https://doi.org/10.47641/JRS.2026-13-1.01
Palestine Technical College Journal for Research and Studies **ISSN 2518-5721**
Vol. 13, **No.** 1, 2026, **pp.** 1-23

Received: (21-06-2026), **Accepted:** (30-07-2026)

Digital Resilience of Software Development under Crisis: The Role of Remote Operations and Green Computing in Ensuring Operational Continuity in Gaza

Yousef A. Yousef[1*]	**Wessam M. Kollab[2]**
Al-Aqsa University, Palestine [1] ya.yousef@alaqsa.edu.ps ORCID: 0009-0003-0542-7193 [2] wm.kolabh@alaqsa.edu.ps ORCID: 0009-0008-5793-6412 * Corresponding author	

Abstract:
This study examines the impact of large-scale technological disruptions caused by the war in the Gaza Strip since October 2023 on software development projects, and the role of Resilient Technological Strategies (RTS), which encompass remote operations and green computing practices, in maintaining operational continuity and organizational resilience. A quantitative descriptive-analytical approach was employed, using data collected from 150 software professionals, including software engineers, project managers, quality assurance engineers, and UI/UX designers. Data were analyzed using SPSS and AMOS through descriptive statistics, Pearson correlation, exploratory and confirmatory factor analysis, and structural equation modeling (SEM). The findings indicate that infrastructure disruption is strongly associated with the adoption of RTS and, contrary to the hypothesized direction, shows a significant positive direct effect on operational continuity. RTS, in turn, significantly enhance operational continuity and partially mediate (complementary partial mediation) the relationship between infrastructure disruption and operational continuity. The study concludes that software organizations in war-affected environments can strengthen operational continuity and adaptive capacity through remote operational models, cloud-based solutions, and energy-efficient computing practices, contributing to the literature on digital resilience and crisis-induced technological adaptation.
Keywords: Software Development Resilience; Siege-Induced Infrastructure Disruption and Risks; Remote Operations; Cloud Computing; Green Computing; Resource Optimization

License: CC BY 4.0 (https://creativecommons.org/licenses/by/4.0/). © Copyright held by the authors.

Introduction

Since October 7, 2023, the Gaza Strip has been exposed to extensive and sustained bombardment by Israel. Infrastructure destruction has reached unprecedented levels. Critical infrastructure, including electricity and telecommunications networks, as well as key sectors such as education, healthcare, industry, agriculture, and information technology, has been severely affected. These systems and sectors constitute the foundation of socioeconomic development. National and international bodies have recorded infrastructure damage above 90% in some areas, and the continuing deterioration will deepen both humanitarian and operational difficulties (Abuawad et al., 2025; Palestinian Central Bureau of Statistics, 2024; The World Bank et al., 2024). With critical systems down, daily life and the way institutions work have changed sharply. Organizations now operate under extreme constraints marked by uncertainty, volatility, and scarce resources, and institutions and companies have moved step by step toward remote operating models and other survival strategies.

To keep operational continuity going, organizations have turned to several measures, among them renewable/hybrid energy solutions (solar energy, local generators, and rechargeable batteries) and temporary shared workspaces (Younis & Tunç, 2023). These adaptations point to a move away from traditional organizational structures toward crisis-based models of operational resilience, which depend on continuous adaptability, decentralization, and technological innovation. Because the software development industry depends heavily on reliable electricity, internet connectivity, and access to digital infrastructure, it has been one of the most affected sectors (Hollnagel et al., 2006). These disruptions reduced collaboration among programmers and engineers and negatively affected software development activities, as power shortages, communication disruptions, and mobility restrictions significantly constrained daily operations. Software companies have been driven toward remote operations models and have increasingly adopted technological approaches, including green computing, cloud-based infrastructure, and advanced software risk management practices.

According to socio-technical resilience theories and frameworks of crisis adaptation, the process of transformation can be understood in terms of the interrelationship between technological systems, organizational structures, and environmental constraints surrounding the system (Baek et al., 2015). In particular, there is a shift in software development in a crisis context from optimizing for efficiency to adapting for survival through continuity of operations as opposed to maximization of performance (Tucnik et al., 2023; Zhang et al., 2025). As a result, risk management, green computing, and remote operations represent interconnected mechanisms of resilience, not independent or autonomous activities.

Although research on organizational resilience, digital transformation and crisis management has gained increasing attention, limited studies have examined these concepts in environments affected by a crisis, particularly in regions experiencing conflict. To address this gap, this study introduces the concept of Resilient Technology Strategies (RTS). In this study, RTS are the technological and managerial strategies that help organizations cope with infrastructure disruption so that they can keep working under crisis conditions; they include remote operations and green computing. Operational continuity is the ability of an organization to keep its core software development activities running despite disruption and environmental uncertainty.

This study looks at how RTS have been adopted in the software sector of the Gaza Strip and how they support organizational resilience during a crisis. It also takes current software

engineering theories beyond the stable, traditional settings they come from and applies them to extreme and conflict-affected environments, adding to the emerging literature on crisis-driven digital transformation and technological resilience.

Literature Review

Software Development in Crisis and Conflict Environments

Software development is a complex and dynamic process that involves managing several phases of the project life cycle, including requirements analysis, design, implementation, testing, and deployment (Dey et al., 2007; Sanmocte & Costales, 2025; Tucnik et al., 2023; Yousef, 2022).

Software projects can be inherently exposed to various types of risk arising from communication failures, cybersecurity threats, budget overruns and schedule delays (Aregbesola et al., 2025). Risks are defined as uncertain future events that could affect the project outcome if they occur (Dey et al., 2007). Effective software risk management therefore has to identify, assess, monitor, and mitigate risks continuously across the whole software development lifecycle. This enhances project success and organizational resilience (Arnuphaptrairong, 2011; Pilliang & Munawar, 2022).

However, compared to regular situations, software development risks are much more serious in crisis or conflict areas. Infrastructure destruction compounds traditional operational and technical risks, such as population displacement, electricity shortages, internet disruptions, and elevated psychological stress. Such circumstances generate uncertainty in the technological, managerial, and human aspects of software development (Zhang et al., 2025). Faced with a growing amount of uncertainty, organizations are compelled to develop adaptable and decentralized operational models in order to ensure continuity. Before the current crisis, agile approaches have assisted software companies in Gaza by enhancing teamwork, communication, leadership, and planning processes (Pilliang & Munawar, 2022; Yousef, 2022). Due to the destruction of telecommunications and electricity infrastructure, software companies had to move more quickly toward remote operations, distributed teams, and cloud-based systems in order to maintain continuity.

Organizational vulnerability in these settings can be significantly affected by the absence of structured and adaptive risk management, particularly in Small and Medium-sized Enterprises (SMEs), whose survival hinges on proactive risk mitigation and ongoing operational adaptation (Ekwere, 2016). Consequently, software firms in Gaza increasingly rely on cloud computing, distributed architectures, remote backups, remote operations, and adaptive governance mechanisms to continue making progress toward their development plans to cope with the extreme infrastructure collapse and disruption triggered by the war. This adaptability aligns with resilience engineering concepts (Hollnagel et al., 2006), which emphasize adaptation over failure avoidance as the primary mechanism for sustaining operations under adverse conditions. However, empirical evidence on the role of green computing and remote operations in supporting operational continuity of software development projects in conflict-affected environments is restricted despite the increased uptake of cloud-based information technologies and remote operations in contexts where there are crisis settings.

