Building Digital Resilience in Major Shocks: How Ukrainian Organizations Enact Digital Transformation in Times of War

Nataliya Berbyuk Lindström
University of Gothenburg
Sweden
nataliya.berbyuk.lindstrom@ait.gu.se

Liana Razmerita
Copenhagen Business School
Denmark
lra.msc@cbs.dk

Serhii Prokopenko
Simon Kuznets National University of Economics
Ukraine
prokopenko.serhii@gmail.com

Nataliya Popovich
One Philosophy
Ukraine
np@one-philosophy.com

Abstract

Limited IS research is available on digital transformation (DT) and digital resilience in major shocks. Drawing on Boh et al. (2023) digital resilience framework and using the case of Ukrainian organizations operating during the war, we explore how DT is enacted to build digital resilience. Analysis of 40 interviews with the Ukrainian managers shows that DT unfolds emergently to ensure organizational survival, involving the integration of social media and messaging in work practices to ensure continuous contact, morale support, and decision-making. Re-adapting remote work practices from the pandemic, handling infrastructure damages, enhancing cybersecurity protection, and developing new online services to reach out to customers are key strategies that contributed to building digital resilience. Further, volunteering and donating to the army contribute to community feelings, pivotal for building resilience in war. The study provides suggestions for extending the digital resilience framework and offers insights for managing organizations in times of major shocks.

Keywords: crisis-driven digital transformation, digital resilience, war, Ukraine.

1. Introduction

Major shocks such as disasters and crises have always been inevitable, causing widespread destruction, displacement, and loss of life. Emerging unexpectedly, they threaten an organization's priorities, restrict the time available to respond to the events unfolding, and result in greater stress on managers and their employees (Di Gangi et al., 2022). At the same time, crises are catalysts for enhancing adaptability and resilience, offering us opportunities for learning, innovation, and growth (Duchek, 2020; Magutshwa et al., 2022). While the recent COVID-19 pandemic has had a significant and wide-ranging impact on businesses across various sectors, causing enormous disruptions in supply chains and financial challenges, the pandemic also forced organizations to make digitalization a strategic focus, resulting in a tremendous acceleration of digital transformation (DT) in terms of the explosion of remote work (Sundermeier, 2022), telemedicine and digital health services (Anthony Jnr, 2021), e-commerce (Han et al., 2022), and online education (Carugati et al., 2020) to mention a few. Crisis-driven DT presents an opening for organizations to expedite ongoing DT endeavors and reconsider previously held notions regarding the implementation of digital technologies, contributing to resilience in times of crisis (Boh et al., 2023; Di Gangi et al., 2022).

There is a plethora of studies on DT and resilience, especially in relation to the pandemic (see the recent MISQ special issue on digital resilience (Boh et al., 2023) and MISQ Executive Issue on Crisis-Driven DT (Di Gangi et al., 2022) for reviews). The research with a focus on the role of digital technologies in general, and DT in particular in other types of crises than COVID-19 is still in its infancy. As major shocks are inevitable, e.g., climate crisis is expected to bring more frequent and severe natural disasters (The Intergovernmental Panel on Climate Change (IPCC), 2022), urbanization can cause significant health and economic impacts

URI: https://hdl.handle.net/10125/107202
978-0-9981331-7-1

(World Health Organization (WHO), 2022), and growing political and economic tensions can lead to military conflicts and loss of life, poverty, and social unrest (United Nations (UN), 2022), learning about DT and how it can contribute to resilience in various crises is pivotal to be better prepared for future crises and to mitigate their impact.

At this moment, we are witnessing the Russo-Ukrainian War, one of the largest armed conflicts since World War II (Mankoff, 2022). Ukrainian organizations find themselves in a unique predicament, facing an unprecedented crisis due to military aggression and the aftermath of a global pandemic. Amidst these challenges, there is a silver lining in the form of widespread adoption of digital technologies and remote work practices. These advancements have become increasingly prevalent, enabling businesses to sustain their operations despite difficult circumstances. This was a scenario that would have posed significant challenges or even been deemed impossible until recently, before the COVID-19 pandemic. Ukrainian organizations continue to strive; reports indicate the remarkable resilience of Ukrainian organizations that manage to survive and even grow (Economist, 2022; Gorodnichenko et al., 2022), For instance, Ukrainian Railways — Ukrzaliznytsia — has been awarded European Rail Champion Award 2023 for remarkable resilience and continuation of transport services in war times (European Railway Award, 2023). The Ukrainian organizations offer an interesting case for IS research to explore in terms of DT and digital resilience perspectives in times of such a major shock as war, which to our knowledge has not been done before. To this end, we pose the following research question:

How is digital transformation enacted in organizations to build digital resilience during war?

