). In today’s dynamic and uncertain corporate world this concept is becoming more and more relevant (Nauck et al., 2021).

In order to stay resilient, organisations must cultivate critical adaptive skills that enable them to function efficiently in the face of both anticipated and unexpected difficulties. In the article ‘How Resilient Is Your Organisation? An Introduction to The Resilience Analysis Grid’ Hollnagel (2010) outlines four critical abilities that define organizational resilience: the capacities to respond, monitor, anticipate, and learn.

2.1.1. The ability to respond

A resilient organization must be able to respond swiftly and effectively to both routine disturbances and unexpected events. This means that companies have to recognise important shifts, choose the best course of action, and allocate resources to address the facing challenges. Without timely action, organizations risk being affected by rising threats.

2.1.2. The ability to monitor

Monitoring is the process of continuously observing both internal and external processes in order to identify any changes early. Monitoring using reliable indicator sources is essential to identify neither challenges nor opportunities, since it allows proactively to take actions before problems intensify.

2.1.3.The ability to anticipate

Anticipation is the ability to see beyond the present and forecast possible future events that may have an impact on the organisation. A wide range of changes such as technological advancements, political shifts, evolving market conditions and so on, must be considered as all these influences on a company's well-being. In the uncertainty presence, anticipation requires both strategic foresight and a readiness to investigate adaptive solutions.

2.1.4. The ability to learn

Another important component of resilience is the ability to learn, as it allows organizations to implement the knowledge gained from past experiences in order to enhance future performance. In addition to learning from failures, this includes recognizing and enhancing successes. The adoption of learning ability leads to enhancing adaptive capacity and decreasing recurrent errors.

Resilience, according to Hollnagel (2010), is "something an organization does rather than something it has" and it should be viewed as a dynamic, continuous activity rather than a fixed characteristic. Consequently, it is vital to consistently cultivate and regulate all four capabilities, as an organization may become vulnerable if it concentrates excessively on a single aspect, without giving equal consideration to other capabilities. Truly resilient organizations that incorporate all four capabilities, in result have a system that is proactive, thoughtful, and adaptable, that can remain stable and thrive in the face of uncertainty and change.

As a result, we characterize organizational resilience as the ability of an organization to forecast difficulties, respond to crises effectively, and remain adaptable in dynamic evolving contexts (Duchek, 2020). Business continuity and organisational success depend on having this capability. Organisations can attain sustained competitive positioning and this explains why some businesses perform better than others (Sheffi, 2007).

2.2. Defining technologies and their role in organizational resilience

Nowadays, industries have been transformed by fast growth of digital technologies, such as artificial intelligence, big data analytics, cloud computing, and the Internet of Things, which have allowed organizations to proactively navigate disruptions (Meena & Santhanalakshmi, 2023). As a strategic shift from traditional management models, digital transformation serves as a fundamental component for building organizational resilience (Benner & Waldfogel, 2023). Digital technologies are not only tools for efficiency, but they also function as dynamic enablers of adaptability, risk mitigation, and continuity (Duchek, 2020).

2.2.1. Artificial Intelligence and Predictive Analytics

The recent rapid rise of Artificial Intelligence is radically reshaping the way how organizations and societies create resilience, by promoting efficiency and innovation across industries, and facilitating adaptability in an unstable environment. By utilizing machine learning algorithms that detect threats in real-time, automate problem response, and protect sensitive data during cyber-attacks, AI facilitates a proactive approach to cybersecurity. Companies can strengthen their emergency response abilities, optimize resource allocation, and anticipate disruptions through predictive analytics, which is a critical AI application (Zhang, Long & Von Schaewen, 2021). Overall, AI serves as an essential enabler for ensuring continuity in the face of disruptions by enhancing predictive capabilities and decision-making processes under pressure.

2.2.2. Cloud computing

The adoption of cloud computing enables organizations to rapidly address operational changes during crises by eliminating physical resource constraints (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin, Stoica& Zaharia, 2010). Cloud platforms guarantee operational continuity by enabling the immediate transfer of data that comply with regulations. Especially, when cloud platforms are combined with real time predictive analytics and machine learning systems to automate decision-making and anticipate market changes, it dramatically increases proactive crisis response (Jordan & Mitchell, 2015). This kind of technology combination allows organizations to adaptively transform resources and data-driven solutions into sustained operational resilience (Sambamurthy, Bharadwaj& Grover, 2003).

2.2.3. Blockchain

Decentralized blockchain architecture enhances organizational resilience, which chains data blocks to ensure immutability, transparency, and security (Hu, Zhou, Zhang & Behl, 2023). In supply chain management, it acts as a transformative tool by improving visibility through real-time tracking of goods and mitigating risks like disruptions via encrypted, secure data exchanges, thereby fostering trust among stakeholders (Dubey, Gunasekaran, Childe, Blome & Papadopoulos, 2019). Additionally, information asymmetry can be addressed by blockchain, which then strengthens resource integration, enabling organizations to enhance operational sustainability and adaptability in dynamic environments (Hu et al., 2023).

The transformative potential of digital technologies lies in their ability to reconfigure organizational structures and processes. As noted by Vial (2019), resilience depends on aligning technological adoption with strategic goals, investing in digital literacy, and addressing cybersecurity risks. Without holistic integration, technologies risk underutilization or unintended vulnerabilities (Mikalef, Krogstie, Pappas & Pavlou, 2020).

2.3. Defining disruptions

This study is not limited to specific types of disruption and considers all types of challenges that organizations face. Both natural disasters and human-caused disruptive events impair organizations' ability to respond effectively, reducing operational capacity (Shaluf, Ahmadun & Said, 2003). These disruptions range in intensity and scale, potentially resulting in significant destruction, operational interruptions, financial impacts, physical harm, or even fatalities in extreme cases (Burnard, Bhamra & Tsinopoulos, 2018). Such events demand immediate attention and reaction from organizations, which may not have anticipated them. Given the rise of natural disasters, climate change, and other significant disruptions, creating resilient infrastructure has become more crucial than ever.

2.3.1. Geopolitical instability

Geopolitical disruptions arise when international conflicts or political crises suddenly disrupt markets and operations. Global financial markets have been fundamentally affected by the geopolitical risks triggered when Russia invaded Ukraine on February 24, 2022 (Shahzad, Mohammed, Tiwari, Nakonieczny & Nesterowicz, 2022). The international community has enacted severe economic sanctions against Russia, which are affecting cross-border commerce in goods & services and severely limiting access to international banking and transaction processing capabilities (Tosun & Eshraghi, 2022). Faced with these developments, numerous multinational corporations have opted to either exit the Russian market completely or freeze investment activities for the indefinite future, as they recognized that staying could do more long-term damage to their reputation than the short-term cost of leaving (Sonnenfeld, Tian, Zaslavsky, Bhansali & Vakil, 2022). This highlights that resilience goes beyond just recovering from setbacks, it highly involves difficult decisions guided by values and principals, especially in the presence of uncertainty.

2.3.2. Pandemic

The term pandemic originates from the Greek words "pan" meaning "all" and "demos" meaning "the people", and it refers to the widespread occurrence of an infectious disease. In its modern usage, a pandemic is understood as an epidemic that has extended beyond national borders, impacting numerous countries or even the global population, and involving a substantial number of people (Suryasa, Rodríguez-Gámez & Koldoris, 2021). The recent example of this disruption is Covid-19 pandemic that caused unprecedented disruption across societies and economies worldwide, pushing organizations to adapt in ways that previous crises hadn't. While businesses had previously concentrated on economic adjustments, the pandemic made it clear that long-term resilience depends on more than just financial agility, it also requires flexible strategies and structures that can respond to sudden change (Paeffgen, 2023). Researchers note that Covid-19 has "emphasized the importance of resilience in an organisational context" (Aldianto, Anggadwita, Permatasari, Mirzanti & Williamson, 2021). The effects of the pandemic varied across different sectors: for example, whereas manufacturing operations were disrupted due to strict travel and workplace restrictions, many service-oriented firms were able to adapt by switching operations to online mode, allowing them to continue functioning or even expand in the face of adversity (Vanany, Ali, Tan, Kumar & Siswanto, 2021). Consequently, the presence of digital infrastructures was essential for businesses to maintain their operations. Overall, the Covid-19 crisis demonstrated that organizational resilience requires both technological readiness and adaptable frameworks (Paeffgen, 2023).