Remote Operations and Digital Resilience

In times of crisis, interruptions in business activities can lead to significant financial losses with a long recovery period. Remote operations support businesses in maintaining continuity and

preserving business productivity in times of crisis (McPhail et al., 2024). The increase in remote operations has led to a higher demand for infrastructure for distributed software development, such as cloud storage, virtual collaboration software, asynchronous communication systems and project management systems (Radu, 2017). This decreases the dependence on centralized office locations and enhances organizational agility, enabling distributed teams to stay productive in an uncertain environment (Awwad & Awwad, 2026; McPhail et al., 2024; Sanmocte & Costales, 2025; Zhang et al., 2025).

Most previous studies only frame remote operations as nothing more than an efficiency tool, but in reality, it is a core resilience strategy in conflict-affected zones. Baek et al. (2015), Yousef (2022), and Okolie and Egbon (2025) have each examined digital resilience from a different angle. Software companies in the Gaza Strip have increasingly adopted cloud-based platforms, mobile internet services, freelance work networks, and remote working arrangements to address movement restrictions and the deterioration of critical infrastructure (Younis & Tunç, 2023). These measures bring clear operational benefits, but they also create problems of their own: cybersecurity weaknesses, unstable internet access, power outages, weaker managerial oversight, and more psychological pressure on employees (Emanuel & Harrington, 2024; Okolie & Egbon, 2025). Pushing digital transformation further, developing workforce skills, preparing better for cyber threats, and adopting adaptive management practices can all contribute to long-term organizational resilience and sustainability. Seen this way, remote operations are a strategic capability for staying in operation through prolonged crises, and not only a short-term reaction to disruption.

Green Computing and Energy Adaptation

As environmental problems have grown, green computing has drawn more research attention. The term covers the sustainable design, use, disposal, and recycling of computing resources, with a focus on good resource management because of its positive effect on the economy and the environment (Kollab & Yousef, 2023). Its goal is to raise energy efficiency and lower environmental impact through sustainable software engineering practices and sensible use of resources (Anser et al., 2021; Jeyamurugan et al., 2025; Paul et al., 2023).

Recent research emphasizes that green cloud and edge computing, along with energy-aware task allocation, also improve system efficiency and resilience in resource-limited scenarios. Radu (2017) refers to green cloud computing as a dual-benefit approach that reduces data center energy consumption while improving scalability by shifting workloads to distributed infrastructures. There is also evidence that green computing advocates energy-efficient deployment strategies using workload optimization, task optimization, and cloud resource utilization (Atadoga et al., 2024). These practices support the development of energy-efficient applications and cloud service design without affecting the overall software performance. Wu and Tham (2023) find an interesting connection between environmental regulations and the development and sustainability in business by making technological innovation an accelerator and sustainability and resilient development agents.

The adoption of Environmental, Social, and Governance (ESG) principles, thus, builds environmental consciousness and promotes the development of innovative solutions. Moreover, many organizations today use renewable and alternative energy sources such as solar energy, battery storage systems, and other energy-efficient devices to support business operations during fluctuating power conditions. Devineni and Gorantla (2023) mention that during power

interruptions, runtime power management and hardware optimization can also be adopted to be more adaptable to the operating conditions of the hardware and ensure system functionality.

Although these technical interventions are often covered by the concept of ecological responsibility, their utilization in the conditions of complete electricity grid disruption adds an unexplored level to software engineering. IT and software companies must secure the resources necessary for operational continuity, particularly cloud computing services and renewable energy solutions. Digital transformation, cloud computing, and remote operation are vital to sustain Palestinian institutions during these systemic shocks (Awwad & Awwad, 2026). IT professionals in the Gaza Strip had a prior understanding of green computing, which enabled the implementation of energy-efficient technologies during the recent crisis (Kollab & Yousef, 2023). As such, the Gaza context expands the definition of green computing beyond environmental sustainability and into crisis resilience, operational continuity, and infrastructure adaptation in places of conflict.

Research Hypotheses

Based on the theoretical framework and the identified research gap, this study proposes the following research hypotheses:

H1: There are statistically significant relationships among Siege-Induced Infrastructure Disruption and Risks (SIIDR), Resilient Technology Strategies (RTS), and operational continuity in Gaza's software development sector.

Empirical evidence has demonstrated that adaptive practices, resource efficiency, and proactive risk management contribute to building organizational resilience during a crisis (Ekwere, 2016). Gaza-based companies are increasingly adopting remote management, cloud computing and green computing strategies to enhance operational resilience and overcome operational challenges and disruptions (Kollab & Yousef, 2023; Yousef, 2022).

H2: Siege-Induced Infrastructure Disruption and Risks (SIIDR) have a statistically significant negative effect on operational continuity in the software development sector.

Infrastructure destruction, including damage to electricity networks, telecommunications systems, and office facilities, negatively affects software development continuity and increases operational risks (Dey et al., 2007; Tucnik et al., 2023). In Gaza, the destruction of infrastructure has caused major operational disruption and pushed companies to rely on remote work and cloud-based solutions as temporary adaptations. These approaches, though, cannot fully replace the essential physical infrastructure that has been lost. Consequently, in the absence of sufficient resilience mechanisms, higher levels of infrastructure disruption are expected to result in lower operational continuity (Pilliang & Munawar, 2022).

H3: Siege-Induced Infrastructure Disruption and Risks (SIIDR) have a statistically significant positive effect on the adoption of Resilient Technology Strategies (RTS).

This hypothesis is supported by evidence that crisis severity and IT awareness have a positive impact on the adoption of digital resilience practices (Kollab & Yousef, 2023). In Gaza, the frequent breakdown of infrastructure and power cuts have accelerated the transition from voluntary green computing practices to necessary adoption. Consequently, organizations are increasingly adopting resource optimization, cloud-based systems and energy-efficient technologies as resilience strategies to sustain operations.

H4: Resilient Technology Strategies (RTS) have a statistically significant positive effect on operational continuity in the software development sector under crisis conditions.

Resilient Technology Strategies (RTS) enhance flexibility and continuity; however, they also introduce challenges such as unstable connectivity, increased coordination costs, dependence on hardware availability, and energy constraints (Emanuel & Harrington, 2024; Okolie & Egbon, 2025). Organizations respond to these challenges by adopting cloud-based systems and energy-efficient infrastructures that improve resource utilization and reduce dependency on local physical systems (Aregbesola et al., 2025).

H5: Resilient Technology Strategies (RTS) significantly mediate the relationship between Siege-Induced Infrastructure Disruption and Risks (SIIDR) and operational continuity in the software development sector under crisis conditions.

According to this hypothesis, Resilient Technology Strategies (RTS) act as a mediator between Siege-Induced Infrastructure Disruption and Risks (SIIDR) and operational continuity, because they allow software firms to limit the effects of disruption and keep operations stable in a crisis (Sutcliffe & Vogus, 2003; Yousef, 2022).

Research Methodology

A quantitative methodology was used to examine how Siege-Induced Infrastructure Disruption and Risks (SIIDR) after October 2023 affected the adoption of Resilient Technology Strategies (RTS) and operational continuity in Gaza's software development sector.

Research Design

The study used a quantitative descriptive–analytical design to measure how far infrastructure had been disrupted and how software development professionals responded. This design suits the examination of relationships among variables and the testing of hypotheses on SIIDR, remote operations, green computing, and resource optimization. The study model assumes that crisis conditions shape organizational resilience through technological and operational adaptation mechanisms, which are represented here by RTS.

Population and Sampling

The study targeted software development professionals in the information technology and software industry in the Gaza Strip. The final sample included 150 professionals, some of whom remained in Gaza and some of whom were displaced from their homes after the events of October 2023. The participants included software engineers, project managers, quality assurance engineers, user interface/user experience designers, and other professionals involved in software development activities. Since there was no official database for the number of software development professionals in Gaza during the ongoing crisis, their number could not be determined. Displacement and the shift in communication channels also made potential participants hard to reach. For this reason, the study relied on non-probability sampling, combining convenience and snowball techniques through professional social networks (i.e., WhatsApp, Telegram, and LinkedIn).

