Navigating Digital Resilience in Complex Emergency Management Environments

Jaziar Radianti
Centre for Integrated Emergency Management/
Dept. of Information Systems
jaziar.radianti@uia.no

ABSTRACT

The concept of digital resilience is becoming important in emergency management, due to the immense pressure toward digital transformations and numerous cyber threats against digital infrastructure that follows. This article suggest the need for incorporating cybersecurity dimension within emergency management and digital resilience to ensure business continuity of digital infrastructure if crisis hits. The reviews literature approach were conducted to decompose the digital resilience concept. This paper looks at key attributes of digital resilience, the role of technological tools, operational insights, and organizational practices in enhancing resilience. The study identifies research gaps, calling for holistic digital resilience approaches, cross-sectoral collaboration, and leveraging emerging technologies to enhance digital resilience in emergency management, derived from literature. Pre-crisis and post-crisis digital resilience strategies are examined as a basis for proposing the future research agenda.

Keywords

Digital Resilience Framework, Cybersecurity, Emergency Management, Digital Infrastructure

INTRODUCTION

Literature on the concept of digital resilience suggests a vision for future emergency management that understands the interconnection of cybersecurity, societal security and crisis management (Magutshwa & Radianti, 2022; Radianti, 2024). This is crucial, considering rapid ongoing digital transformations and reliance on interconnected devices and systems in these three domains. These papers call for a comprehensive understanding of digital resilience to enable effective response to emergencies in an increasingly complex cyber-physical systems landscape. Radianti (2024) also points out that digital resilience includes managing risks and ensuring the continuity of operations during disruptions caused by cyber threats and other digital disasters.

Digitalization of technologies supporting essential services is unstoppable, making such sectors attractive targets for perpetrators. Over the years, cyberattacks have been increasingly targetting digital infrastructure of critical societal functions. A notable, recent case is the discovery of critical vulnerabilities in the Enphase OQ Gateway, an IoT-based solar panel infrastructure, by Dutch ethical hackers (DIVD-CSIRT, 2024). This device, crucial for converting solar power for home use, had six zero-day vulnerabilities that could have granted attackers full control if connected to the public internet. With over four million systems in 150+ countries at risk, a successful attack could have caused widespread power outages, financial losses, and national security threats (Gevers, 2024). As solar energy integrates into national grids, its *digital resilience* becomes vital for a secure transition to sustainable energy.

The Pennsylvania water system cyberattack is another example of attack against essential service. It forced the Municipal Water Authority of Aliquippa running manual operations. The breach aimed at compromising a programmable logic controller (PLC) that regulates water pressure for two townships with over 7,000 populations (Toulas, 2023). Although no direct harm occurred, the attack accentuates the rising threat to essential services that requiring for organizations to reinforce *digital resilience*.

Cybersecurity measures to counteract such events, are just one dimensions of digital resilience. These cases signify inseparable link between *cybersecurity*—preventing virus and malware from cascading into other critical digital infrastructure—and *emergency management* such as a municipality anticipating water supply disturbance. In these examples, digital resilience encompasses the responders´digital capacity, an organization´s ability to recover and prevent cascading effects on societal safety, or even national security, and the use of digital tools for rapid coordination. In brief, I argue that securing critical digital infrastructure goes beyond cybersecurity measure. *Digital resilience is a core*.

The digital resilience theme surfaced during the Covid-19 crisis and the Ukrainian war, as cyberattacks have intensified following these two events (Garcia-Perez et al., 2023; Lee et al., 2024). Scholars pinpoint the significance of innovative solutions to help societies withstand and recover from crises (Magutshwa & Radianti, 2022; Park et al., 2023; Zubok, 2023), including strengthening digital resilience (Al-Abdulghani et al., 2021). The Information Systems field, e.g., has significantly contributed to this discourse by offering frames for digital resilience (e.g., Al-Abdulghani et al., 2021; Fleron et al., 2021; Kohn, 2020; Spagnoletti & Za, 2021; Tim & Leidner, 2023) and suggest for holistic digital resilience strategies. Several white papers representing connected industries have exclusively stressed digital resilience to cope with the pandemic, providing general outlines and frameworks (Abassi, 2021; Abbasi, 2021; Abbasi & Jung, 2023).