2.3.3. Cybersecurity threats

As corporations increasingly implement technologies, such as artificial intelligence, blockchain and cloud computing, cybersecurity becomes a significant problem. Developing technology's opportunities also increases facing threats. Organizations are at risk from cyberattacks, particularly those that depend largely on Information and Communication Technologies. The focus is now not only on preventing these attacks, but on how well an organization can respond and recover when such incidents occur (Araujo, Machado & Passos, 2024). Because of the strategic nature of cyber threats, IT and business leadership must closely align on decision making, as many cybersecurity failures stem from organizational issues rather than technological ones (Bagheri, Ridley & Williams, 2023). Given that cyber catastrophes threatening data security can interrupt operations and result in significant financial losses, cyber resilience is recognized as a critical aspect of overall organizational resilience (Araujo et al, 2024). Encryption, authentication, and access control techniques are used to protect data and networks from unauthorized access or malicious actions (Saeed, Altamimi, Alkayyal, Alshehri & Alabbad, 2023). Furthermore, corporations should invest in cyber insurance to protect financial data and prioritize employee awareness to promote reliable cybersecurity practices (Saeed et al, 2023). Consequently, cultivating resilience against cyber challenges involves continuous monitoring, employee training, and investment in adaptive cybersecurity technologies.

2.3.4. Natural disasters

Natural disasters are major geological or meteorological phenomena that significantly disturb the interaction between humans and the environment (Young, Balluz & Malilay, 2004). These environmental changes expose the organizations to significant opportunities for success and growth and substantial threats and challenges (Burnard et al., 2018). Unlike any other disruptions, natural disasters are often characterized by their geographic specificity, meaning the direct physical impact is usually concentrated in a particular region. Natural hazards, such as earthquakes and floods may disrupt operations by destroying infrastructure and interrupting supply chains. Earthquakes occur without warning and can devastate facilities and communication networks, while floods can drown factories, warehouses, and transportation routes. These events directly interrupt organizational processes and as reviewed by Skouloudis et al. (2020), they "create discontinuity and damages to business operations". Resilience during crises requires synergistic physical and strategic measures: (1) operational hardening through structural reinforcements, geographic redundancy, and inventory buffers; and (2) technology-enabled planning utilizing satellite monitoring, early-warning sensors, resilient communication networks to enable real-time assessment and coordinated response (Skouloudis, Tsalis, Nikolaou, Evangelinos, & Filho 2020). For this reason, companies need to create resilience strategies that encompass both operational and strategic processes.

2.3.5. Economic or trade disruption

Systematic shocks affecting financial institutions, trade networks and market stability form a unique class of organizational risks economic and trade disruptions. Unlike natural disasters or cyberattacks, these disruptions often emerge from complex geopolitical tensions, policy shifts, or macroeconomic imbalances, creating ripple effects across global supply chains and business operations. This pattern was clearly demonstrated in 2018 as America and China, the globe's top economic powers, engaged in successive rounds of tariff increases, leading to the US–China trade war (Itakura, 2019). According to recent academic research, tariff wars are "reshaping global supply chains" (Sabadosa, Rengifo, Resendez, Beato, Said & Styers, 2024). Businesses are adjusting to the trade dispute by diversifying their suppliers across nations, relocating their manufacturing closer to home, and creating new markets to help with tariff protection. Building resilience is primary for organizations facing such economic challenges. Companies must implement both short and long term operational strategies like transparent supply chains, flexible decision making systems, and strong partnership to stay adaptable.

According to Sahebjamnia et al. (2018), environmental turbulence, including natural disasters and man-made risks, is what motivates modern organizations to develop organizational resilience in order to guarantee company continuity. These disruptions come from both endogenous and exogenous sources and affect how organizations respond to such a danger to survive (Burnard et al., 2018). Particularly in the globally interconnected world of today, the effects of such incidents frequently go beyond the organization itself, impacting larger communities and regions (Burnard et al., 2018). In light of this continuous risk environment, businesses are increasingly dependent on technology as a vital tool for fostering organizational resilience. Advanced instruments such as AI-driven risk analytics, IoT-enabled supply chain oversight, and blockchain-secured logistics improve real-time hazard identification, swift reaction coordination, and operational flexibility. Companies can reduce immediate disruptions and increase systemic capacity to foresee and recover from future crises by adopting these technologies.

2.4. Defining organizational stability

Despite the view of many scholars that consider organizational resilience as "desired outcome", Su and Junge (2023) investigated that it relates to resilience phases or resilience 'as a whole'. In the majority of empirical studies on organizational resilience, stability is identified as one of the key indicators through a variety of performance outcomes (Su & Junge, 2023). From this perspective, stability is both the aim and the outcome of resilience processes. Research by Ortiz-de-Mandojana and Bansal (2016) indicates that organizations that can absorb shocks through strategic flexibility while preserving core functions, rather than just resisting crisis, are able to achieve long-term stability. Their longitudinal examination of sustainable enterprises indicates that stability arises from ongoing learning and strategic adaptation following disruptions, allowing for sustained performance. The ability to maintain stability after setbacks is a vital sign of resilience, reflecting an organization's vulnerability prior to adversity and its capability to endure systemic shocks (Su & Junge, 2023).

The role of technologies in facilitating this dynamic stability is crucial. Duchek (2020) posits that stability results from improved "absorptive capacity," wherein technology such as AI-driven predictive analytics or IoT-enabled real-time monitoring furnish the necessary data visibility and simulation capabilities to foresee stressors and proactively modify operations. This post-resilience stability is fundamentally temporary, necessitating ongoing investment in sensing technology, adaptive frameworks, and a culture that fosters controlled experimentation. The idea is not to eradicate change but to manage it with adequate coherence to uphold fundamental goals, a dynamic equilibrium facilitated by strategic technology integration.

3. Methodology

This study employs in-depth interviews as a primary data collection method to gain ground-level understanding of how people experience technology's role in helping organizations bounce back from challenges. The research cohorts strictly establish ethical protocols to safeguard participant welfare and data confidentiality. Furthermore, the study implements clear audit trails and maintains openness about methodological limitations to commit to research transparency, thereby preserving the integrity of the research outcomes.

3.1. Research Design

Given the exploratory nature of the research topic, a qualitative research design was considered most appropriate. Qualitative research allows for understanding of complicated social realities, especially when the focus lies in understanding human experiences, organizational practices, and context-specific technological applications (Creswell, 2014). Since the objective of this study is to explore how technologies support organizational resilience through real-world examples and managerial experiences, qualitative inquiry provides the flexibility and depth required to capture nuanced insights. The qualitative study helps us better to understand the empirical results, supports the reliability and validity of our findings (Garrido-Moreno, Martín-Rojas & García-Morales, 2024), and complements our understanding of the phenomenon.

3.2. Data Collection

Data was collected from semi-structured comprehensive interviews. Traditional personal interviews have been the principal approach for collecting qualitative data (Creswell, 2013), maintaining their significance despite technological progress (Cater, 2011). The major advantages of face to face interviews is that it provides deeper insights except spoken words, through personal communication researchers can interpret non-verbal signals including gestures, posture, and facial expressions. This element is especially important when studying evolving educational practices, because nonverbal communication can uncover hidden perspectives, emotional responses, and cultural subtleties that may not be fully expressed only through verbal answers.

3.3. Instruments

In developing our interview questions for examining the role of technologies in organizational resilience, we have derived inspiration from existing literature while adapting them to align with our specific research objectives. By asking open ended questions, the interviews allow participants to unreservedly express their opinion and experiences, enhancing the richness of the collected data. Recognizing that the application of technology to the recovery of the organization has a significant influence, we seek to explore the personal experiences of participants, to gather their ideas, with the challenges they have faced and reflect on how digital tools reinforce the ability to recover in their workplaces.

3.4. Sampling

Fifteen semi-structured interviews were carried out with industry professionals across multiple sectors including technology consulting, logistics, education, and nonprofit organizations - to obtain direct experiential data. The participant selection employed purposive sampling methodology, with the key requirement that all interviewees needed to have either led or been directly involved in deploying technological interventions during organizational crises or disruptions.

To ensure the integrity and validity of the findings and achieve maximum diversity within the sample, we decided to ask individuals from different departments, various fields and levels of experience.

The sample size was established through a progressive method, dedicated to the concept of data saturation (Saunders, Sim, Kingstone, Baker, Waterfield, Bartlam, Burroughs & Jinks, 2017), which stands for continued until new insights and thoughts regarding impact of technology to organizational resilience.

3.5. Data preparation and collection procedures

The interview phase took place from February to April 2025, with each session typically running between 20 and 30 minutes. Prior to commencement, participants received a briefing on the study's objectives, and researchers provided explanations of key concepts while addressing any participant inquiries. Respondents were encouraged to elaborate on their perspectives. While a predetermined question framework guided the conversations, enabling the collection of significant qualitative data. The semi-structured approach maintained consistency while permitting adaptive dialogue. Following participant approval, all interviews were audio-recorded and subsequently transcribed to facilitate thorough analysis.