Statistical power for the CFA model was checked a priori with the RMSEA-based approach of MacCallum et al. (1996). With 20 observed indicators, three latent constructs, df = 167, α = 0.05, $RMSEA_0$ = 0.05, and $RMSEA_a$ = 0.08, the sample of 150 respondents gave statistical power above 95%, exceeding the recommended 80% threshold.

Data Collection Instrument

Data were collected through a structured online survey. The initial instrument had two sections. The first asked about respondents' demographic characteristics: job title, gender, education, work experience, working hours, and the main energy source they relied on for their work. The

second section measured the initial study constructs using a five-point Likert scale and included four core dimensions (see Appendix A):

1. Siege-Induced Infrastructure Disruption and Risks (SIIDR)
2. Remote Operations and Cloud Adaptation
3. Green Computing and Resource Optimization
4. Operational Continuity

These dimensions aimed to reflect how software development organizations adapt through operational, technological, and adaptive measures in response to extreme crises.

Validity and Reliability of the Instrument

Content validity was established through expert reviews validating the instrument's representativeness of the constructs being studied. Reliability was assessed using Cronbach's alpha coefficient and all constructs surpassed the recommended threshold of 0.70, indicating acceptable internal consistency. These results validate the measurement instrument and show the appropriateness of the application of further statistical analyses.

Data Analysis Techniques

Two complementary statistical approaches were used for hypothesis testing. The relationship between Resilient Technology Strategies (RTS) and operational continuity was tested using Pearson correlation analysis for H1. The other hypotheses (H2–H5) were tested using Structural Equation Modeling (SEM) to assess the direct and indirect relationships among the study constructs. The data were analyzed using SPSS and AMOS. The following statistical techniques were employed for data analysis:

- Descriptive statistics, including means, standard deviations, and frequencies, were employed to summarize the data.
- Pearson correlation analysis was conducted to examine the relationships among the study constructs.
- Exploratory Factor Analysis (EFA), employing Principal Component Analysis (PCA) with Varimax rotation, was performed to identify the underlying factor structure.
- Confirmatory Factor Analysis (CFA) was conducted to validate the measurement model and assess construct validity.
- Structural Equation Modeling (SEM) was employed to test the research hypotheses and evaluate the structural model.

These analytical procedures enabled a comprehensive assessment of measurement validity and the structural relationships among the study constructs.

Sample Characteristics

Demographic characteristics of the sample (N = 150) are shown in Table (1). Participants consisted of 56.00% females and 44.00% males. The largest groups of respondents were programmers and software developers (37.33%), others (31.33%), UI/UX designers (20.00%), project managers/business owners (7.33%) and QA engineers (4.00%). Most of them had a bachelor's degree (82.67%) and 14.00% had graduate studies, while 3.33% held diplomas. During the crisis, the largest share of participants worked from co-working spaces or cafés using alternative energy (41.33%), followed by tents or displacement centers (37.33%), company headquarters (16.00%), and outside the Gaza Strip (5.33%). In daily working hours, 58.67%

worked 3–6 hours, 27.33% worked less than 3 hours, and 14.00% worked more than 6 hours, indicating that participants maintained a certain level of operational activity during the crisis.

Table (1): Demographic Characteristics of Participants

Variable	Category	Frequency (n)	Percentage (%)
Gender	Male	66	44.00
	Female	84	56.00
Current Job Role	Project Manager / Business Owner	11	7.33
	Programmer / Software Developer	56	37.33
	UI/UX Designer	30	20.00
	Software Quality Assurance (QA) Engineer	6	4.00
	Others	47	31.33
Educational qualification	Diploma	5	3.33
	Bachelor's degree	124	82.67
	Graduate studies	21	14.00
Main workplace and employment during the current crisis period (since October 7th)	From the company headquarters	24	16.00
	From inside a tent or an individual shelter/displacement center.	56	37.33
	Remotely from outside the Gaza Strip (after external displacement).	8	5.33
	From a co-working space / temporary café relying on alternative energy sources.	62	41.33
Average daily available technical working hours during the crisis	Less than 3 hours	41	27.33
	3 to 6 hours	88	58.67
	More than 6 hours	21	14.00
Primary energy source used to power your digital devices:	Commercial / local electric generators	3	2.00
	Solar power system (private or shared)	73	48.67
	Rechargeable batteries and small energy storage units (power banks)	20	13.33
	Private solar power system + commercial generators	54	36.00
Total		**N = 150**	**100%**

Exploratory Factor Analysis (EFA)

To assess construct validity, Exploratory Factor Analysis (EFA) was carried out through Principal Component Analysis (PCA) with Varimax rotation. The analysis started from 24 measurement items and 150 valid responses. The Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy was calculated as 0.842, which suggested that it is a very good sample to use in factor analysis. Bartlett's Test of Sphericity was significant ($p < 0.001$), indicating that the variables are adequately correlated with one another. As demonstrated in Table (2), three factors were extracted with eigenvalues greater than 1 and accounted for 64.78% of the total variance. The three factors correspond to these constructs:

1. Siege-Induced Infrastructure Disruption and Risks (SIIDR)
2. Resilient Technology Strategies (RTS)
3. Operational Continuity.

The initially proposed dimensions of Remote Operations and Cloud Adaptation, and Green Computing, converged into a single factor, indicating a strong empirical association between these technology adaptation practices in crisis context. Moreover, the rotated component matrix presented in Table (3) indicates that four items (Q2.3, Q2.5, Q3.5, and Q4.1) were removed due to cross-loading issues. The remaining items (n = 20) all loaded strongly (> 0.50) on their own factors, which supports the adequacy of the factor structure and the construct validity of the

retained dimensions. Table (2) covers the initial 24-item solution, while Tables (3) and (10) cover the 20 retained items.

Table (2): Total Variance Explained by the Extracted Dimensions

Extracted Dimension	Initial Eigenvalue	% of Variance Explained	Cumulative % of Variance
1	7.34	30.58%	30.58%
2	4.82	20.08%	50.66%
3	3.39	14.12%	64.78%

Table (3) gives the rotated component matrix from the Varimax rotation. Every retained item loaded satisfactorily on its factor, with loadings between 0.512 and 0.890, above the recommended threshold of 0.50. The three factors are:

1. Siege-Induced Infrastructure Disruption and Risks (SIIDR): Items on infrastructure damage and operational risks, capturing how infrastructure disruption affects software development activities.
2. Resilient Technology Strategies (RTS): Items on technology-enabled adaptation practices such as remote operations, green computing, and Lightweight Development Practices.
3. Operational Continuity: Items on operational continuity, that is, how well software organizations keep development activities going despite ongoing disruption.

No substantial cross-loadings were found, which adds support for the factor structure and gives preliminary evidence of construct validity.