We answer our research question by analyzing semi-structured interviews with managers from Ukrainian companies about their experiences of managing businesses during the first year of the war. Drawing on DT research and Boh et al. digital resilience framework (Boh et al., 2023), we investigate how managers enact crisis-driven DT to build organizational resilience, answering the calls from Di Gangi et al., 2022 and Boh et al., 2023 on further research on how grand challenges impact a company's efforts to operate and to survive in extreme crises.

2. Previous research and theoretical framework

Previous studies have emphasized the complexity and lack of a comprehensive understanding of DT and its implications (Matt et al., 2015; Vial, 2019). DT, "a change in how a firm employs digital technologies, to develop a new digital business model that helps to create and appropriate more value for the firm" (Verhoef et al., 2021)p. 1) implies a company-wide change that affects business logic and value creation beyond digitalization, triggering significant organizational improvements (Vial, 2019). DT is a dynamic journey, in which organizations not only merely adopt new tech tools but alter their operational methods to provide value to their customers (Westerman et al., 2014), encompassing cultural and organizational changes, employee engagement, leadership commitment, and a customer-centric mindset.

While extant literature has focused on DT as a challenging and time-consuming organizational change process loaded with tensions and resistance and consisting of certain stages (Baiyere et al., 2020; Vial, 2019), this study aims to contribute insights into crisis-driven DT which occurs as an accelerated change process, not following the traditional stages previously identified in DT. Often involving adopting agile methods, DT allows organizations to swiftly respond to changing situations, contributing to resilience (Baskerville & Pries-Heje, 2021). DT plays a crucial role in enhancing digital resilience, involving the implementation of strategies, technologies, and practices that enable organizations to withstand and quickly recover from disruptions while maintaining operational continuity (Oliveira, 2023).

In this paper, we adopt the definition of digital resilience as "the capabilities developed through the use of digital technologies to absorb major shocks, adapt to disruptions, and transform to a new stable state" (Boh et al., 2023, p.5). Based on IS resilience research in general, and the most recent research on digital resilience in times of COVID-19 in particular, Boh et al. (2023) present a theoretical framework for digital resilience research (Figure 1). This framework encompasses 'digital technology characteristics' and 'organizational conditions' for organizations to build resilience by 'absorbing', 'adapting', and 'transforming' in response to major shocks.

	RESILIENCE CAPABILITIES		
	Absorb	**Adapt**	**Transform**
Digital Technology Characteristics	• **Redundancy:** *Creating diversity of options for continuity.* • **Intelligent Sensing:** *Gathering and analyzing data to anticipate and withstand the shock*	• **Ubiquity and Accessibility:** *Responding quickly to disruptions* • **Experimentation:** *Engaging in rapid learning, development, and implementation*	• **Reconfigurability:** *Leveraging the modularity and recombinability of digital technologies* • **Scalability:** *Leveraging the power of digital platforms*
Conditions for Building Resilience	• **Coordination:** *Facilitating internal operations, identifying redundant (or slack) resources and supporting their swift utilization across a collective* • **Data Governance:** *Organizing structures for ensuring trust on the use of data between collaborating entities*	• **Organizational restructuring:** *Enacting organizational routines to leverage available technologies (e.g. move from offline to digital activities)* • **Adaptive culture and positive mindset:** *Being open and flexible to experimenting (and failing) with new ways of working*	• **Business model innovations:** *Assessing the impact of reconfigured technologies on existing and new business opportunities* • **Ecosystem strategies:** *Building multilateral complementarities that can enable scale and stronger resilience against future shocks*

Figure 1. Theoretical framework for digital resilience (Boh et al., 2023).

'Absorption' encompasses the ability of an entity to endure shocks while maintaining its original structure and functions intact (Martin & Sunley, 2015; Vogus & Sutcliffe, 2007), which involves minimizing the initial impact following a shock to ensure ongoing survival. Apart from absorbing, resilience also entails the capability to 'adapt' (Hollnagel & Woods, 2017), also referred to as 'rebounding' – to the previous or to a better state. Adaptation means responding to disruptions "through ubiquitous and accessible technologies, as well as by learning, developing, and implementing changes through experimentation" (Boh et al., 2023, p. 350). Finally, the 'transformation' capability "entails the development of new capabilities, changing organizational structures, or even new business models" (Boh et al., 2023, p. 352).

In the model, the characteristics and conditions are also additionally specified and illustrated, based on the research evidence, primarily from the pandemic. Further, the authors emphasize the complexity of how 'absorb', 'adapt', and 'transform' capabilities can be developed during and after the shock. They can be sequentially developed but even likely to overlap or even may be developed simultaneously. Further, these capabilities tend to overlap, jump, e.g., from 'absorb' to 'transform' or limit to only some capabilities, depending on the characteristics of digital technologies and organizational conditions for building digital resilience.