On the other hand, emergency management scholars have acknowledged and scrutinized the increasing use of digital tools in the domain, however, digital resilience is often overlooked or not framed as an essential part of emergency management cycles. Current literature highlights some issues such as conceptual confusion due to inconsistent usage across studies and calls for comprehensive frameworks and practical strategies for enhancing digital resilience across various contexts, including education, healthcare, and critical infrastructure (Tim & Leidner, 2023). This article highlights the multiple definitions and discussions in the literature that limit its use in emergency management literature, especially with inerconnectedness with cybersecurity, and argues for enhancing the concept´s applicability by aligning it with the pre- and post- emergency management lifecycle.

In summary, while digital resilience offers a valuable framework for managing physical-cyber threats in emergency management, more studies are required to make this concept applicable in the domain. This article seeks to systematize knowledge on themes related to digital resilience in complex systems, its attributes, and methods for measurement and operationalization. The ultimate goal is to outline future research directions how to tailor better digital resilience within the scope of interconnectedness between cybersecurity and emergency management research.

RELATED WORKS AND THE CONCEPT

To understand how digital resilience is conceptualized in the literature, I analyze multiple studies to explore: 1) the definition of the digital resilience concept and 2) key dimensions of digital resilience thinking.

What is Digital Resilience?

Resilience as a concept has been scrutinized across various research domains and applied in different ways (Marana et al., 2019; Radianti, 2016; Radianti & Gjøsæter, 2021) since the concept was coined by Holling (1973) as the ability to respond to and recover from disturbances, absorb changes and persist. Radianti (2016) demonstrate the conceptual variations of resilience, ranging from resilience of critical infrastructure, cities, ecology, cybersecurity, and economy, to organizations to individual and psychological resilience—indicating the challenge for mainstreaming the concept and achieving consensus (Radianti & Gjøsæter, 2021), and establishing widely accepted definitions (Kohn, 2023). However, I concur with Manyena (2006) who argues that having multiple definitions of resilience is not necessarily problematic, as long as they do not hinder conceptual clarity, since reaching consensus is not an end itself (Radianti & Gjøsæter, 2021). What matter is how the concept can be meaningfully applied to explain how a systems, societies, individuals and communities withstand the disturbances and disasters. However, only recently the concept is “reinvented”, increasingly studied, and popularized within the IS literature (Kohn, 2023), especially in the context of digital resilience during crises. This resurgence underscores the concept´s appeal, inspiring ongoing reinterpretation and redefinition to address the contemporary challenges. Moreover, to be more applicable, researchers also have addressed the importance of operationalizing and develop measurements and indicators of the concept, to move the concept from theory to practice, and to and to contextualize it such as “resilience to what?” (Radianti, 2016).

What then is digital resilience? As with the preceeding issues, the cofusion around how to define *digital resilience* (DR) occurs, with the term being conceptualized in various ways across different studies. Earlier definition of DR

has been proposed to refer to "*design, deployment, and use of information systems* to recover from or adjust to major disruptions (Boh et al., 2023) in complex organizations" (Spagnoletti & Za, 2021). Another definition suggests DR as the ability of a system to respond to external shocks, grow, and survive in a changing environment. This includes the capacity to adapt and maintain functionality despite disruptions (Lin & Tao, 2024; Zubok, 2023). Basically, the concept encapsulates the *system response and adaptation* or *the design, deployment and use of information systems* to adapt to changes by major external shocks.

Within this broad definition, researchers propose a *multi-tiered* perspective of DR, where two or more of these aspects are intertwinned: individual, organizational, national, and community. It is about the ability to manage risks from diverse threat sources, such as natural disasters, health crises, and online threats through adaptability, recovery capability, and the continuous use of digital technologies.

From the *national and community resilience* standpoint, DR focuses on the resilience of digital infrastructures. Nationally, it emphasize the need for national ICT infrastructure *to endure and recover* from external threats, ensuring continuity of essential services. Before the DR term became popular, the e-resilience term was introduced to indicate the contribution of digital information systems to community resilience (Kohn, 2020, 2023). The concept underscores the ability *to use* information technologies to cope with challenges and self-governing recovery (Abassi, 2021; Itzhak & Ferri, 2023; Pan et al., 2024). Pan et al., (2024) suggest enhancing DR service community organization and platform intervention.