Table (3): Rotated Component Matrix (Factor Loadings per Item)

Item Code	Core Item Concept / Statement	Factor 1: Siege-Induced Infrastructure Disruption and Risks (SIIDR)	Factor 2: Resilient Technology Strategies (RTS)	Factor 3: Operational Continuity
Q1.2	Office and server destruction increased data loss risk.	0.78		
Q1.3	Alternative energy and communication solutions increased development time.	0.64		
Q1.4	Alternative energy and internet solutions increased operational costs.	0.68		
Q1.5	Project delays increased contract and penalty risks.	0.61		
Q1.6	Power and communication outages reduced software quality and testing effectiveness.	0.78		
Q3.1	Infrastructure disruptions increased reliance on low-power devices.	0.65		
Q3.2	Resource constraints encouraged the use of lightweight development environments.	0.65		
Q4.4	Energy and connectivity expenses increased production costs.	0.66		
Q2.1	Remote operations enabled task distribution during displacement.		0.70	
Q2.2	Cloud servers facilitated rapid remote operations.		0.89	
Q2.4	Remote operations improved staff safety.		0.53	
Q2.6	Remote Agile practices supported project rescheduling.		0.65	

Item Code	Core Item Concept / Statement	Factor 1: Siege-Induced Infrastructure Disruption and Risks (SIIDR)	Factor 2: Resilient Technology Strategies (RTS)	Factor 3: Operational Continuity
Q3.3	Remote operations enabled flexible work despite power and internet constraints.		0.64	
Q3.4	Green cloud computing reduced dependence on local servers and power consumption.		0.66	
Q3.6	Green computing became essential for sector continuity.		0.55	
Q4.6	Lightweight development practices improved efficiency during the crisis.		0.81	
Q1.1	Companies resumed operations after initial disruption.			0.67
Q4.2	Software development continued despite power outages.			0.512
Q4.3	Low-cost cloud solutions helped control budgets.			0.757
Q4.5	Remotely developed software maintained required standards.			0.622

Reliability Analysis of the Measurement Scales

As Table (4) shows, internal consistency was strong for all constructs, with Cronbach's Alpha values between 0.794 and 0.871. Reliability for the overall scale was also high ($\alpha = 0.895$), so the instrument was suitable for further statistical analysis.

Table (4): Reliability Analysis of Study Dimensions

Construct / Dimension	Number of Items	Cronbach's Alpha	Internal Consistency Status
Siege-Induced Infrastructure Disruption and Risks (SIIDR)	8	0.842	Highly Reliable / Excellent
Resilient Technology Strategies (RTS)	8	0.871	Highly Reliable / Excellent
Operational Continuity	4	0.794	Reliable / Very Good
Overall Research Instrument (Total Scale)	20	0.895	Highly Reliable / Robust

Results

Descriptive Analysis

Siege-Induced Infrastructure Disruption and Risks

Descriptive statistics for Siege-Induced Infrastructure Disruption and Risks (SIIDR) appear in Table (5). The composite mean score was high ($M = 4.42$, $SD = 0.54$), indicating that respondents strongly perceived the severity of infrastructure disruption and its impact on software development in the Gaza Strip. The highest-rated item was Q1.4, which reflected the additional costs associated with securing alternative energy and internet solutions ($M = 4.72$, $SD = 0.52$). This was followed by Q1.3, which indicated that searching for alternative energy and communication sources increased software development time ($M = 4.66$, $SD = 0.57$). Other highly rated impacts included Q4.4, which reflected the increase in production cost due to additional energy costs ($M = 4.61$, $SD = 0.61$), and Q1.2, which reflected the increased risk of data loss due to the destruction of offices and local servers ($M = 4.53$, $SD = 0.73$). Respondents

also strongly agreed that power and communication outages negatively affected software quality and testing effectiveness (Q1.6, M = 4.45, SD = 0.69). Respondents also saw contract and penalty risks as a significant operational challenge (Q1.5, M = 4.28, SD = 0.86). Agreement was high for adaptive responses as well, such as greater reliance on low-power devices (Q3.1, M = 4.16, SD = 0.78) and moving development environments to lighter, less CPU-intensive configurations (Q3.2, M = 3.94, SD = 0.89). Taken together, these results suggest that infrastructure disruption in the Gaza Strip has placed heavy financial, operational, and technical pressure on software development organizations, which have had to fall back on costly, resource-constrained coping mechanisms to keep working.

Table (5): Siege-Induced Infrastructure Disruption and Risks (SIIDR)

Item Code	Core Item Concept / Statement	Mean (M)	Standard Deviation (SD)	Rank
Q1.4	Alternative energy and internet solutions increased operational costs.	4.72	0.52	1
Q1.3	Alternative energy and communication solutions increased development time.	4.66	0.57	2
Q4.4	Energy and connectivity expenses increased production costs.	4.61	0.61	3
Q1.2	Office and server destruction increased data loss risk.	4.53	0.73	4
Q1.6	Power and communication outages reduced software quality and testing effectiveness.	4.45	0.69	5
Q1.5	Project delays increased contract and penalty risks.	4.28	0.86	6
Q3.1	Infrastructure disruptions increased reliance on low-power devices.	4.16	0.78	7
Q3.2	Resource constraints encouraged the use of lightweight development environments.	3.94	0.89	8
Composite	SIIDR	4.42	0.54	—

Resilient Technology Strategies (RTS)

Table (6) reports the descriptive statistics for Resilient Technology Strategies (RTS). The composite mean was high (M = 4.43, SD = 0.48), showing strong agreement that RTS practices matter for keeping software development going under crisis conditions in the Gaza Strip. Q2.2, on using external cloud server systems to support fast remote operations, had the highest rating (M = 4.78, SD = 0.49). Next came Q2.4, on how remote operations protect staff, for example by reducing the risks of moving around (M = 4.69, SD = 0.53), and Q2.1, on distributing tasks during displacement (M = 4.56, SD = 0.61). Respondents also agreed on the value of operational flexibility during power and internet outages (Q3.3, M = 4.48, SD = 0.64) and on cloud computing reducing their dependence on local servers (Q3.4, M = 4.39, SD = 0.72). Lightweight development (Q4.6, M = 4.25, SD = 0.69) and remote agile management (Q2.6, M = 4.19, SD = 0.76) were also positively rated. Although green computing had the lowest mean (Q3.6, M = 4.11, SD = 0.83), the findings still demonstrate that energy efficiency practices are regarded as key to sustaining technological resilience across crises.

Table (6): Resilient Technology Strategies (RTS)

Item Code	Core Item Concept / Statement	Mean (M)	Standard Deviation (SD)	Ranking
Q2.2	Cloud servers facilitated rapid remote operations.	4.78	0.49	1
Q2.4	Remote operations improved staff safety.	4.69	0.53	2
Q2.1	Remote operations enabled task distribution during displacement.	4.56	0.61	3

Item Code	Core Item Concept / Statement	Mean (M)	Standard Deviation (SD)	Ranking
Q3.3	Remote operations enabled flexible work despite power and internet constraints.	4.48	0.64	4
Q3.4	Green cloud computing reduced dependence on local servers and power consumption.	4.39	0.72	5
Q4.6	Lightweight development practices improved efficiency during the crisis.	4.25	0.69	6
Q2.6	Remote Agile practices supported project rescheduling.	4.19	0.76	7
Q3.6	Green computing became essential for sector continuity.	4.11	0.83	8
Composite	(Overall Construct)	4.43	0.48	—

Operational Continuity

The results reveal that software firms maintain a high level of continuity of operations and systemic resilience in a crisis context. The highest-rated item was Q1.1, indicating that software firms were able to resume operations after the initial phase of disruption (M = 4.81, SD = 0.43). The next was Q4.2, indicating that software development persisted, even after a persistent power outage, but with increased task completion time (M = 4.73, SD = 0.51), signifying the capacity of firms to operate during severe infrastructure-related bottlenecks. Additionally, Q4.5, which measures the capability of remotely developed software to sustain the desired performance and technical standards under displacement or crisis conditions, was scored as high on average (M = 4.34, SD = 0.76). Q4.3 earned the lowest score—low-cost cloud solutions helped to control development budgets (M = 3.89, SD = 0.82). Overall, software firms demonstrated strong operational resilience through their ability to resume activities, maintain software quality, and continue development despite crisis-induced disruptions.