3.6. Data analysis

The collected qualitative data were analyzed using the Gioia Methodology (Gioia, Corley & Hamilton, 2013) which is a qualitative methodological approach to developing a data analysis that can meet the rigorous standards of trustworthy research. The analytical approach follows a systematic, multi-phase procedure. Initially, raw interview data are categorized into first-order codes that preserve participants' original language and viewpoints. These preliminary codes are subsequently organized into second-order themes, revealing broader patterns in the data. Ultimately, these thematic clusters are consolidated into higher-order conceptual dimensions that provide a holistic interpretation of the research outcomes. Utilizing this established qualitative methodology guarantees a methodical and replicable analysis while maintaining the nuanced depth of participants' contributions.

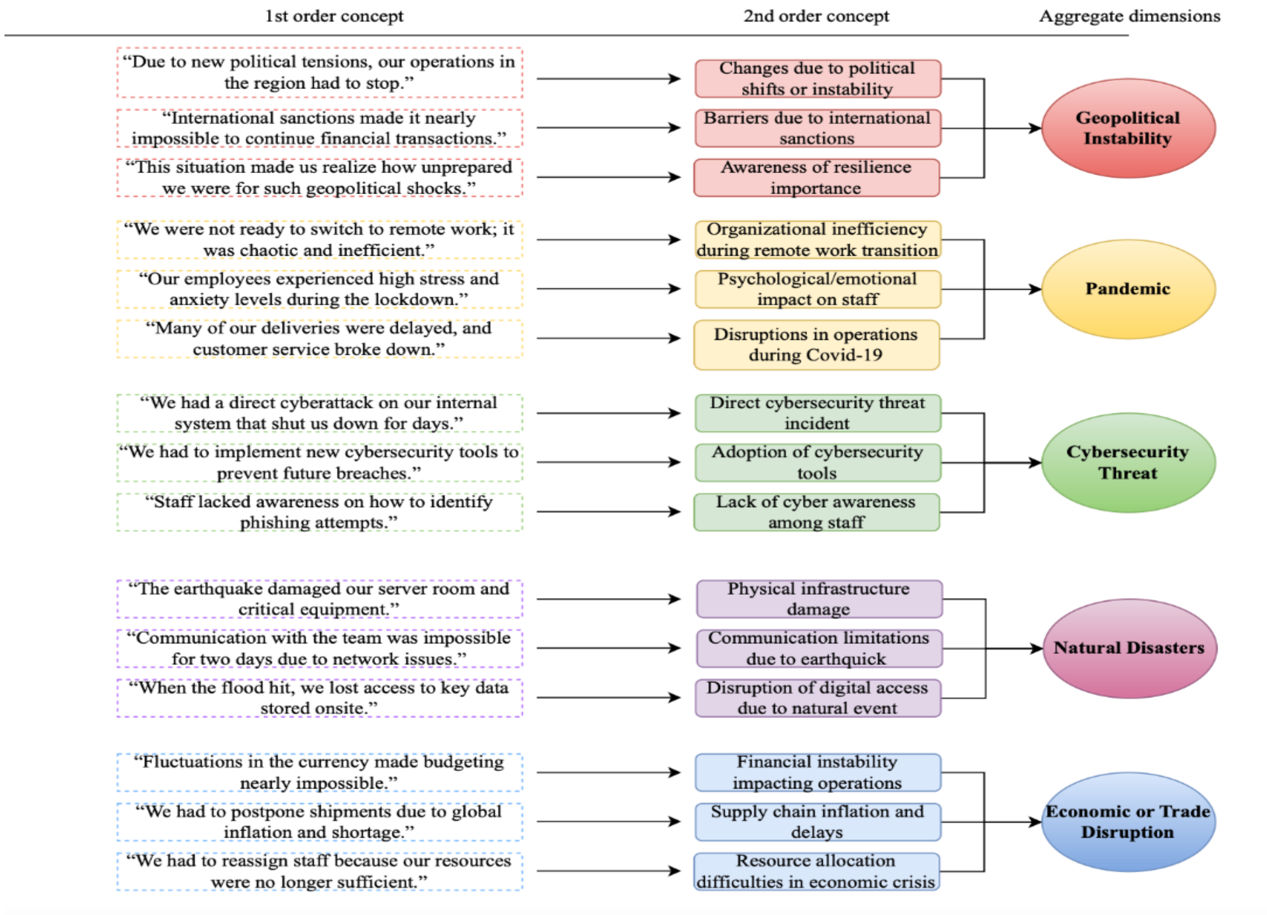
3.7. Ethical issues

In making qualitative study on the impact of technologies in increasing organizational resilience, it was important to address the ethical considerations essential in the research process. Ethical difficulties in studies involving human participants require careful consideration to preserve participant's rights, well-being, and anonymity while preserving the honesty and validity of the research (Creswell & Creswell, 2017).

The most important ethical aspect was gaining informed permission, whereby participants were fully informed about the study’s objectives, procedures and benefits before choosing to participate. Additionally, strong steps were implemented to preserve confidentiality and anonymity, ensuring participants’ privacy and prohibiting unauthorized publication of sensitive information (Guest, Bunce & Johnson, 2005). In line with these principles, verbal confirmation was acquired from participants before each interview to reconfirm their consent and resolve any concerns, thereby upholding ethical standards throughout the research process.

4. Analysis and Findings

Figure 1. Data structure


1st order concept
2nd order concept
Aggregate dimensions
“Due to new political tensions, our operations in the region had to stop.”
“International sanctions made it nearly impossible to continue financial transactions.”
“This situation made us realize how unprepared we were for such geopolitical shocks.”
Changes due to political shifts or instability
Barriers due to international sanctions
Awareness of resilience importance
Geopolitical Instability
“We were not ready to switch to remote work; it was chaotic and inefficient.”
“Our employees experienced high stress and anxiety levels during the lockdown.”
“Many of our deliveries were delayed, and customer service broke down.”
Organizational inefficiency during remote work transition
Psychological/emotional impact on staff
Disruptions in operations during Covid-19
Pandemic
“We had a direct cyberattack on our internal system that shut us down for days.”
“We had to implement new cybersecurity tools to prevent future breaches.”
“Staff lacked awareness on how to identify phishing attempts.”
Direct cybersecurity threat incident
Adoption of cybersecurity tools
Lack of cyber awareness among staff
Cybersecurity Threat
“The earthquake damaged our server room and critical equipment.”
“Communication with the team was impossible for two days due to network issues.”
“When the flood hit, we lost access to key data stored onsite.”
Physical infrastructure damage
Communication limitations due to earthquick
Disruption of digital access due to natural event
Natural Disasters
“Fluctuations in the currency made budgeting nearly impossible.”
“We had to postpone shipments due to global inflation and shortage.”
“We had to reassign staff because our resources were no longer sufficient.”
Financial instability impacting operations
Supply chain inflation and delays
Resource allocation difficulties in economic crisis
Economic or Trade Disruption

4.1. Geopolitical instability

Organizational operations can be greatly impacted by geopolitical interruption, which might vary from national revolution to armed conflicts. Interview respondents noted that political insecurity in nearby regions forced office relocations. One of the respondent’s operations manager remarked:

“When our government imposed sudden military restrictions, we had to move our regional hub within three months to avoid supply chain breakdowns.” (participant 5)

Another executive underlined that after physical relocation followed strategy transformation:

“Relocating wasn’t just about geography we had to adopt a leaner, remote-friendly workflow to accommodate dispersed teams.” (participant 13)

Many corporations have encountered operating difficulties due to political instability in neighboring nations, causing them to shift offices to more stable regions. This transition basically requires not just physical relocation of the team but also adjustments in corporate strategies and operational processes, because these relocations are immediate response to threads like trade limitations, legislative alterations, or security threats, which can significantly affect business continuity. In other situations, firms relocated operations or altered contracts to safeguard their reputation and avert consumer boycotts. Thus, geopolitical crises necessitate not only infrastructural resilience but also cautious reputational risk management.

Interviewees generally acknowledged technology as the primary enabler during relocations. An IT Director explained: *"The moment we decided to relocate, we rolled out mandatory VPN access for all employees." (participant 5).*

Another cybersecurity specialist added:

We used cloud solutions to prevent risks. also, have a local copy in the same case with military situation of neighbour countries. (participant 8)

The interviewed companies showed that geopolitical disruptions demand not just physical relocations, but also strategic technological investments. Key solutions enterprise VPNs, hybrid backup systems, and cloud platforms proved useful in maintaining business continuity. This practice aligns with academic speech on digital resilience (Smith, 2022), which stand for VPNs and zero-trust frameworks are deemed critical for abrupt geopolitical pivots.

VPNs and Secure Networks acted as immediate stabilizers, enabling encrypted communication across new borders while mitigating data breach risks during chaotic transitions. Cloud Technologies (AWS/Azure) emerged as the backbone of long-term resilience, decoupling operations from physical locations and allowing near-instant operational transfers to stable jurisdictions.