3. Participants and methods

We conducted 40 semi-structured interviews with managers from large and middle-sized Ukrainian companies within the financial, energy, retail, consultancy, IT, transport, medicine, pharmacy, media and communication, publishing, construction, agriculture, and food sectors. Our interview questions concerned four main areas: 1) Background (the company's mission and vision, the role of the respondent in the company, number of employees, and main activities); 2) Use of digital technologies in times of war and its impact on building organizational resilience; 3) Managerial and leadership responses at in response to the crises and additional comments (any other relevant information); 4) Additional comments (any other relevant information). Interviews were conducted between September 2022 - February 2023, via Zoom or MS Teams, and were recorded. The interview length varies between 45-70 minutes upon the interviewee's consent. The interviews were conducted in Ukrainian or Russian, transcribed verbatim, and translated into English.

Anonymity was emphasized, and the respondents could cancel their participation or change the interview time anytime. Due to air-raid alarms, disruptions were common. Another challenge was to ensure sufficient protection of data that contains many layers of sensitive personal information about vulnerable people and is by its very nature impossible to de-identify. This challenge was handled by meeting standard requirements from ethical review boards regarding the protected storage of sensitive raw data in a secure location. Access to this data is limited to authorized persons (Swedish Research Council (Vetenskapsrådet), 2003).

The interviews were transcribed verbatim, translated into English, and analyzed following Thematic Analysis (TA) principles (Braun & Clarke, 2012). In the analysis, the six-stage process of TA was followed such as (1) data familiarization; (2) coding; (3) searching for themes; (4) reviewing themes; (5) defining and naming themes; and (6) writing up. The familiarization process (1) was completed as follows. First, all authors read the transcripts several times to establish initial impressions. Second, the initial impressions were discussed, and then each author coded the transcripts independently (2). Third, the codes were discussed again to ensure consistency, refined, and sorted into categories (3). Next, the codes and categories were discussed, revised (4), and organized into overarching themes (5) to reflect DT in response to different crisis events. Finally, the identified themes were discussed through the theoretical lens of the digital resilience model (6) (Boh et al., 2023).

4. Results

Seven salient themes have been discerned in the analysis of interviews with the Ukrainian managers:

1. Pausing/interrupting organizational activities, and ensuring contact during relocations;
2. Implementing continuous communication for employee morale support;
3. Enhancing security and cyberattack prevention practices;
4. Re-adopting remote work practices from the pandemic;
5. Handling infrastructure damages and associated disruptions in work practices;
6. Supporting employees in engaging in volunteering;
7. Developing new services for reaching out to customers.

4.1. Pausing/interrupting organizational activities, and ensuring contact during relocations

The start of the war in February 2022 proved to be overwhelmingly disruptive, leading to pausing /interrupting organizational operations for three-four weeks for the majority of companies. The managers of the companies from the areas under attack mentioned being forced to prioritize saving the lives of their employees and their families by urgently organizing relocations to safer locations and keeping connections:

"The main thing was to stay [keep in touch] with each other. Communication was vital"(C21) for keeping track of relocations:

Regular online meetings became an indispensable part of daily activities for keeping in touch with employees. Some managers had to conduct frequent online meetings 24/7, also being constantly available online to answer any questions:

"In the first weeks, we met daily with the team because we wanted to be sure that everyone was alive and well since the situation was changing quickly" (C22).

The necessity of keeping continuous contact with employees in case of bombings, in the midst of chaos and panic, also resulted in an explosion in the use of social media and messengers, such as Telegram, Facebook, WhatsApp, and Viber:

"I communicated with the team on Telegram and recorded addresses daily. We started by creating a coordination chat where, during the first days, we gathered information about who was heading where and what people's plans were. After that, we agreed to always stay in touch" (C18).

The same message, especially if the important one, was sent via various channels to make sure that it would reach out to everyone:

"if someone did not see it on [Facebook], they saw the SMS or Viber. We were playing it safe so that we could always reach everyone" (C4).

The managers also mentioned allowing their employees to become more self-organized, and social media becoming a tool for supporting self-organizing and communicating swift decision-making:

"*The fact that the team is self-organized and there's no micromanagement or immersion in minutiae helped us a great deal. This high level of team freedom allowed everyone to act on what they understood and had the ability to do. Everything was decided on the fly, in messengers, and during calls without lengthy approvals because people took responsibility for their actions" (C3).*

Internal Telegram channels became especially popular, being used for continuous updates about the situation, and sharing work-related information.

4.2. Implementing continuous communication for employee morale support

In the initial stages of the war, many employees experienced extreme stress and fear. Many had to leave everything they owned behind, some lost relatives and friends in the hostilities. Enforced relocations also resulted in employees experiencing a lack of connection to their organizations, not being able to come to offices and meet their colleagues. In response, the managers implemented regular online meetings to encourage their employees, to talk about the situation with the company, listen to employees' concerns, and discuss the way forward.