Table (7): Operational Continuity

Item Code	Core Item Concept / Statement	Mean (M)	Standard Deviation (SD)	Ranking
Q1.1	Companies resumed operations after initial disruption.	4.81	0.43	1
Q4.2	Software development continued despite power outages.	4.73	0.51	2
Q4.5	Remotely developed software maintained required standards.	4.34	0.76	3
Q4.3	Low-cost cloud solutions helped control budgets.	3.89	0.82	4
Composite	Operational Continuity (Overall Construct)	4.44	0.52	—

Correlation Analysis

The relationships between the study variables were examined through Pearson correlation. All the dimensions showed positive relationships with one another. The correlation between SIIDR and RTS was strong ($r = 0.641$, $p < 0.01$), and between SIIDR and operational continuity it was $r = 0.553$, $p < 0.01$. RTS and operational continuity correlated at $r = 0.594$, $p < 0.01$, pointing to the role RTS play in sustaining software development during a crisis. H1 is therefore supported.

Table (8): Correlation Matrix of Study Variables

Variables	1	2	3
Siege-Induced Infrastructure Disruption and Risks (SIIDR)	1	—	—
Resilient Technology Strategies (RTS)	0.641**	1	—
Operational Continuity	0.553**	0.594**	1

Variables	1	2	3
**. Correlation is significant at the 0.01 level (2-tailed).			

Confirmatory Factor Analysis (CFA)

Confirmatory factor analysis (CFA) was conducted to evaluate the adequacy of the refined measurement model after the preliminary item-purification stage. The CFA assessed whether the retained indicators adequately represented the three latent constructs: SIIDR, RTS, and operational continuity. The evaluation covered model fit, reliability, convergent validity, and discriminant validity.

Model Fit Indices

Table (9) indicate good overall fit. CMIN/DF is 1.428, which is excellent, while CFI (0.948) and TLI (0.941) lie in the acceptable-to-good range. With RMSEA at 0.054, under the 0.06 threshold, the measurement model was judged adequate for the structural equation modeling stage.

Table (9): Model Fit Indices for the Measurement Model

Fit Index	Value	Recommended Threshold	Result
CMIN/DF	1.428	≤3.00 (Excellent); ≤5.00 (Acceptable)	Excellent Fit
CFI (Comparative Fit Index)	0.948	≥0.90 (Good) ; ≥0.95 (Excellent)	Good Fit
TLI (Tucker-Lewis Index)	0.941	≥0.90 (Good); ≥0.95 (Excellent)	Good Fit
RMSEA (Root Mean Square Error)	0.054	≤0.06 (Excellent); ≤0.08 (Good)	Good Fit

Common Method Bias (Harman's Single Factor Test)

Harman's single-factor test was used to check for common method bias, that is, whether one factor accounts for most of the variance among the measured variables. Table (10) shows three factors with eigenvalues above 1. The first explained 34.230% of the total variance, under the commonly used 50% threshold. Common method bias is therefore unlikely to be a major concern here.

Table (10): Harman's single-factor test

Factor	Total	% of Variance	Cumulative %
1	6.846	34.230%	34.230%
2	2.115	10.575%	44.805%
3	1.638	8.190%	52.995%

Discriminant Validity (Fornell-Larcker Criterion)

Table (11) reports the Fornell-Larcker criterion. The square root of each construct's AVE exceeded its correlations with the other constructs: SIIDR (0.718), RTS (0.732), and operational continuity (0.715). The constructs are therefore empirically distinct, and discriminant validity was established for the measurement model.

Table (11): Discriminant Validity Results

Construct	1	2	3
Siege-Induced Infrastructure Disruption and Risks (SIIDR)	0.718	—	—
Resilient Technology Strategies (RTS)	0.641	0.732	—
Operational Continuity	0.553	0.594	0.715

Convergent Validity and Reliability

Reliability and validity results for the constructs appear in Table (12). Cronbach's alpha was used to evaluate reliability, while composite reliability (CR) and average variance extracted

(AVE) were used to evaluate both convergent validity and reliability. All constructs meet the criteria for convergent validity and reliability. Cronbach's alpha ranges from 0.794 to 0.871, composite reliability from 0.807 to 0.884, and every AVE is above 0.50. On these data the measurement model is reliable, shows adequate convergent validity, and is suitable for structural equation modeling.

Table (12): Convergent Validity and Reliability

Construct	Cronbach's α	Composite Reliability (CR)	Average Variance Extracted (AVE)
Siege-Induced Infrastructure Disruption and Risks (SIIDR)	0.842	0.851	0.516
Resilient Technology Strategies (RTS)	0.871	0.884	0.536
Operational Continuity	0.794	0.807	0.511

Structural Equation Modeling (SEM) and Hypotheses Testing

The structural model was evaluated to examine the direct and indirect relationships among Siege-Induced Infrastructure Disruption and Risks (SIIDR), Resilient Technology Strategies (RTS), and operational continuity.

Analysis of Direct Effects

Table (13) shows that H2 was not supported in its hypothesized direction, whereas H3 and H4 were supported. H2 predicted a negative effect of SIIDR on operational continuity, yet the estimate was positive and significant ($B = 0.329$, $\beta = 0.292$, C.R. = 3.061, $p = 0.003$). For H3, SIIDR significantly and positively affected RTS ($B = 0.628$, $\beta = 0.641$, C.R. = 8.831, $p < 0.001$): firms facing greater disruption were more likely to adopt RTS. For H4, RTS had a positive and significant effect on operational continuity ($B = 0.467$, $\beta = 0.407$, C.R. = 4.260, $p < 0.001$), which indicates that RTS improve operational continuity in a crisis. Firms that were hit harder by disruption therefore relied more heavily on technological adaptation, and these strategies helped them keep operating.

Table (13): Summary of Structural Model Results (Direct Effects)

Hypothesis	Structural Path	Unstandardized Coefficient (B)	Standardized Beta (β)	S.E.	C.R. (t-value)	p-value	Result Evaluation
H2	SIIDR → Operational Continuity	0.329	0.292	0.107	3.061	0.003	Not supported (significant effect in the opposite direction)
H3	SIIDR → RTS	0.628	0.641	0.071	8.831	p < 0.001	Supported (Positive)
H4	RTS→ Operational Continuity	0.467	0.407	0.110	4.260	p < 0.001	Supported (Positive)

Mediation Analysis (Indirect Effects)

Mediation was assessed following Baron and Kenny (1986), with bootstrapping used to test the significance of the indirect effect. SIIDR significantly and positively predicted RTS ($\beta = 0.641$, $p < 0.001$) and also had a significant positive direct effect on operational continuity ($\beta = 0.292$, $p = 0.003$). With SIIDR controlled, RTS still had a significant positive effect on operational continuity ($\beta = 0.407$, $p < 0.001$). Bootstrapping confirmed a significant positive indirect effect of SIIDR on operational continuity through RTS ($\beta = 0.261$, $p < 0.001$, 95% CI [0.127, 0.395]). The direct and indirect effects were both significant and shared the same sign, which is the

pattern of complementary partial mediation: RTS partly mediate the relationship between SIIDR and operational continuity.