A notable case occurred in Kazakhstan in early 2022 when nationwide protests resulted in a complete telecommunications blackout lasting multiple days. As one respondent described:

“The January 2022 crisis left us without any communication channels - neither cellular networks nor internet connections remained functional, cutting off contact with our entire workforce.” (Participant 6)

This situation is widely known critical weaknesses in centralized digital infrastructure, prompting strategic shifts toward decentralized systems. Several organizations implemented geographically distributed data solutions, with technical issues manager explaining:

“We now maintain duplicate databases across multiple locations, including international servers, ensuring continued access during regional outages.” (Participant 6)

The crisis of fast adoption of effective continuity methods, particularly cloud-based backup systems and multi-site data replication. These technological solutions help preserve business operations when national infrastructure becomes disrupted.

4.2. Pandemic

The COVID-19 crisis disrupted business operations on an extraordinary scale, compelling organizations to quickly transform their workflows. As one interviewee described:

“Nobody was prepared for such an unexpected and global pandemic. We had to catch up with every aspect of our operations, communication, service delivery, even corporate culture.” (participant 3)

The most urgent challenge was changing everyone to remote work, companies swiftly adopted online communication tools like Zoom and Microsoft Teams to continue with work processes. An HR leader recalled:

"We switched to Zoom and Google Meet within days. It wasn't just about meetings, we had to digitize onboarding, performance reviews and even team-building changed their habitual nature." (participant 10)

Beyond operational shifts, organizations faced significant disruptions to their supply chains. An operations executive explained:

"Adopting to new realities companies started to use cloud-based CRM systems (e.g., Salesforce) and digital payment processors for maintaining customer relationships and cash flow. Adopting cloud tools and online payment systems wasn't optional; it was the only way to stay operational and make business." (participant 4)

Scholarly research indicates that the COVID-19 crisis significantly accelerated the digitization of supply chains, enhancing visibility, flexibility, and resilience. Supporting this, Chinese firms show that digital platforms such as IoT-enabled traceability systems fully mediate the positive effect of digital adoption on supply chain resilience during the pandemic (Ning, Li, Xu & Yang, 2023).

Overall, the epidemic prompted organizations to undergo a digital makeover at a rate previously believed unachievable. The crisis underlined the requirement of adaptive capacity, driving enterprises to embrace not just temporary remedies, but lasting structural and technological change to withstand future global shocks.

4.3 Cybersecurity threat

Modern organizations are facing huge disruptions from cybersecurity threats, ranging from distributed Denial of Service (DDoS) attacks to data scraping operations. Such actions lead to a lack of stability and as indicated by the observations of its professionals, one of the operational manager hazards:

"Automated parser bots everyday attack ticket availability data, causing server overloads and data integrity." (Participant 6)

The potential impact of such threats became particularly evident during popular incidents like Amazon's Content Delivery Network outage and the July 2024 CrowdStrike system failure, which was a worldwide failure. As a security analyst noted,

"The CrowdStrike incident demonstrated how a routine software update could paralyze critical infrastructure across healthcare, transportation, and financial sectors for extended periods." (Participant 9)

Organizations implement extensive protection strategies including both preventive and responsive measures to mitigate these risks. Standard security protocols now typically include traffic filtering systems, redundant data backup solutions, and alternative power supply arrangements. One operations manager explained,

"Our defense strategy combines network blockers, backup servers, and independent power infrastructure to ensure continuous operation." (Participant 7)

Advanced monitoring systems have become particularly valuable to prevent those attacks, especially when everyday people find new ways to hack systems. Security engineer emphasizing,

"Nowadays, we have to monitor everyday new activity happening in the world of cybersecurity. Through security information and comprehensive log analysis, we can detect and neutralize threats during early stages." (Participant 4)

Specialized diagnostic tools like LogRocket provide additional protection by enabling detailed session reconstruction. A development team lead described its utility:

“The platform's session replay capability allows rapid identification of failure origins by tracking user interactions in real time.” (Participant 9)

These examples collectively demonstrate that contemporary cybersecurity requires a stratified defense approach combining technological solutions, continuous surveillance, and cautious update management. The growing frequency of high-impact incidents underscores the critical importance of developing robust digital resilience frameworks for organizational sustainability.

4.4 Natural disaster

Natural disasters can cause undelayed and significant disruptions, cutting off essential communications for everything not only business operations. One respondent recounted their experience during the recent earthquakes in Turkey:

“During the earthquakes in Turkey, mobile networks and internet access were unavailable. We couldn’t communicate with our families for days.” (Participant 2)

This disruption with nature highlighted the unstableness of traditional telecommunications systems to disasters. To address these challenges, organizations have implemented robust communications solutions. A logistics manager said:

“We provided satellite phones to our regional managers and established emergency contact procedures. It helped our teams stay connected, even without Internet access.” (Participant 8)

For a long time in history satellite phones have proven essential during various disasters, including earthquakes and wildfires (Research Dive, 2021) because they provide voice, SMS, and low-speed internet services, operating independently of terrestrial networks (DHS, 2015).

“Our company has arranged drones equipped with LTE units and cell towers to restore connectivity within hours.” (Participant 9)

Research shows that drones equipped with a base station can quickly assist in rescue operations when terrestrial infrastructure is compromised (Shakhatreh, Hayajneh, Bani-Hani, Sawalmeh & Anan, 2021).

4.5 Economic or trade disruption

Economic instability and changing trade policies force companies to reorganize their operations and implementation of tariff barriers has been a major obstacle, especially for businesses with manufacturing networks that are geographically concentrated. As participant 8 pointed out:

“When new tariffs in China made it difficult for us to operate our factories, we quickly had to set up a parallel manufacturing facility in Thailand while maintaining quality standards.” (Participant 8)

This claim points to a larger pattern of intentional geographic diversification, which is a reaction strategy meant to reduce supply chain unstableness. However, because of decentralization coordination, quality assurance, and cost effectiveness become more difficult.

Businesses to keep operations connected across occasional sites using more and more cloud-based ERP systems (like SAP S/4HANA). These systems allow for centralised decision-making and real-time data integration. Furthermore, we have been able to anticipate the effects of tariffs with the help of predictive analytics technologies.

Additionally, it has become clear that proactive risk assessment requires predictive analytics technologies. As one manager told that:

“Machine learning models now forecast for us potential tariff scenarios, allowing us to adjust procurement and production schedules ahead of any changes.” (participant 11)

These tools demonstrate how data-driven decision-making like modelling disruptions using historical trade data, geopolitical risk indicators, and policy forecasts improves resilience.

4.6 The challenge of technology implementation

Two key issues repeatedly arise when implementing new technologies: technical limitations and staff adaptation issues. Infrastructure solutions are not perfect.

"The service delay still occurred due to a server failure." (Participant 15)

This shows that even a robust system can have problems under real-world conditions.

Due to integration and maintenance management, the human factor is equally important. Staff often have to overcome abrupt learning curves.

"Many team members had difficulty adapting to the new system because some of them were absolutely new to this type of interaction." (Participant 18)

This pattern is confirmed by research findings. It points out that experienced employees experience cognitive and interface barriers. Therefore, tailored training is essential.

"We organised multiple training workshops and one-on-one sessions to make the rollout smoother." (Participant 7)

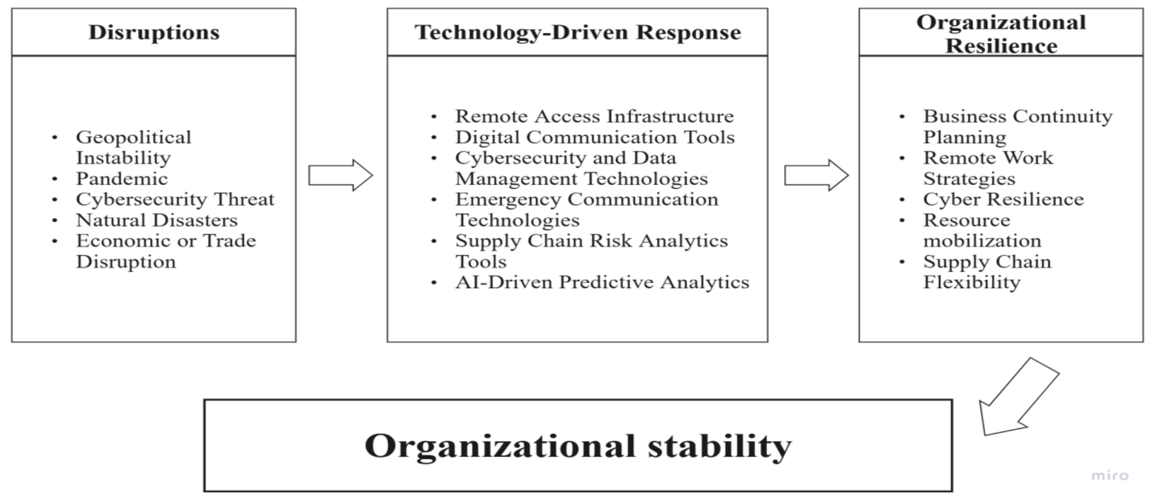
This approach perfectly cooperates with the practices supporting that gradually change of system significantly improve employee engagement and digital knowledge (PwC, 2020; Gruben, Sheil, Das, O Keeffe, Camilleri, Cronin & Murray, 2025)

Moreover, it reveals that successful tech implementation requires more than just hardware and software. The quick change of usual work style often overwhelms staff, especially less digitally informed employees like elderly people. Instead, phased training, intuitive interfaces, and ongoing support prove vital. When organizations address both the technical and human dimensions simultaneously, they transform implementation challenges into opportunities for sustainable growth.