One of the managers, inspired by President Volodymyr Zelenskyy's daily video addresses to the people of Ukraine, started recording his own videos and posting them daily in the internal Telegram group:

"The team must stay united, and so for the first six months of the full-scale war, I recorded a video message every morning to address the team. I modeled it after the president of Ukraine's addresses. I spoke to my team, and I believe that it was vital for them to hear their

director, understand what was happening, and see they weren't alone, they were supported, and no one was running away. It was also essential for me. These six months of my daily video addresses brought people closer together" (C22).

Further, when possible, some managers mentioned traveling to visit their employees:

"There are five people there, seven there, thirteen in L'viv, in Kyiv. We, the founders, have no restrictions on travel. I went to Poland and talked to the staff there. Another founder travels around Ukraine. We post a picture here and there [on social media], have dinner with someone, together - this adds a lot to kinship and provides some kind of emotional connection to our company" (C3).

Posting pictures and messages from these visits on their companies' internal channels and social media was considered important for supporting employees' feelings of connection to the company and showing managerial support. The managers also considered these physical meetings especially important for supporting the employees who experienced enforced relocations, lost their properties and family members, and felt lonely in the new places.

The respondents also encouraged their employees to communicate their experiences on internal channels, considering it to be a useful strategy for making people feel better. One of the examples was a digital project for sharing war experiences, in which the employees were asked to record and publish their stories from the first weeks of the war on the online platform:

"*Nearly the entire team remained in Kyiv, and new people subsequently joined in. We launched an extensive online project, 'Voices,' which documented the voices of courageous and resilient Ukrainians, artists, and musicians. We worked like that until early April 2022" (C29).*

4.3. Enhancing security and cyberattack prevention practices

The respondents, especially those working in telecom, media, and influential public organizations, mentioned cybersecurity risks becoming increasingly common during wartime. The respondent from a media company commented:

"The main thing is that Russia failed to deprive us of the Internet, even though they launched a DDoS attack on our website, making 200,000 requests per second. Once, they managed to shut down our website for five hours, but we restored everything, and they never succeeded again. We located their Telegram channel, which they use to coordinate their actions, so now we know about their plans to attack us" (C25).

Also, the manager from a human rights organization working on strategic cases related to war crimes and documentation of human rights violations noted an increased risk of data leakage, which put his employees at risk. He mentioned that they had to destroy the entire archive in the office and put enormous efforts into data protection. The danger of cyber-attacks was also common in public services such as mass online courses and product organizations. One of the respondents commented:

"we had to significantly increase the requirements for employees regarding information security, thinking of cyberattacks as the primary vector of Russian attacks. We prepared instructions and agreed on the plan in case of connection failure" (C38).

The respondents also commented on their companies paying more attention to security and configuration issues for laptops during the war, which became *"a more urgent issue compared to the pandemic due to cyber-attacks" (C9).*

The managers also emphasized the necessity of constantly backing up all data on EU servers rather than the national ones, informing employees about the potential risks:

"We wrote to our people in advance about what to do in the event of an invasion, recommended everyone to think of their own plan of action, and backed up all platform data in the cloud and on servers in the EU. We significantly increased the requirements for our employees regarding information security, thinking of cyberattacks as the primary vector of Russian attacks. We prepared instructions in case of connection failure" (C28).

Cyberattacks also pushed companies to take measures to prevent them by keeping track of potential attacks:

"We located their [the hackers] Telegram channel, which they use to coordinate their actions, so now we know about their plans to attack us" (C15).

4.4. Re-adopting remote work practices from the pandemic

The managers of the companies located in the areas under attack recognized their staff's inability to come to offices due to safety reasons/relocations/offices being destroyed or damaged. After the period of relocations, the managers re-introduced the remote work practices, adopted during the pandemic, which allowed their companies to rapidly get back on track:

"The experiences of the pandemic were important because back then, we developed the necessary infrastructure and learned how to work remotely. This experience enabled us to stabilize things quite quickly and nearly reach our pre-war work levels in two weeks after the full-scale invasion"(C24).

During the pandemic, many companies substituted desktop computers for laptops and switched to remote work for the companies not involved in manufacturing, e.g., IT companies, was relatively fast:

"Mostly everyone has laptops. It is not a problem for us to work from any corner of the world. The pandemic showed us that a physical office is not such an important part of work" (C1).

At the same time, the managers expressed concerns about the urgent need to handle inequalities among employees concerning access to digital technologies, Internet connection, and living and working conditions. The employees who were relocated outside Ukraine had more favorable conditions, compared to the ones staying in Ukraine. The managers had to handle these inequalities by offering additional support to some employees, e.g., buying Starlinks to ensure internet access and helping with finding accommodation. Further, for the companies involved in manufacturing, getting back on track was more complicated. Damage/destruction of offices and warehouses actualized the need to transport goods to alternative locations and sharing office costs was vital for survival.