Table (14): Mediation Analysis Results

Effect Type	Structural Path	Standardized Coefficient (β)	C.R. / t-value	p-value	95% Bootstrap Confidence Interval	Result
Path a	SIIDR → RTS	0.641	8.831	<0.001	[0.498, 0.784]	Supported
Path c (Direct Effect)	SIIDR → Operational Continuity	0.292	3.061	0.003	[0.104, 0.480]	Significant (Positive)
Path b	RTS → Operational Continuity (controlling for SIIDR)	0.407	4.260	<0.001	[0.219, 0.595]	Supported
Indirect Effect (a×b)	SIIDR → RTS → Operational Continuity	0.261	3.824	<0.001	[0.127, 0.395]	Supported (Complementary Partial Mediation)

Explained Variance (R^2)

Table (15) shows that the model explains 41.1% of the variance in RTS ($R^2 = 0.411$) and 40.3% of the variance in operational continuity ($R^2 = 0.403$). SIIDR thus accounts for part of how firms adapt technologically, and SIIDR and RTS together account for part of the variation in operational continuity under severe conflict conditions.

Table (15): Squared Multiple Correlations (R^2)

Endogenous Construct	*R^2 Value*	*Variance Explained (%)*	*Predictive Power Level*
Resilient Technology Strategies (RTS)	0.411	41.1%	Moderate
Operational Continuity	0.403	40.3%	Moderate

The final structural equation model in Figure (1) illustrates the relationships among SIIDR, RTS, and operational continuity.

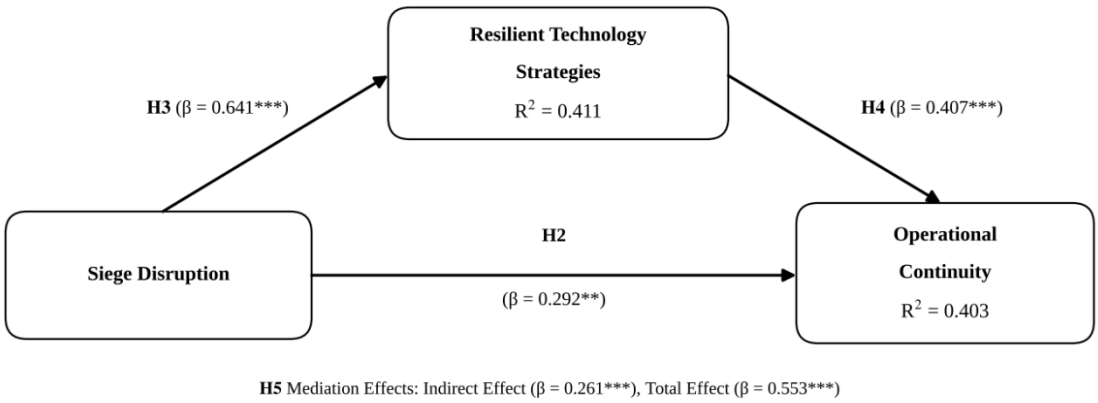


Figure (1): Final structural model with standardized path coefficients

Discussion

The results show that software development professionals in the Gaza Strip face severe infrastructure disruption and, alongside it, show considerable adaptive capacity through digital transformation strategies. Respondents agreed strongly both on how severe the disruption caused by the siege has been and on the vital role technology plays in keeping operations going.

The greatest constraints on software development activities within the region stem from infrastructure disruption. Both the destruction of electricity and internet networks and the loss of physical office space and local servers have resulted in very high levels of instability and uncertainty in terms of operational expenses, increased potential for data loss, and significant delays in delivering new software applications. In addition, organizations experience additional economic and organizational pressures that necessitate the allocation of additional resources for alternative energy and communications solutions as a result of infrastructure destruction. These findings provide further support for the notion that the collapse of infrastructure in conflict zones has an impact on multiple levels, including impacts on the cost structure of an organization, the productivity of an organization, and the reliability of the systems of an organization. The results indicate that remote operations and cloud-based infrastructure are critical means that enable organizations to maintain operations.

The adoption of distributed development environments and cloud infrastructures indicates that software organizations are redefining operational resilience through digital architectures rather than dependence on physical co-located workplaces (Hollnagel et al., 2006). These findings suggest that remote operation is more than a short-term crisis response. It has become part of the basic operational frameworks that keep software production going during a crisis. In the same way, because organizations face serious energy limits, resource optimization and green computing practices are becoming the main drivers of efficiency. This move from sustainability-oriented computing toward optimizing resources out of need can be described as necessity-driven resource optimization. The results also suggest that energy efficiency should be treated as a necessary operational task, and not as an individual decision made mainly for environmental reasons.

The correlation analysis shows significant relationships among the study constructs. Siege impacts, resilient technologies, and operational continuity are strongly correlated with one another, which suggests that the constructs are coherent and linked within the crisis-response context. The strong correlation between RTS and operational continuity means that technology-based adaptation practices go hand in hand with keeping operations running during a crisis. The correlation and SEM results point to a similar structural relationship among the study variables: infrastructure disruption drives the adoption of Resilient Technology Strategies, and these strategies are associated with operational continuity.

This pattern shows that technological adaptation is one of the main ways software organizations build resilience (Sutcliffe & Vogus, 2003). Moreover, infrastructure disruption is positively related to operational continuity both directly and through RTS, which partially mediates the relationship (complementary partial mediation). The positive direct effect runs against H2, which predicted a negative effect. A possible explanation is that firms hit hardest by infrastructure disruption also mobilize alternative continuity arrangements most intensively, an interpretation that future research should test. The findings therefore indicate that the resilience of the software industry in Gaza is shaped by the intensity of the crisis, because firms respond with adaptive strategies of digital transformation. RTS serve as a mediator, giving organizations a way to handle the adverse consequences of environmental shocks. The findings contribute to the literature on software engineering resilience and on SME survival in times of crisis.

Previous studies, including Ekwere (2016), considered small- and medium-sized enterprises to be structurally weak with regard to coping with catastrophic shocks, whereas the evidence from

the Gaza Strip suggests a more complex pattern. Software companies in this category have developed adaptive capabilities through their fast-paced digital transitions, including cloud migration, remote work coordination, and energy-efficient computers. This is indicative of a shift away from the traditional survival models toward the frameworks of digitally mediated resilience. Additionally, this evidence builds upon previous research on agile adaptations in the Gaza context (Yousef, 2022). It provides additional support that the agility of organizations in this region is no longer only methodological flexibility but rather fully distributed operational ecosystems. In this context, agile practices are not limited to internal organizational processes; they are integrated into the cloud-based infrastructures and decentralized work environments that allow organizations to operate during a significant disruption to the physical and technological infrastructure.

The study concludes that crisis conditions serve as disruptive forces for rapid technological change and digital transformation. The integration of remote operations and green computing practices within RTS forms a resilience strategy that enables software organizations to sustain functionality, reduce vulnerability, and maintain continuity in one of the most extreme operating environments.

Implications

The findings of this study offer important theoretical, practical, and policy implications for understanding software development resilience in conflict-affected and infrastructure-constrained environments.

Theoretical Implications

This study extends the literature on software engineering, crisis management, and resilience frameworks by proposing a composite framework that integrates Siege-Induced Infrastructure Disruption and Risks (SIIDR), remote operations, green computing, and operational continuity. Unlike existing models that examine risk management, technology adoption, and sustainability as separate domains, this study proposes a resilience-oriented perspective in which infrastructure shocks affect operational continuity through technological adaptation mechanisms. The study therefore adds to the literature on SME survival (Ekwere, 2016). Its findings suggest that under extreme crisis conditions, operational continuity is not determined solely by managerial effectiveness or financial resources and capabilities; it depends more and more on digital adaptability and distributed technological infrastructures.