5. Discussion

The discussion part interprets the findings through a process-oriented lens, identifying how digital technologies bridge the gap between disruptions and organizational resilience by enabling stability. Through interviews with industry experts, a consistent pattern was enabled: when disruptions occur, digital technologies contribute to activation of resilience strategies. These technologies driven strategies build organizational resilience, which then turn into sustained organizational stability. The findings demonstrate that digital tools are not an immediate solution to challenges but their implementation systematically strengthens an organization's ability to withstand future challenges. This process model provides both practical guidance for implementation and theoretical insight into how technology transforms traditional resilience concepts and contributes to lasting organizational stability.

Figure 2. Process model



Disruptions

- Geopolitical Instability
- Pandemic
- Cybersecurity Threat
- Natural Disasters
- Economic or Trade Disruption

Technology-Driven Response

- Remote Access Infrastructure
- Digital Communication Tools
- Cybersecurity and Data Management Technologies
- Emergency Communication Technologies
- Supply Chain Risk Analytics Tools
- AI-Driven Predictive Analytics

Organizational Resilience

- Business Continuity Planning
- Remote Work Strategies
- Cyber Resilience
- Resource mobilization
- Supply Chain Flexibility

Organizational stability

5.1. Business continuity planning

Business continuity planning fundamentally mitigates disruptions by avoiding risks and reducing crisis impacts (Cerullo & Cerullo, 2004). It is especially vital for sustaining critical operations when geopolitical instabilities make local business impossible to continue. When a company decides not to continue local business, it faces numerous problems. The 2022 Russia-Ukraine escalation exemplifies this, where mass corporate exits from the Russian market created unprecedented operational challenges (Sonnenfeld et al., 2022). Therefore, companies had to relocate their offices to other countries. Here, digital technologies enable rapid response: for example, cloud computing guarantees operational continuity by enabling the immediate transfer of data to jurisdictions that comply with regulations. Ibrahim (2024) states that cloud platforms “significantly enhanced organizational resilience and recovery capabilities by providing scalable, flexible, and cost-efficient solutions.” These digital tools support a smooth data transition and restore operational stability, while ensuring security and reliability. As one interviewee noted, “if one country is completely disrupted then you have set off the key processes being either run from another country or the backup opportunity to run outside of the impacted country” via remote access infrastructure. This underscoring how business continuity planning coupled with digital preparedness underpins organizational stability.

5.2. Remote work strategies

Another vital strategy in today's digital era is remote work enablement. When employees have the ability to access their work from any location, the organization is no longer restricted to a specific physical site or a specific person. A thorough development of these strategies began at COVID-19 pandemic shutdown, when everything was closed everywhere, but “Internet was not impacted during COVID times and we could very quickly move into the completely online mode of operations”, as highlighted by a specialist. Companies are using digital communication tools like Zoom and Microsoft Teams which enable not only virtual real time communication but also replicate physical collaboration through AI-enhanced features: breakout rooms simulate department-level coordination, real-time co-editing (e.g., SharePoint OneDrive integration) maintains documentation continuity. Given the sensitivity of corporate data, corporations employ Virtual Private Networks (VPNs) integrated with zero-trust architecture (Palo Alto Networks) to facilitate authenticated access. This adaptability enhances productivity and enables a seamless return to normalcy with minimal disruption. In conclusion, digital technology-enabled remote work maintains operations amid crises, thereby enhancing organizational stability.

5.3. Cyber resilience

Cyber resilience refers to the ability to consistently attain desired outcomes even when faced with adverse cyber events (Björck, Henkel, Stirna & Zdravkovic, 2015). It goes beyond simple attack prevention, but according to the NIST glossary it is “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises” on cyber systems. This corresponds with our process paradigm (Figure 2), wherein cybersecurity tools are incorporated into the Technology-Driven Response to disruptions. Study participants underscored that cyber resilience included preserving system functionality in the face of persistent threats, with one participant asserting that systems were “designed to remain operational even during active attacks.” Cyber disruptions can lead to significant financial losses, operational standstill, and damage to reputation (Björck et al., 2015).

To mitigate these risks, organizations use firewalls, Endpoint Detection and Response (EDR) systems, Security Information and Event Management (SIEM) platforms and automated recovery solutions that facilitate real-time monitoring, quick threat identification, and system restoration. Behavioral analytics and machine learning are employed by prominent platforms such as Palo Alto Networks and CrowdStrike Falcon to proactively identify and mitigate threats. Interviewees highlighted the significance of the implementation; one IT architect said that the deployment of advanced firewalls and EDR systems enabled threats to be “identified and contained automatically,” hence diminishing manual workload and downtime. By carefully integrating these technologies, companies may effectively mitigate cyber dangers while maintaining trust, performance, and adaptability amid continuous digital disruptions.

5.4. Resource mobilization

Resource mobilization during a crisis is an essential aspect of organizational resilience, requiring companies to rapidly shift individuals and resources when typical communication channels and infrastructure are not accessible. In such scenarios, organizations increasingly rely on emergency digital technology such as satellite communication to maintain operational continuity, as confirmed by the interviewed top manager: “in this case our country directors have satellite phones”. This communication method is essential when cellular towers and internet services are unavailable, as satellite systems are unaffected by the failures of physical infrastructure due to their position in space (Shah, 2024). Moreover, firms that proactively include these technologies into their disaster recovery strategies are more adept at recognizing needs and deploying resources rapidly. By ensuring that scarce resources are quickly put to use where needed, digital-enabled mobilization contributes to mitigating the crisis and restoring equilibrium, thereby fostering renewed stability within the organization.

5.5. Supply chain flexibility

Finally, supply chain flexibility is greatly enhanced by digital tools, strengthening ability to adapt supply networks under stress. Modern disruptions, previously discussed, demand that organizations rapidly reconfigure supply chain strategies and logistics. Examples of supply chain distractions include situations where companies could not ship to Russia because of sanctions they needed to “repurpose the products that were already produced for the Russian market and that was a big challenge”, as mentioned by one of the respondents. Another example occurred when supply chains were distracted by tariffs and sanctions on China, and it hit the global economy "we have introduced a factory in another country and moved production there".

In response to these disruptions, organizations have adopted supply chain risk analytics tools, including SAP Integrated Business Planning and Resilience, which were utilized to evaluate supplier dependencies and identify alternative sourcing regions that present reduced exposure to geopolitical risks. These platforms facilitated quick scenario planning and provided real-time insights into upstream vulnerabilities, assisting decision-makers in assessing the potential effects of sanctions or tariffs prior to their actualization. Together, these digital technologies contributed to a more flexible, responsive supply chain architecture. They enabled organizations not only to overcome short-term logistical disruptions but also played critical roles in transforming external shocks into opportunities for resilience and, ultimately, ensuring long-term organizational stability.

Generally, the five organizational resilience strategies identified in the process model (Figure 2) operate as a technology-driven framework for crisis management. First of all, business continuity planning, supported by digital technologies like cloud computing, is essential for continuing business activities during geopolitical disturbances to enable rapid relocation and data transfer. Remote work strategies strengthen organizational stability by allowing employees to sustain productivity and communication from any place, hence providing uninterrupted operational continuity amid crises. Real-time threat detection platforms and automated recovery enable organizations to maintain cyber resilience by reducing downtime and ensuring consistent performance during ongoing cyberattacks. During infrastructure disruptions, companies can maintain coordination and quickly deploy resources by mobilizing digital technology, such as satellite communication systems. Last but not least, digital tools enhance supply chain flexibility by enabling quick scenario planning, identifying alternative sourcing regions to reduce geopolitical risks. Together these technology-driven strategies create an agile response capability by allowing organizations to adapt real-time to disturbances, reallocate resources, and preserve continuity of business operations. In this way, organizational resilience translates into stability, since resilient firms sustain their core objectives under stress and quickly regain equilibrium after crises.

6. Limitations

This study provides useful insights into the relationship between technology and organizational resilience during disruptive situations. It is important to understand certain limitations that influence the scope and relevancy of its findings. The research sample was average in size and sourced from a limited number of industries only in Kazakhstan. The semi-structured interviews offered comprehensive insights but the absence of representation from sectors like healthcare and education limits the validity of the conclusions across industries with varying digital infrastructure requirements and operational contexts.