Enormous stress caused by alarms, relocations, mobilizations, and loss of properties in combination with re-enforced remote work additionally deteriorated the psychological well-being of employees, already tired after the pandemic. The managers especially mentioned re-introducing online professional psychological support, adopted during the pandemic:

"We invited the psychologist and the psychotherapist who helped us during the COVID-19 period. We also organized psychological support for our employees, and about 300 people used it"(C26).

Unlike the pandemic times, when it was possible to come to the office, during the war, due to relocations, destructions, transportation problems, and safety issues, people could not come and sign the documents in the offices at all. The managers in all companies mentioned completely switching to digital signatures "*all documents are signed in a digital form, as we cannot meet" (C10),* primarily via the electronic ID and Diia (Action; Ukrainian: Дія, lit. 'Action').

4.5. Handling infrastructure damages and disruptions in work practices

Remote work was relatively unproblematic before early October 2022, when the missile strikes and drone attacks destroyed parts of Ukraine's energy infrastructure, causing power shortages and unstable Internet connection in the country. As frequent blackouts became common, access to the Internet and electricity, pivotal for remote work, could not be taken for granted. The managers had to buy Starlinks, generators, and organize co-working hubs in larger cities:

"We have offices in L'viv and Kyiv, where everything is provided. You can come to those places. There is a generator, and the Internet is stable - we provide all this" (C4).

According to the respondents, as co-working hubs were costly, collaborations among companies became necessary and increasingly common to survive:

"Someone rents an office, and we share these costs in proportion to the number of people who come there to work" (C3).

The new situation with infrastructure damages also additionally increased inequalities among the employees staying abroad, experiencing no changes in their work practices, and the employees staying in Ukraine. In smaller cities, co-working spaces were limited or even non-existent. The managers mentioned handling the challenges by implementing practices of recording work meetings and making them available on internal platforms for those employees who could not join the meeting to be able to access them at any time.

4.6. Supporting employees in engaging in volunteering

The managers reported noticing a strong need expressed by their employees to contribute to society, the army, and the shared goal - victory. Thus, in many

organizations, work practices were combined with online activism, volunteering, and providing support to the military. The managers mentioned initiating and supporting a number of online projects in relation to volunteering on companies' platforms to make it possible for people to combine remote working with contributing to the common good. Via internal platforms and Telegram channels, the employees could become involved in raising money for military uniforms, humanitarian aid, medical care, launching free training courses, etc.:

"Following a pressing request from our colleagues, we launched several volunteer projects on our internal platform [name of the platform]. By the end of 2022, the company managed to raise over 40 million UAH to support the Ukrainian defenders. And we have no intention of slowing down in our efforts to bring our victory closer" (C20).

The managers identified volunteering both as a human need for their employees and a contribution to the future of the country:

"Three weeks into the war and after meeting basic needs, our employees began using our internal platforms for fundraising and humanitarian initiatives. That's also a human need: feeling your involvement and being needed" (C15).

The respondents also emphasized the collaboration among different companies in relation to volunteering, offering support, and developing digital initiatives, e.g., companies jointly financing digital platforms for fundraising was mentioned:

"More than a thousand of our employees engaged in volunteer work. To increase the efficiency and guaranteed delivery of humanitarian aid directly to its recipients, a network of regional hubs was created, with a specially developed digital platform ensuring transparency of the processes. Nearly 800,000 people and 433 medical and social institutions in Ukraine received our assistance. Overall, the financial assessment of charitable contributions and humanitarian aid to the Common Help UA project is almost UAH 600 million. In addition, UAH 41 million has been directed to projects for the development of medium and small businesses, which will also be able to contribute to Ukraine's reconstruction in the future" (C26).

4.7. Developing new services for reaching out to customers

All managers mentioned some outflow of customers, which resulted in financial losses their companies had to handle. For instance, medical companies lost patients as many people relocated to other parts of the country or abroad, national contracts for IT companies were put on hold, publishing companies lacked access to storage facilities for printing materials due to relocations, etc., which spurred the development of digital services. For instance, the manager of a publishing house considered increasing the share of electronic books as a central strategy when paper deliveries were irregular and storage facilities were destroyed:

"Right now, we have to implement as many innovative solutions as possible, which in our case is connected to electronic books. This year, we observe essential growth in digital content, and we are sure this demand will continue in the years to come" (C14).

One of the medical companies invested in developing an online consultation platform to reach out to patients who relocated abroad:

"We're launching online consultations and subscriptions for patients living abroad. We received a request for this service from our customers [in Germany], who, being used to paying for and receiving services here and now, had to wait four months for a doctor's visit in Germany. But it's equally convenient for customers in Ukraine, for example, for follow-up consultations" (C31).