Practical Implications

On the technical side, the results show that software firms working under severe instability need to build and strengthen digital resilience capabilities. For firms trying to keep operating through severe infrastructure disruption, remote operations, cloud-based development environments, and lightweight computing practices are increasingly essential, not optional. Software companies in similar crisis-affected contexts should therefore consider the following strategic actions:

- Adopting distributed cloud infrastructure so that data stay available and development processes continue
- Setting up remote collaboration so teams can keep working together despite mobility and security constraints
- Using energy-efficient computing practices to depend less on unstable electricity sources

- Applying agile, flexible project governance that can adapt to sudden and unpredictable developments

Together, these strategies enable software companies to maintain productivity even in environments severely constrained by crisis conditions.

Policy Implications

At the policy level, the study points to the need to fund digital resilience infrastructure in conflict-affected areas. Policymakers, NGOs, and international development agencies should give priority to funding initiatives that develop:

- Reliable, decentralized internet infrastructure (e.g., satellite internet).
- Renewable and alternative energy systems such as solar microgrids.
- Cloud access programs and digital transformation support for small and medium-sized enterprises.
- Capacity building in remote software development and cybersecurity.

These interventions can make ICT infrastructure more viable and help it keep supporting economic recovery or survival after the crisis.

Future Research

In the future, longitudinal research on digital resilience strategies across time and comparisons of areas affected by conflict or disasters are required. Qualitative research could also examine what software professionals went through during this period of extraordinary infrastructure breakdown, particularly their psychological stress, productivity problems, and creative efforts.

Limitations of the Study

The present study has several limitations that should be taken into account when interpreting the results. Due to crisis conditions, non-probability sampling was employed, and it was not possible to identify the exact population of software development professionals working in Gaza. Although the sample size of 150 met SEM-based requirements, conclusions should be drawn with caution. In addition, the study was conducted under extremely constrained operational conditions, which could have affected participants' perceptions and reported experiences. The cross-sectional nature of the design also precludes the investigation of whether resilience strategies change over time. Although RTS significantly mediated the relationship between infrastructure disruption and operational continuity, they cannot replace the physical infrastructure that was lost. Future research should employ longitudinal and qualitative studies that examine how digital resilience evolves and the human and organizational factors affecting software professionals during prolonged crises.

Conclusion

This paper investigated the impact of Siege-Induced Infrastructure Disruption and Risks (SIIDR) on the software industry in the Gaza Strip and the contributions of remote operations and green computing to maintaining operational continuity under crisis conditions. The results show that infrastructure disruption has a significant impact on software development by raising operating costs, decreasing productivity, interrupting communication, and increasing the risk of data loss. Yet these limitations are a source of impetus for the rapid technology adaptation, as opposed to the cessation of software development activities. Results reveal a growing reliance on robust technology practices such as remote work, cloud-based development

environments, lightweight systems, and energy-efficient computing measures to maintain operations during significant environmental destabilization.

The structural model also indicates that infrastructure disruption promotes the adoption of Resilient Technology Strategies that significantly contribute to enhancing operational continuity. This suggests a resilience pathway in which Resilient Technology Strategies (RTS) mediate the relationship between infrastructure disruption and operational continuity.

On a theoretical level, this research contributes to the literature by integrating risk management, remote operations, and green computing within a single resilience framework for software engineering in conflict-affected regions. It also disrupts conventional assumptions about the vulnerability of SMEs by showing that software companies can sustain operations via digitally enabled and distributed infrastructures.

In practice, the results underscore the significance of cloud computing, distributed development platforms, green computing practices, and flexible working schemes as crucial survival strategies in highly unstable environments. These measures should also be viewed as critical continuity mechanisms that enable, rather than hinder, organizational survival during times of crisis.

References

1. Abuawad, A., Griffiths, M., Edwards, G. H., Eftekhari, A., Al-Ebweini, M., Al-Najar, H., Butmeh, A., Abu Dayyeh, R., El-Shewy, M., & Aker, A. (2025). The ongoing environmental destruction and degradation of Gaza: The resulting public health crisis. *American Journal of Public Health, 115*(7), 1053–1061. https://doi.org/10.2105/AJPH.2025.308140
2. Anser, M. K., Ahmad, M., Khan, M. A., Zaman, K., Nassani, A. A., Askar, S. E., Abro, M. M. Q., & Kabbani, A. (2021). The role of information and communication technologies in mitigating carbon emissions: Evidence from panel quantile regression. *Environmental Science and Pollution Research, 28*(17), 21065–21084. https://doi.org/10.1007/s11356-020-12114-y
3. Aregbesola, G. D., Asghar, I., Akbar, S., & Ullah, R. (2025). Fuzzy logic model for informed decision-making in risk assessment during software design. *Systems, 13*(9), 825. https://doi.org/10.3390/systems13090825
4. Arnuphaptrairong, T. (2011). Top ten lists of software project risks: Evidence from the literature survey. In *Proceedings of the International MultiConference of Engineers and Computer Scientists* (Vol. 1, pp. 16–18). Hong Kong.
5. Atadoga, A., Umoga, U. J., Lottu, O. A., & Sodiya, E. O. (2024). Advancing green computing: Practices, strategies, and impact in modern software development for environmental sustainability. *World Journal of Advanced Engineering Technology and Sciences, 11*(1), 220–230. https://doi.org/10.30574/wjaets.2024.11.1.0052
6. Awwad, L. S., & Awwad, B. (2026). Digital empowerment and remote work in Palestine: Towards an economic sustainability strategy through digital transformation. In B. Awwad & R. A. Awwad (Eds.), *Technology and Innovation Towards a Future of Business Sustainability* (pp. 219–227). Springer. https://doi.org/10.1007/978-981-95-6469-9_17
7. Baek, J. S., Meroni, A., & Manzini, E. (2015). A socio-technical approach to design for community resilience: A framework for analysis and design goal forming. *Design Studies, 40*, 60–84. https://doi.org/10.1016/j.destud.2015.06.004
8. Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations.

Journal of Personality and Social Psychology, 51(6), 1173–1182. https://doi.org/10.1037/0022-3514.51.6.1173