Secondly, the exclusive use of qualitative approaches, while suitable for examining lived experiences and contextual circumstances, results in findings that lack the statistical foundation necessary for broader comparisons. The ability to compare patterns between different organizational types or geographical areas is limited due to the lack of measurable criteria. Because this study relies on analytical self-reporting, it can lead to memory deformations and biased interpretations. Also, participants may mistakenly filter their own experiences, prioritizing certain elements over others, which has an effect on the consistency and objectivity of the results.

Lastly, the cross-sectional design of the study provides entirely a view of organizational reactions at a certain moment in time. Long-term adjustments, like the arrangement of emergency practices, the transformation of leadership priorities or the discontinuation of ineffective tools, are beyond the analytical scope of the study.

7. Recommendations

Building on the findings and limitations of this research, multiple sources are recommended for future studies to deepen the understanding of how technologies strengthen organizational resilience. First, expanding the sample size and broadening industry types would enhance the richness and applicability of future findings. A more diverse participant base including organizations of varying sizes, digital maturity levels, and sectors would allow for comparisons across different resilience strategies and contexts, and strengthen the external effectiveness of the conclusions.

Second, recommend for future research consider adopting a longitudinal design that tracks technological responses before, during, and after disruption, because this would offer a clearer picture of how digital initiatives develop over time, whether short-term fixes mature into lasting capabilities, and how organizations reconfigure their operations in the post-crisis phase. In particular, focusing on the post-disruption phase would provide more valuable insights into the sustainability and arrangement of resilience-building measures.

Third, combining qualitative interviews with quantitative methods could reveal a comprehensive view of the whole problem. For instance, integrating interviews with organizational metrics such as technology adoption rates, recovery timelines, or digital resilience indices would allow researchers to triangulate insights and test emerging models at scale. This mixed-methods approach would not only enhance analytical accuracy but also support the development of frameworks that are both theoretically sound and practically relevant.

In addition, future studies may benefit from making narrow focus to specific industries such as manufacturing, logistics, or education where digital responses to disruption can be examined in detail. This would help identify contextual drivers, bottlenecks, and successful strategies that may be concealed in more generalized studies.

Finally, integrating broader theoretical frameworks such as socio-technical systems theory, dynamic capabilities, or institutional theory could enrich the conceptual grounding of future work. These lenses would help illuminate the agreement between technological adaptation and non-digital factors like leadership styles, organizational learning, and stakeholder coordination, offering a more comprehensive understanding of how resilience is constructed in complex environments.

8. Conclusion

In an increasingly digital world, technologies are a critical part of organizational resilience enablement. Digital tools now are at the center of enhancing an organization's capabilities to prepare for, respond to, adapt to and recover from disruptions.

This paper qualitatively explored the role of digital technologies in creating resilience strategies to address disruptions. As a result, a process model (Figure 2) was developed, which demonstrates how disruptions initiate technology-driven responses, which subsequently enhance organizational resilience and ultimately result in long-term stability. As a conceptual link between strategy and practice, this process model illustrates how resilience is operationalized through technology.

Currently, organizations are facing an increasing range of disruptions, such as geopolitical conflict, natural hazards, cyber-attacks, economic instabilities and public health crises. Although these crises vary in scope and duration, all of them threaten core operations and demand rapid, adaptive responses. In order to mitigate such pressures, companies are implementing resilience strategies such as Business Continuity Planning, Remote Work Enablement, Cyber Resilience, Resource Mobilization, and Supply Chain Flexibility. These strategies are not fixed traits, but as stated by Hollnagel (2010), these are "something an organization does rather than something it has". Meaning these are flexible tools that allow organizations maintain core function while mitigating risks and adapting to changing environments.

These resilience strategies significantly rely on digital technologies. They provide the tools to foresee disruptions early, respond with agility, and maintain operational coherence under stress. For example, cloud infrastructure supports remote work, cybersecurity platforms defend against digital threats, AI and analytics assist with resource planning, and supply chain technologies enhance visibility and flexibility. As shown in the Technology-Driven Response phase of the model (Figure 2), technologies are the operational core that activates and scales these strategies, transforming abstract plans into real-time actions.

Organizational resilience, once activated, serves as a buffer and stabilizer during disruption. By using technologies to absorb shocks and maintain continuity, organizations reduce the time and cost of recovery, preserve trust with stakeholders, and protect strategic objectives. Over time, this resilience generates organizational stability by increasing the capacity to adapt and reconfigure without losing identity or function. The process model visualizes this as a reinforcing loop: the more effectively organizations integrate technology into resilience strategies, the more stability they build over time.

In summary, research demonstrates that technologies are indispensable components of how resilience is achieved in current days. Digital tools facilitate the coordination, flexibility, and rapidity necessary to transform disruption into manageable change. Implementing these technologies into strategic processes, allow organizations not only to improve their immediate responsiveness but also establishes the foundation for sustained stability in an unpredictable environment. This research's process model offers a framework for understanding and applying these strategies, providing a guide for both researchers and practitioners seeking to build more resilient organizations through technology.

References

- Aldianto, L., Anggadwita, G., Permatasari, A., Mirzanti, I. R., & Williamson, I. O. (2021). Toward a business resilience framework for startups. Sustainability, 13(6), 3132. https://doi.org/10.3390/su13063132
- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50–58. https://doi.org/10.1145/1721654.1721672
- Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational Cyber resilience: management perspectives. AJIS. Australasian Journal of Information Systems/AJIS. Australian Journal of Information Systems/Australian Journal of Information Systems, 27. https://doi.org/10.3127/ajis.v27i0.4183
- Benner, M. J., & Waldfogel, J. (2020). Changing the channel: Digitization and the rise of "middle tail" strategies. Strategic Management Journal, 44(1), 264–287. https://doi.org/10.1002/smj.3130
- Bharadwaj, A., Sawy, O. a. E., Pavlou, P. A., & Venkatraman, N. (2013). Digital Business Strategy: Toward a next generation of insights. MIS Quarterly, 37(2), 471–482. https://doi.org/10.25300/misq/2013/37:2.3
- Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience – fundamentals for a definition. In Advances in intelligent systems and computing (pp. 311–316).
- Burnard, K., & Bhamra, R. (2011). Organisational resilience: Development of a conceptual framework for organisational responses. International Journal of Production Research, 49(18), 5581–5599. https://doi.org/10.1080/00207543.2011.563827
- Burnard, K., Bhamra, R., & Tsinopoulos, C. (2018). Building organizational resilience: four configurations. IEEE Transactions on Engineering Management, 65(3), 351–362. https://doi.org/10.1109/tem.2018.2796181
- Cater, J. K. (2011). Skype: A cost-effective method for qualitative research. Rehabilitation Counselors & Educators Journal, 4(2), 10–17.
- Cerullo, V., & Cerullo, M. J. (2004). Business Continuity Planning: a comprehensive approach. Information Systems Management, 21(3), 70–78. https://doi.org/10.1201/1078/44432.21.3.20040601/82480.11
- Creswell, J. W. (2013). Qualitative inquiry and research design: Choosing among five approaches (3rd ed.). SAGE Publications.
- Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.
- Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

- De Araujo, M. S., Machado, B. a. S., & Passos, F. U. (2024). Resilience in the context of Cyber Security: A review of the fundamental concepts and relevance. Applied Sciences, 14(5), 2116. https://doi.org/10.3390/app14052116
- DHS. (2015). Satellite-Phones TechNote. U.S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/Satellite-Phones-TN_0615-508_0.pdf
- Dubey, R., Gunasekaran, A., Childe, S. J., Blome, C., & Papadopoulos, T. (2019). Big Data and Predictive Analytics and Manufacturing performance: Integrating institutional theory, Resource-Based View and Big Data culture. British Journal of Management, 30(2), 341–361. https://doi.org/10.1111/1467-8551.12355
- Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. Business Research, 13(1), 215–246. https://doi.org/10.1007/s40685-019-0085-7
- Garrido-Moreno, A., Martín-Rojas, R., & García-Morales, V. J. (2024). The key role of innovation and organizational resilience in improving business performance: A mixed-methods approach. International Journal of Information Management, 77, 102777. https://doi.org/10.1016/j.ijinfomgt.2024.102777
- Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia Methodology. Organizational Research Methods, 16(1), 15–31.
- Gruben, M., Sheil, A., Das, S., O Keeffe, M., Camilleri, J., Cronin, M., & Murray, H. (2025). “It’s like not being able to read and write”: Narrowing the digital divide for older adults … arXiv.
- Guest, G., Bunce, A., & Johnson, L. (2005). How many interviews are enough? Field Methods, 18(1), 59–82. https://doi.org/10.1177/1525822x05279903
- Holling, C. S. (1973). Resilience and Stability of Ecological Systems. Annual Review of Ecology and Systematics, 4, 1–23. http://www.jstor.org/stable/2096802
- Holling, C.S. (1996) Engineering Resilience versus Ecological Resilience. In: Schulze, P.E., Ed., Engineering within Ecological Constraints, National Academy Press, Washington DC, 31-43.
- Hollnagel, E. (2010, May). How resilient is your organisation? An introduction to the Resilience Analysis Grid (RAG). In Sustainable Transformation: Building a Resilient Organization, Toronto, Canada
- Hu, L., Zhou, J., Zhang, J. Z., & Behl, A. (2023). Blockchain technology adaptation and organizational inertia: moderating role between knowledge management processes and supply chain resilience. Kybernetes, 53(2), 515–542. https://doi.org/10.1108/k-12-2022-1661
- Ibrahim, O. (2024). Impact of cloud computing on business continuity and disaster recovery. Journal of Technology and Systems, 6(5), 16–28. https://doi.org/10.47941/jts.2146
- Itakura, K. (2019). Evaluating the impact of the US–China trade war. Asian Economic Policy Review, 15(1), 77–93. https://doi.org/10.1111/aepr.12286
- Jordan, M. I., Mitchell, T. M., M. De Choudhury, S. Counts, E. Horvitz, A. Hoff, J. S. Brownstein, C. C. Freifeld, L. C. Madoff, G. Eysenbach, D. A. Broniatowski, M. J. Paul, M. Dredze, A. Sadilek, H. Kautz, V. Silenzio, R. W. White, R. Harpaz, N. H. Shah, . . . M. Schrems. (n.d.). Machine learning: Trends, perspectives, and prospects. https://www.cs.cmu.edu/~tom/pubs/Science-ML-2015.pdf