Another company introduced ambulances equipped with a laptop and Starlink connection for providing medical services to the civilians, volunteers, and the military in the localities under attack or in the liberated territories, suffering much infrastructure damage:

"We were faced with a catastrophic number of volunteer requests for antibiotics without a doctor's prescription. We didn't have to motivate our employees. Those working in hot spots receive extra pay, but they all simply understand the importance of doing their jobs for the settlements' residents and the military" (C19).

5. Discussion

The COVID-19 pandemic was a major crisis that accelerated the extensive DT across all sectors in just a few months, showing the pivotal role of digital technologies in building resilience and ensuring the

survival of organizations (Boh et al., 2023; Magutshwa et al., 2022), enabling an abrupt switch to remote work practices (Razmerita et al. 2021; Richter 2020). Research on the role of DT in building resilience in other types of crises than the pandemic is scarce (Berbyuk Lindström et al., 2023). In our study, we investigate how crisis-driven DT contributes to building digital resilience in times of war, using the case of Ukrainian organizations.

To start with, our study shows that DT unfolds emergently and quickly to ensure organizational survival.

In times of war, communication and focus on people, rather than profits, becomes pivotal to ensure that the employees are safe; employee retention is central for organizations to survive as people become mobilized, leave in different directions, or become relocated, get hurt, or killed. To address this challenge, many Ukrainian organizations paused their activities and swiftly integrated social media into their work practices to keep track of employee relocations during the first weeks of the war (Theme 1). In line with previous research on social media in crisis (Eismann et al., 2016; Rosenberg et al., 2018), our findings show that social media channels became indispensable for coordinating relocations and spreading internal information swiftly, communicating decisions, swift knowledge sharing and facilitating business value for efficient and transparent communication related to digital work processes (Kirchner & Razmerita, 2019). Social media also supports a more agile way of working and less managerial control, which the companies adopted during the war, contributing to resilience.

Turning to the digital resilience framework (Boh et al., 2023), while the model defines 'absorption' as the initial step in digital resilience, targeting the ability of an organization to endure shocks while maintaining its original structure and functions intact, our study shows that many Ukrainian organizations decided to pause/interrupt or 'freeze' their functions (Theme 1). To this end, we suggest complementing Boh et al. (2023)'s model by considering such capability as 'freezing' if facing such extreme crises as war, which entails pausing work activities, sacrificing contracts, customers, and profits for the sake of saving lives and retaining employees.

Second, our findings signal the central role of the preceding crisis, the COVID-19 pandemic, in building resilience in times of war (Berbyuk Lindström et al., 2023). The experiences from the extensive DT in terms of implementation of remote work in Ukraine during the pandemic became pivotal for meeting the challenges in times of war. Many companies simply re-adopted the remote work practices from the pandemic, which enabled them to get back on track fast, contributing to resilience (Theme 4). Thus, 'adapting' in the digital resilience framework, i.e., rebounding to the previous or to a better state, for the Ukrainian organizations did not entail, as the framework claims, "[using] ubiquitous and accessible technologies, as well as by learning, developing, and implementing changes through experimentation" (p. 350). Instead, our findings show the importance of considering the learnings from the previous crisis, in our case the remote work practices from the pandemic, for managing the next one.

Third, turning to employee well-being, the war additionally deteriorated the well-being of employees, which resulted in the implementation of different online support activities, such as professional psychological support, inspirational talks, and managers' talks (Theme 2 and 4). As we learned from the COVID-19 pandemic with regard to remote work, employee well-being is impacted negatively by enforced and lengthy remote work practices, abundant research emphasizing the importance of socializing and managerial support (Bowen & Pennaforte, 2017; Wang et al., 2021). In our study, the managers supporting volunteering on their companies' platforms for the employees to get involved in connection to their work to support their country also believe to contribute to employee well-being (Theme 6). While organizational resilience is dependent on employees' individual resilience (Duchek, 2020), our study also shows the importance of a collective, unity perspective on resilience in times of war, when people have a shared goal. Our findings also indicate the importance of responsive leadership and managerial support towards the employees in crisis (Oliveira, 2023).

Next, while the digital resilience model distinguishes 'adapting' and 'transforming' capabilities in response to major shocks, it is complicated to make this distinction in our data. The Ukrainian organizations develop new digital tools (Theme 7), but if, how and when they actually 'transform' the organizations is unclear. As war is an extremely changing, unpredictable, and unstable situation, e.g., infrastructure destructions which changed overnight the possibilities of managing remote work practices (Theme 5), facing constant risks in relation to cyber security threats (Theme 3), it is complicated to track what practices have actually been transformed in the long run. Our findings indicate that in such extremely challenging environments, constantly absorbing and adapting can be more plausible for organizations to consider compared to 'transformation', which requires more time to think through and implement. This finding can also offer a new angle to the digital resilience model.