9. Devineni, S., & Gorantla, B. (2023). Energy-efficient computing and green computing techniques. *Computer Science, Engineering and Technology, 1*(4), 37–45. https://doi.org/10.46632/cset/1/4/5
10. Dey, P. K., Kinch, J., & Ogunlana, S. O. (2007). Managing risk in software development projects: A case study. *Industrial Management & Data Systems, 107*(2), 284–303. https://doi.org/10.1108/02635570710723859
11. Ekwere, N. (2016). Framework of effective risk management in small and medium enterprises (SMEs): A literature review. *Bina Ekonomi, 20*(1), 23–46. https://doi.org/10.26593/be.v20i1.1894.23-46
12. Emanuel, N., & Harrington, E. (2024). Working remotely? Selection, treatment, and the market for Remote Work. *American Economic Journal: Applied Economics, 16*(4), 528–559. https://doi.org/10.1257/app.20230376
13. Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Ashgate Publishing, Ltd.
14. Jeyamurugan, A., Vijayan, S. B., Adaikkammai, A., & Yamini, B. (2025). *Green computing and big data analytics: Towards sustainable and eco-efficient systems*. Paper presented at the 2025 5th International Conference on Evolutionary Computing and Mobile Sustainable Networks (ICECMSN). https://doi.org/10.1109/ICECMSN68058.2025.11382742
15. Kollab, W. M., & Yousef, Y. A. (2023). Exploring the relationship between green IT awareness and adoption: A case study of IT students in the Gaza Strip. *Jurnal Sistem Informasi, 19*(2), 61–78. https://doi.org/10.21609/jsi.v19i2.1338
16. MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological Methods, 1*(2), 130–149. https://doi.org/10.1037/1082-989X.1.2.130
17. McPhail, R., Chan, X. W., May, R., & Wilkinson, A. (2024). Post-COVID remote working and its impact on people, productivity, and the planet: An exploratory scoping review. *The International Journal of Human Resource Management, 35*(1), 154–182. https://doi.org/10.1080/09585192.2023.2221385
18. Okolie, U. C., & Egbon, T. N. (2025). Adoption of remote work in the Nigerian public sector: Challenges and opportunities in Delta State. *BIMA Journal (Business, Management, & Accounting Journal), 6*(2), 1563–1578. https://doi.org/10.37638/bima.6.2.1563-1578
19. Palestinian Central Bureau of Statistics (PCBS). (2024). *Impact of the Israeli aggression on the Gaza Strip*. PCBS. http://www.pcbs.gov.ps
20. Paul, S. G., Saha, A., Arefin, M. S., Bhuiyan, T., Biswas, A. A., Reza, A. W., Alotaibi, N. M., Alyami, S. A., & Moni, M. A. (2023). A comprehensive review of green computing: Past, present, and future research. *IEEE Access, 11*, 87445–87494. https://doi.org/10.1109/ACCESS.2023.3304332
21. Pilliang, M., & Munawar, M. (2022). Risk management in software development projects: A systematic literature review. *Khazanah Informatika: Jurnal Ilmu Komputer dan Informatika, 8*(2), 133–144. https://doi.org/10.23917/khif.v8i2.17488
22. Radu, L.-D. (2017). Green cloud computing: A literature survey. *Symmetry, 9*(12), 295. https://doi.org/10.3390/sym9120295
23. Sanmocte, E. M. T., & Costales, J. A. (2025). Exploring effectiveness in software development: A comparative review of system analysis and design methodologies. *International Journal of Computer Theory and Engineering, 17*(1), 1–8.

24. Sutcliffe, K. M., & Vogus, T. J. (2003). Organizing for resilience. In K. S. Cameron, J. E. Dutton, & R. E. Quinn (Eds.), *Positive organizational scholarship* (pp. 94–110). Berrett-Koehler.
25. The World Bank, United Nations, & European Union. (2024). *Gaza Strip interim damage assessment: Summary note*. World Bank Group. https://documents.worldbank.org
26. Tucnik, P., Otcenaskova, T., & Horalek, J. (2023). Project and risk management in the context of IT projects. In *Proceedings of the International Scientific Conference Hradec Economic Days* (pp. 71–80). https://doi.org/10.36689/uhk/hed/2023-01-071
27. Wu, Y., & Tham, J. (2023). The impact of environmental regulation, Environment, Social and Government Performance, and technological innovation on enterprise resilience under a green recovery. *Heliyon, 9*(10), e20278. https://doi.org/10.1016/j.heliyon.2023.e20278
28. Younis, S., & Tunç, G. (2023). Investigation of electricity distribution, shortages in the Gaza Strip, and the role of renewable energy technologies for addressing the electricity crisis. *International Journal of Energy Studies, 8*(3), 557–579. https://doi.org/10.58559/ijes.1317267
29. Yousef, Y. A. (2022). Investigating the role of critical success factors in achieving the success of agile projects in the Gaza Strip. *Journal of Computing and Information Technology, 30*(2), 117–137. https://doi.org/10.20532/cit.2022.1005498
30. Zhang, M., Antwi-Afari, M. F., Wang, C., Sun, W., Mohandes, S. R., & Abdulai, S. F. (2025). Uncertainty in software development projects: A review of causes, types, challenges, and future research directions. *Systems, 13*(8), 650. https://doi.org/10.3390/systems13080650

Appendix A.

Digital Resilience of Software Development under Crisis

Instructions to Respondents

Please read the following statements carefully and indicate the extent to which you agree or disagree with each statement. Your responses will be used for scientific research purposes only and will be treated with strict confidentiality.

There are no right or wrong answers.

Section A: Demographic Information

Please tick (✓) the option that best describes you.

All information is confidential and used for research purposes only.

Gender ☐ Male ☐ Female

Current Job Nature ☐ Project Manager / Business Owner ☐ Programmer / Software Developer ☐ Software Quality Assurance (QA) Engineer ☐ UI/UX Designer

Educational Level ☐ Diploma or below ☐ Bachelor's degree ☐ Master's degree ☐ PhD degree ☐ Other (please specify):

Years of Work Experience ☐ Less than 5 years ☐ 5–9 years ☐ 10–14 years ☐ 15–19 years ☐ 20 years or more

Primary place of work and operation during the current crisis (after October 7)

☐ From within a tent or displacement/shelter center, working individually

☐ From a shared workspace or temporary café relying on alternative energy sources

☐ Remotely from outside the Gaza Strip (after external displacement).

☐ From the company premises (partially operational or reactivated with alternative energy sources).

Average daily available technical working hours during the crisis

☐ Fewer than 3 hours ☐ From 3 to 6 hours ☐ More than 6 hours

Primary energy source currently used to power your digital devices

☐ Commercial / local electric generators

☐ Solar power system (private or shared)

☐ Rechargeable batteries and small energy storage units (power banks)

☐ Private solar power system + commercial generators

The following statements are measured using a 5-point Likert scale:

Statement	**1**	**2**	**3**	**4**	**5**
Section B: Siege-Induced Infrastructure Disruption and Risks (SIIDR)					
Q1.1 Software companies were able to resume their operations after an initial period of disruption following the onset of the crisis.					
Q1.2 Destruction of offices and local servers increased data loss risk					
Q1.3 Searching for alternative energy and communication sources increased software production time.					
Q1.4 Companies incurred additional costs to secure alternative energy and internet solutions.					
Q1.5 Project delays increased the risk of contract termination or penalties.					
Q1.6 Power and communication outages negatively affected software quality and testing.					
Section C: Remote Operations and Cloud Adaptation					
Q2.1 Remote operations platforms enabled task distribution despite displacement.					
Q2.2 External cloud servers supported a rapid shift to remote operations.					
Q2.3 Remote operations provided developers with high flexibility to complete their tasks during periods when electricity and alternative internet access were available, whether during the day or at night.					
Q2.4 Remote operations enhanced staff safety by reducing movement risks.					
Q2.5 Remote operations faced cybersecurity and data protection challenges when connecting through unsecured local internet networks in displacement centers.					
Q2.6 Remote Agile management facilitated rescheduling of project delivery.					
Section D: Green Computing and Resource Optimization					
Q3.1 Infrastructure disruptions and power interruptions increased reliance on low-power devices to sustain software development activities under crisis conditions.					
Q3.2 Infrastructure constraints compelled software teams to use lightweight, less CPU-intensive environments due to limited computing resources.					
Q3.3 Remote operations provided flexible task completion based on available power and internet access.					
Q3.4 Cloud computing reduced the need for local servers and continuous power consumption.					

Statement	1	2	3	4	5
Q3.5 The lack of spare parts and new equipment due to the blockade and war has increased reliance on maintaining and extending the life of existing devices.					
Q3.6 Green computing has become a necessity for the survival and continuity of the technology sector in Gaza.					
Section E: Operational Continuity					
Q4.1 Remote work mechanisms enabled us to meet software project delivery deadlines for external clients despite the conditions of war.					
Q4.2 Software development continued despite frequent power outages, albeit with increased task completion time.					
Q4.3 Low-cost cloud solutions helped control development budgets.					
Q4.4 Overall software production costs increased due to additional energy and connectivity expenses.					
Q4.5 Despite displacement and crisis conditions, remotely developed software maintained required performance and technical standards.					
Q4.6 Lightweight development practices improved software efficiency during the crisis.					