- Kitsios, F., & Kamariotou, M. (2021). Artificial Intelligence and Business Strategy towards Digital Transformation: A Research Agenda. Sustainability, 13(4), 2025. https://doi.org/10.3390/su13042025
- Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2010). Developing a capacity for organizational resilience through strategic human resource management. Human Resource Management Review, 21(3), 243–255. https://doi.org/10.1016/j.hrmr.2010.07.001
- Meena G. & Santhanalakshmi k. (2023) ORGANIZATIONAL RESILIENCE: ADAPTING TO RAPID TECHNOLOGICAL CHANGES, 287-296
- Mikalef, P., Krogstie, J., Pappas, I. O., & Pavlou, P. (2019). Exploring the relationship between big data analytics capability and competitive performance: The mediating roles of dynamic and operational capabilities. Information & Management, 57(2), 103169. https://doi.org/10.1016/j.im.2019.05.004
- Nauck, F., Pancaldi, L., Poppensieker, T., & White, O. (2021, May 17). The resilience imperative: Succeeding in uncertain times. McKinsey & Company. https://www.mckinsey.com/business%20functions/risk-and-resilience/our-insights/the-resilience-imperative-succeeding-in-uncertain%20times
- Ning, Y., Li, L., Xu, S. X., & Yang, S. (2023). How do digital technologies improve supply chain resilience in the COVID-19 pandemic? Evidence from Chinese manufacturing firms. Frontiers of Engineering Management, 10(1), 39–50. https://doi.org/10.1007/s42524-022-0230-4
- Ortiz-de-Mandojana, N., & Bansal, P. (2015). The long-term benefits of organizational resilience through sustainable business practices. Strategic Management Journal, 37(8), 1615–1631. https://doi.org/10.1002/smj.2410
- Paeffgen, T. (2023). Organisational Resilience during COVID-19 Times: A Bibliometric Literature Review. Sustainability, 15(1), 367. https://doi.org/10.3390/su15010367
- PwC. (2020). Scale your way to digital upskilling success. ProEdge.
- Research Dive. (2021). Why Mobile Satellite Phones are Proving to be a Beneficial Device. Retrieved from ResearchDive.com database.
- Sabadosa, Z., Rengifo, M. C., Resendez, P. S., Beato, A.R., Said E., & Styers, K., (2024). Trade Titans: The Impact of the U.S.-China Trade War on Global Economics
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for businesses Resilience: Issues and recommendations. Sensors, 23(15), 6666. https://doi.org/10.3390/s23156666
- Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2017). Building organizational resilience in the face of multiple disruptions. International Journal of Production Economics, 197, 63–83. https://doi.org/10.1016/j.ijpe.2017.12.009
- Sambamurthy, N., Bharadwaj, N., & Grover, N. (2003). Shaping Agility through Digital Options: Reconceptualizing the Role of Information Technology in Contemporary Firms. MIS Quarterly, 27(2), 237. https://doi.org/10.2307/30036530
- Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2017). Saturation in qualitative research: exploring its conceptualization and operationalization. Quality & Quantity, 52(4), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8
- Shah, K., (2024). SATELLITE COMMUNICATIONS IN PUBLIC SAFETY: ENHANCING EMERGENCY RESPONSE THROUGH ADVANCED CONNECTIVITY. International Journal of Advanced Research in Engineering and Technology (IJARET), 15(5), 212–232.

- Shahzad, U., Mohammed, K. S., Tiwari, S., Nakonieczny, J., & Nesterowicz, R. (2022). Connectedness between geopolitical risk, financial instability indices and precious metals markets: Novel findings from Russia Ukraine conflict perspective. Resources Policy, 80, 103190. https://doi.org/10.1016/j.resourpol.2022.103190
- Shakhatreh, H., Hayajneh, K., Bani-Hani, K., Sawalmeh, A., & Anan, M. (2021). Cell on Wheels–Unmanned Aerial Vehicle System for Providing Wireless Coverage in Emergency Situations. Journal of Telecommunications Engineering.
- Shaluf, I. M., Ahmadun, F., & Said, A. M. (2003). A review of disaster and crisis. Disaster Prevention and Management an International Journal, 12(1), 24–32. https://doi.org/10.1108/09653560310463829
- Sheffi, Y. (2006). The resilient enterprise: overcoming vulnerability for competitive advantage. Choice Reviews Online, 43(06), 43–3481. https://doi.org/10.5860/choice.43-3481
- Skouloudis, A., Tsalis, T., Nikolaou, I., Evangelinos, K., & Filho, W. L. (2020). Small & Medium-Sized Enterprises, Organizational Resilience Capacity and Flash Floods: Insights from a Literature Review. Sustainability, 12(18), 7437. https://doi.org/10.3390/su12187437
- Smith, R. (2022). "Digital Resilience in an Age of Disruption: Cybersecurity Strategies for Global Enterprises." Journal of International Business Security, 15(3), 45-67.
- Sonnenfeld, J., Tian, S., Zaslavsky, S., Bhansali, Y., & Vakil, R. (2022). It pays for companies to leave Russia. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4112885
- Stoverink, A. C., Kirkman, B. L., Mistry, S., & Rosen, B. (2018). Bouncing back together: toward a theoretical model of work team resilience. Academy of Management Review, 45(2), 395–422. https://doi.org/10.5465/amr.2017.0005
- Su, W., & Junge, S. (2023). Unlocking the recipe for organizational resilience: A review and future research directions. European Management Journal, 41(6), 1086–1105. https://doi.org/10.1016/j.emj.2023.03.002
- Suryasa, I. W., Rodríguez-Gámez, M., & Koldoris, T. (2021). COVID-19 pandemic. International Journal of Health Sciences, 5(2), vi–ix. https://doi.org/10.53730/ijhs.v5n2.2937
- Sutcliffe, K. M., & Vogus, T. J. (2003). Organizing for resilience. In K. S. Cameron, J. E. Dutton, & R. E. Quinn (Eds.), Positive organizational scholarship: Foundations of a new discipline (pp. 94–110). Berrett-Koehler.
- Tosun, O. K., & Eshraghi, A. (2022). Corporate decisions in times of war: Evidence from the Russia-Ukraine conflict. Finance Research Letters, 48, 102920. https://doi.org/10.1016/j.frl.2022.102920
- Vanany, I., Ali, M. H., Tan, K. H., Kumar, A., & Siswanto, N. (2021). A supply chain resilience capability framework and process for mitigating the COVID-19 pandemic disruption. IEEE Transactions on Engineering Management, 71, 10358–10372. https://doi.org/10.1109/tem.2021.3116068
- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003
- Young, S., Balluz, L., & Malilay, J. (2003). Natural and technologic hazardous material releases during and after natural disasters: a review. The Science of the Total Environment, 322(1–3), 3–20. https://doi.org/10.1016/s0048-9697(03)00446-7

- Zhang, J., Li, H., & Zhao, H. (2025). The Impact of Digital Transformation on Organizational Resilience: The Role of Innovation Capability and Agile Response. Systems, 13(2), 75. https://doi.org/10.3390/systems13020075
- Zhang, J., Long, J., & Von Schaewen, A. M. E. (2021). How Does Digital Transformation Improve Organizational Resilience?—Findings from PLS-SEM and fsQCA. Sustainability, 13(20), 11487. https://doi.org/10.3390/su132011487

Appendice-1

Interview questions:

Can you briefly describe your role in the organization?