Finally, our findings show the challenges with digital inequalities in times of crisis, and the importance of collaboration among organizations for building

resilience (Theme 4 and 5). Destruction of critical infrastructure, resulting in electricity and internet shortages forced the companies to complement the relatively stable remote-work mode by swiftly introducing co-working hubs, buying Starlinks, and power generators, and adapting work schedules. To manage this challenge, collaboration among companies was initiated, which emphasizes the importance of collective actions in building resilience in times of major shocks.

To sum up, this study, by analyzing a revelatory case of the Ukrainian organizations striving in times of war reveals the importance of DT which occurred during the previous crisis (the pandemic) for digital resilience in the next crisis (war). Digital technologies and remote work practices, adopted in the pandemic, paved the way for Ukrainian companies to survive, allowing connectivity of enforcedly relocated employees and enabling the managers to provide emotional support for their staff. The war also pushed forward the adoption of more agile management practices (Baskerville & Pries-Heje, 2021), fast decision-making, and less managerial control, which became realized by the integration of social media and messengers in organizations for enabling continuous communication, essential in a highly unpredictable environment.

Our findings contribute to complementing and extending the existing digital resilience model and crisis-driven DT in IS research. We also hope that our study can provide insights for managers to lead their organizations in times of major shocks.

6. Conclusions, limitations, and future research

As has been mentioned above, the war is still ongoing. Some organizations lost critical employees. At this moment, it is complicated to discuss DT and digital resilience in the long run; it requires conducting a longitudinal study. Further, in this paper, we provide a general picture of DT practices; the next step will be a more granular analysis of the differences among the companies, e.g., in terms of uneven access to digital infrastructures (Faraj et al., 2021). We also aim to validate our findings from the interviews with some secondary data, such as the digital traces from Telegram chats and MS Teams/Zoom meetings from the companies.

Accessing the effectiveness of government policies for supporting businesses during a crisis or relocation is another area to look at in future research. Further, all our participants are managers; the perspectives of the employees should be voiced. Going deeper into the managers' perspectives and combining the interviews with documentation analysis to get the perspectives from the organizational level is essential.

Finally, an in-depth analysis of organizations with a focus on sector-specific DT and digital resilience is the next step.

7. Acknowledgments

We acknowledge the grants by The Villum Foundation, The Carlsberg Foundation, the Novo Nordisk Foundation, Universities Denmark, and the Research Grant from the University of Gothenburg. The Fellowship for Scholars at Risk for Ukrainian Universities (SARU fellowships) allowed us to collect parts of the data and further develop this research.

8. References

Anthony Jnr, B. (2021). Implications of Telehealth and Digital Care Solutions During Covid-19 Pandemic: A Qualitative Literature Review. *Informatics for Health and Social Care*, *46*(1), 68-83.

Baiyere, A., Salmela, H., & Tapanainen, T. (2020). Digital Transformation and the New Logics of Business Process Management. *European Journal of Information Systems*, *29*(3), 238-259.

Baskerville, R., & Pries-Heje, J. (2021). Achieving Resilience through Agility. ICIS 2021 Proceedings: Building Sustainability and Resilience with IS: A Call for Action.

Berbyuk Lindström, N., Razmerita, L., & Prokopenko, I. (2023). *From the Pandemic to War: The Role of Digital Technologies in Ukrainian Businesses Responding to Discontinuities and Building Resilience.* Thirty-ninth Americas Conference on Information Systems), Panama.

Boh, W., Constantinides, P., Padmanabhan, B., & Viswanathan, S. (2023). Building Digital Resilience against Major Shocks. *MIS Quarterly*, *47*(1), 343-360.

Bowen, T., & Pennaforte, A. (2017). The Impact of Digital Communication Technologies and New Remote-Working Cultures on the Socialization and Work-Readiness of Individuals in Wil Programs. In *Work-Integrated Learning in the 21st Century* (Vol. 32, pp. 99-112). Emerald Publishing Limited.

Braun, V., & Clarke, V. (2012). Thematic Analysis. In P. M. C. H. Cooper, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Ed.), *Apa Handbook of Research Methods in Psychology. Vol 2. Research Designs: Quantitative, Qualitative, Neuropsychological, and Biological* (Vol. 2, pp. 57-71). American Psychological Association.

Carugati, A., Mola, L., Plé, L., Lauwers, M., & Giangreco, A. (2020). Exploitation and Exploration of It in Times of Pandemic: From Dealing with Emergency to Institutionalising Crisis Practices. *European Journal of Information Systems*, *29*(6), 762-777.

Di Gangi, P. M., Johnson, V. L., & Koch, H. (2022). Special Issue Editorial: Digital Transformation in Times of Crisis—an Introduction to the Special Issue and a Framework for Future Research. *MIS Quarterly Executive*, *21*(4), 4.

Duchek, S. (2020). Organizational Resilience: A Capability-Based Conceptualization. *Business Research*, *13*(1), 215-246.

Economist (2022). How Is Ukraine's Software Industry Weathering the War? *The Economist*

Eismann, K., Posegga, O., & Fischbach, K. (2016). Collective Behaviour, Social Media, and Disasters: A Systematic Literature Review. Twenty-Fourth European Conference on Information Systems (ECIS).

European Railway Award. (2023). *Https://Www.Europeanrailwayaward.Eu/News/54-Ukrainian-Railways-to-Receive-2023-Rail-Champion-Award.Html*. Retrieved 03092023 from https://www.europeanrailwayaward.eu/news/54-ukrainian-railways-to-receive-2023-rail-champion-award.html

Faraj, S., Renno, W., & Bhardwaj, A. (2021). Unto the Breach: What the Covid-19 Pandemic Exposes About Digitalization. *Information and Organization*, *31*(1), 100337.

Gorodnichenko, Y., Sologoub, I., & Weder, B. (2022). *Rebuilding Ukraine: Principles and Policies*. CEPR Press.

Han, B. R., Sun, T., Chu, L. Y., & Wu, L. (2022). Covid-19 and E-Commerce Operations: Evidence from Alibaba. *Manufacturing & Service Operations Management*, *24*(3), 1388-1405.

Hollnagel, E., & Woods, D. D. (2017). Epilogue: Resilience Engineering Precepts. In *Resilience Engineering* (pp. 347-358). CRC Press.

Kirchner, K., & Razmerita, L. (2019). Managing the Digital Knowledge Work with the Social Media Business Value Compass.

Magutshwa, S., Aanestad, M., & Hausvik, G. (2022). *Beyond Crisis Response: Leveraging Sociotechnical Transformability* 13th Scandinavian Conference on Information Systems,

Mankoff, J. (2022). *Russia's War in Ukraine: Identity, History, and Conflict*. Center for Strategic and International Studies (CSIS).

Martin, R., & Sunley, P. (2015). Towards a Developmental Turn in Evolutionary Economic Geography? *Regional Studies*, *49*(5), 712-732.

Matt, C., Hess, T., & Benlian, A. (2015). Digital Transformation Strategies. *Business & information systems engineering*, *57*, 339-343.

Oliveira, M. (2023). *What Is the Role of Information and Communication Technologies (ICT) in Building Resilience Aspects in Case of Disaster?"* Thirty-first European Conference on Information Systems (ECIS) Research Papers. 251.

Rosenberg, H., Ophir, Y., & Asterhan, C. S. C. (2018). A Virtual Safe Zone: Teachers Supporting Teenage Student Resilience through Social Media in Times of War. *Teaching and Teacher Education*, *73*, 35-42.

Sundermeier, J. (2022). Lessons for and from Digital Workplace Transformation in Times of Crisis. *MIS Quarterly Executive*, *21*(4), 5.

Swedish Research Council (Vetenskapsrådet). (2003). *Conducting Ethical Research*. https://www.vr.se/english/applying-for-funding/requirements-terms-and-conditions/conducting-ethical-research.html

The Intergovernmental Panel on Climate Change (IPCC). (2022). *Synthesis Report of the IPCC 6th Assessment Report (Ar6)*. https://www.ipcc.ch/report/ar6/syr/downloads/report/IPCC_AR6_SYR_SPM.pdf

United Nations (UN). (2022). *A New Era of Conflict and Violence*. https://www.un.org/en/un75/new-era-conflict-and-violence

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital Transformation: A Multidisciplinary Reflection and Research Agenda. *Journal of Business Research*, *122*, 889-901.

Vial, G. (2019). Understanding Digital Transformation: A Review and a Research Agenda. *The Journal of Strategic Information Systems*, *28*(2), 118-144.

Vogus, T. J., & Sutcliffe, K. M. (2007). Organizational Resilience: Towards a Theory and Research Agenda. 2007 IEEE International Conference on Systems, Man and Cybernetics.

Wang, B., Liu, Y., Qian, J., & Parker, S. K. (2021). Achieving Effective Remote Working During the Covid-19 Pandemic: A Work Design Perspective. *Applied Psychology*, *70*(1), 16-59.

Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading Digital: Turning Technology into Business Transformation*. Harvard Business Press.

World Health Organization (WHO). (2022). *Imagining the Future of Pandemics and Epidemics: A 2022 Perspective*. https://www.who.int/publications/i/item/9789240052093