How would you define organizational resilience in your company's context?

Could you share an example of a significant disruption your organization experienced and how it was managed?

What types of digital or information technologies were used to respond to or manage that disruption?

In what ways did these technologies contribute to your organization's ability to adapt, respond, or recover?

Are there any technologies that your organization has adopted specifically to improve resilience? Why those?

What challenges have you faced in implementing or relying on technology during disruptions?

Looking ahead, what technologies do you believe will be most critical to strengthening organizational resilience?

List of figures

Figure 1. Data structure

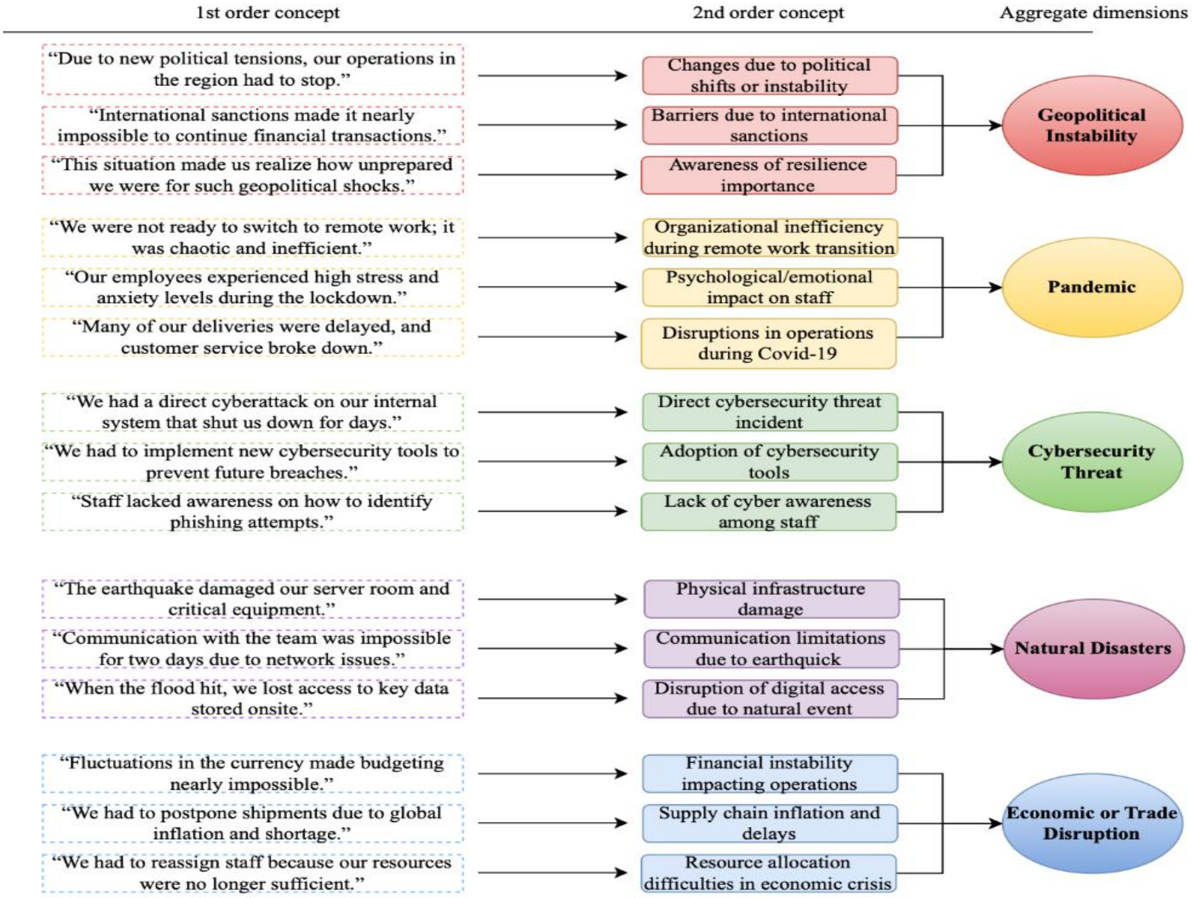
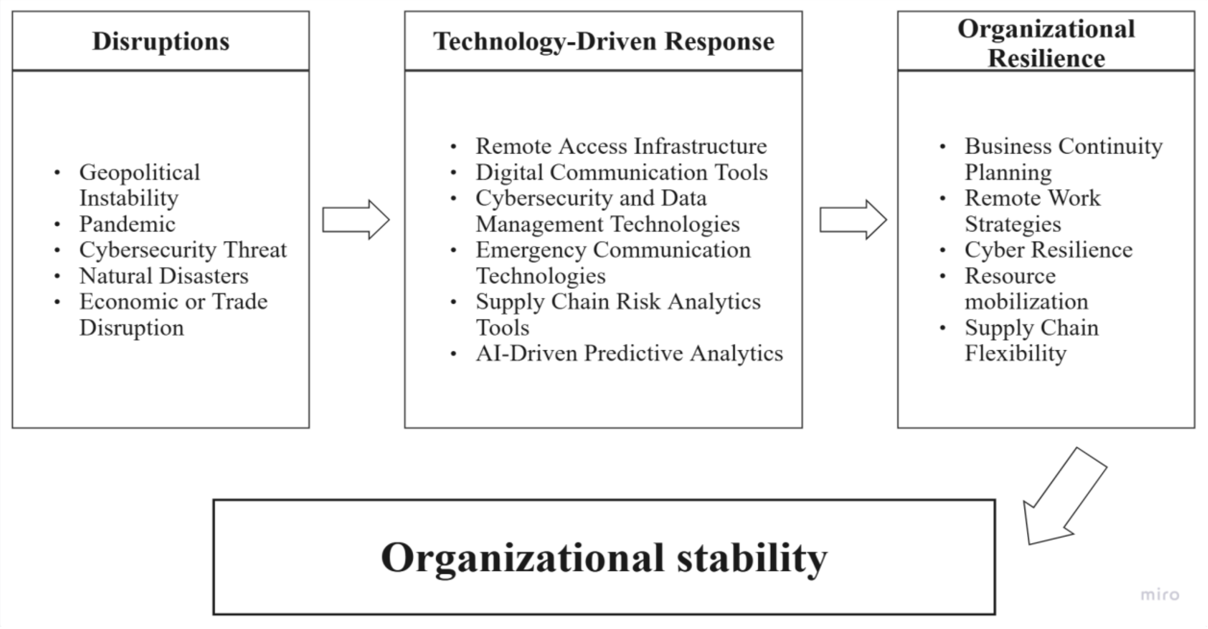

1st order concept
2nd order concept
Aggregate dimensions
"Due to new political tensions, our operations in the region had to stop."
Changes due to political shifts or instability
"International sanctions made it nearly impossible to continue financial transactions."
Barriers due to international sanctions
"This situation made us realize how unprepared we were for such geopolitical shocks."
Awareness of resilience importance
Geopolitical Instability
"We were not ready to switch to remote work; it was chaotic and inefficient."
Organizational inefficiency during remote work transition
"Our employees experienced high stress and anxiety levels during the lockdown."
Psychological/emotional impact on staff
"Many of our deliveries were delayed, and customer service broke down."
Disruptions in operations during Covid-19
Pandemic
"We had a direct cyberattack on our internal system that shut us down for days."
Direct cybersecurity threat incident
"We had to implement new cybersecurity tools to prevent future breaches."
Adoption of cybersecurity tools
"Staff lacked awareness on how to identify phishing attempts."
Lack of cyber awareness among staff
Cybersecurity Threat
"The earthquake damaged our server room and critical equipment."
Physical infrastructure damage
"Communication with the team was impossible for two days due to network issues."
Communication limitations due to earthquick
"When the flood hit, we lost access to key data stored onsite."
Disruption of digital access due to natural event
Natural Disasters
"Fluctuations in the currency made budgeting nearly impossible."
Financial instability impacting operations
"We had to postpone shipments due to global inflation and shortage."
Supply chain inflation and delays
"We had to reassign staff because our resources were no longer sufficient."
Resource allocation difficulties in economic crisis
Economic or Trade Disruption

Figure 2. Process model



Disruptions
- Geopolitical Instability
- Pandemic
- Cybersecurity Threat
- Natural Disasters
- Economic or Trade Disruption
Technology-Driven Response
- Remote Access Infrastructure
- Digital Communication Tools
- Cybersecurity and Data Management Technologies
- Emergency Communication Technologies
- Supply Chain Risk Analytics Tools
- AI-Driven Predictive Analytics
Organizational Resilience
- Business Continuity Planning
- Remote Work Strategies
- Cyber Resilience
- Resource mobilization
- Supply Chain Flexibility
Organizational stability
miro