Broad definitions of DR also describe it as the capability of organizations and systems to manage shocks, adjust to disruptions, and stabilize (Al-Abdulghani et al., 2021; Fernandes et al., 2023; Fleron et al., 2022; Kohn, 2020, 2023). It refers to an orgaization´s capacity to foresee, plan for and effectively deal with changes and difficulties in the digital space (Dzandu et al., 2024). These definitions pinpoint to role of digital technologies in rapid recovery and adjustment to external shocks, and maintaining operational stability (Kohn, 2020; Park et al., 2023). Al-Abdulghani et al. (2021) suggest DR as "implementing information technologies to adapt, rebound, and recover when faced with challenges and disruptive events." These definitions illuminate *strategic and operational agility to overcome disruptions* while *harnessing digital technologies* to enhance resilience (Fleron et al., 2022; Li et al., 2024; Neumannova et al., 2023b).

Moreover, this o*rganizational* perspective (Neumannova et al., 2023b) focuses on situation awareness, IS vulnerability management, and the need for adaptive capacity (Doctor et al., 2023; Kohn, 2020, 2023). Flexibility, agility, and risk intelligence of IS are crucial in a complex and interconnected environment (Neumannova et al., 2023b; Park et al., 2023). Definitions also highlight the importance of organizational capabilities to face disruptions and unexpected events strategically and operationally (Kohn, 2020, 2023). This perspective also extends to *Crisis and Emergency Management*, examining how organizations design, deploy, and use IS to swiftly recover from or adjust to major disruptions. The aim is to maintan high-quality services and customer satisfaction during crises, by leveraging digital technologies to adapt practices while preserving core functions (Magutshwa & Radianti, 2022). The role of IS in supporting business continuity and disaster recovery planning is key (Fleron et al., 2022; Kohn, 2020; Park et al., 2023). Zhang and Wang (2024), illustrate attributes related to various digital infrastructure used for smart emergency response, thereby defining DR as the ability to withstand, adapt to and recover from digital malfunctions and vulnerabilities.

Additionally, resilience is linked to risk management (e.g., Dzandu et al., 2024) andressing both: 1) the resilience of an individual, group or firm in relation tothe risks that digital technologies can present; 2) resilience to risk created by (extraordinary) events to individuals, groups or firms by managing them through digital technologies. Thus, to put the DR concept into action, organizations must create a strategy that successfully mitigates a broad variety of digital risks (Dzandu et al., 2024).

Contrasting the general DR perspective, some scholars emphasize *Individual Resilience* particularly employees facing digital disruptions (Al-Abdulghani et al., 2021; Kohn, 2020, 2023). This definition highlights the *psychological capacity* to bounce back from adversity, adapt to changes, and maintain productivity *using IS and digital channels*. The definitions emphasize the importance of individual resilience in ensuring overall organizational resilience, particularly in response to cyber events. For instance, Al-Abdulghani et al. (2021) note, "individual DR provides cognitive ability to adapt to new technologies adjust lifestyle to digital transformations." This involves recognizing and managing online risks, safeguarding digital assets, and maintaining operational capabilities (Atif & Qureshi, 2024; Garcia-Perez et al., 2023).

Shandilya et al. (2024) add that individual DR evolves through personal experiences and introspective refection. Differences in individual resilience depend on contextual variables, personal backgrounds, chronological progression and additional pertinent aspects. The focus is on *adaptability, recovery, and the ability to thrive* despite digital challenges, ensuring both personal and organizational resilience.

Lasty, literature also discuss the resilience definition in terms of *Technological and Strategic Adaptation.* This perspective highlights the role of technology and strategic adaptation in achieving DR. It describes how organizations utilize digital technologies to change practices, adapt to new circumstances, and maintain productivity. The focus is on strategic awareness and operational management of internal and external shocks, ensuring the resilience of IS output systems and community resilience through ICTs (Fernandes et al., 2023; Fleron et al., 2022; Kohn, 2020; Neumannova et al., 2023b). DR definitions are in line with Boh (2023), that it is about the capabilities to design, deploy, and use information systems to adjust to changes caused from external shocks. Essentially, this definition emphasizes the importance of information systems capabilities in building resilience (Kohn, 2023).

DR is also understood as as the capacity to learn, recover and bounce back after negative or adverse online experiences, encompassing both psychological and behavioral dimensions (Sharma et al., 2022). This perspective integrates elements such as system adaptability, individual psychlogical resilience and cyber resilience. It highlights how digital systems can absorb and recover from cyber threats while preserving core functionalities and operational continuity (Atif & Qureshi, 2024; Garcia-Perez & Sallos, 2023; Lindström et al., 2024; Mahmood et al., 2024). As digital technologies become increasingly embedded within social, economic and political infrastructures, robust cybersecurity measures emerge as essential strategic responses to safeguard these critical dependencies. Overall, the overview of the definitions and keywords can be seen in Table 1:

Table 1 Summary of key concepts in DR definition and DR capacity

Perspectives		**Key concepts**	**Capacity or Capability**
Broad Perspective	**Multitiered Perspective** Boh et al. (2023), Spagnoletti & Za (2021), Lin & Tao (2024), Zubok (2023)	Adaptability, Recovery capability, Digital technologies	Ability to coordinate across multiple levels (individual, organizational, community, national) for adaptability and recovery through digital technologies.
	National and Community Resilience - Kohn (2020, 2023), Abassi (2021), Itzhak & Ferri (2023), Pan et al. (2024)	Digital infrastructure, ICT systems, Community resilience, Self-governing recovery	Strengthening digital infrastructure and ICT systems to support community resilience and self-governing recovery.
	Organization Resilience - Al-Abdulghani et al. (2021), Fernandes et al. (2023), Fleron et al. (2022), Kohn (2020, 2023), Park et al. (2023)	Operational stability, Strategy, Digital technologies, Business continuity	Capacity to maintaining operational stability and continuity through strategic use of digital technologies.
	Risk Management - Dzandu et al. (2024)	Risk identification, Anticipation, Mitigation, Strategy	Capacity to Identifying, anticipating, and mitigating digital risks through strategy.
Individual Resilience - Al-Abdulghani et al. (2021), Kohn (2020, 2023), Atif & Qureshi (2024), Garcia-Perez et al. (2023), Shandilya et al. (2024)		Psychological capacity, Adaptability, Bounce back, Cognitive ability	Psychological adaptability and cognitive ability to bounce back from digital disruptions.
Technology and Strategic Adaptation - Fernandes et al. (2023), Fleron et al. (2022), Kohn (2020, 2023), Neumannova et al. (2023), Boh (2023), Sharma et al. (2022), Atif & Qureshi (2024), Garcia-Perez & Sallos (2023), Lindström et al. (2024), Mahmood et al. (2024)		Strategic adaptation, Operational management, Digital technologies, Cybersecurity measures	Capacity to ensuring strategic adaptation and operational management through digital technologies and cybersecurity measures.

To sum up, this variations show conceptual confusion in current literature due to inconsistent usage across studies. Thus, attempt to create comprehensive frameworks and practical strategies for enhancing digital resilience across various contexts are required (Tim & Leidner, 2023).

Dimensions and Focuses

Existing literature indicates three main streams of thought regarding dimensions and focuses of DR.

The first stream of the literature emphasizes *the key attributes of DR* such as *robustness, flexibility, adaptability, redundancy and intelligence (Zhang & Wang, 2024)* link to inter-jurisdictional data sharing and digital collaboration, essential for building resilience in government emergency management. Son et al. (2020) connect DR to collective sensemaking, team decision making, harmonizing work-as-imagined and work-as-done, and interaction and coordination for emergency management resilience.

The second stream associates DR with *"technological tools and approaches that are deemed "digital"*. This includes mapmaking, event history logging, mobile communication applications, integrated information management systems, and decision support tools enhancing resilience in emergency management. DR can also involve "big data utilization" for early warning systems, weather forecasting, emergency evacuation and relief distribution (Sarker et al., 2020). Through these researchers do not apply the DR idea straightway, they emphasize features like robust infrastructure, local skill enhancement and responsible data sharing. Lee et al. (2024) discuss digital resource orchestration, highlighting dual purposing of existing information systems, balancing data exploitation, enacting online co-production and augmenting social network effects as key patterns to build DR.

The third stream of DR in the literature focuses *on operational and organizational insights*. Park et al. (2023) propose centralized IT governance to help organizations maintain service operations and adapt better during crisesciting the COVID-19 pandemic, though this is mainly applicable to sectors like higher education and seldom addresses managing short-term, sudden crises. Penadés et al. (2017) emphasize the need incorporating resilience in emergency management plans. Gooding et al. (2022) advocate inclusive coordination and partnerships across government sectors, highlighting the importance of clear roles, sufficient capacity, and strong leadership for effective emergency management.

In brief, DR dimensions form literature include:

- Enabling attributes necessary for systems, organizations, and communities to withstand disruptions.
- Disagreement concerning measurement, operationalization and contextualization of DR.
- A needs for real-life examples and frameworks, like Ukrainian´s digital response to power grid missile attacks, illustratrating dependencies and interactions affecting DR.

While DR is an intriguing concept, existing studies rarely examine how DR can be used to deal with increasingly complex, interconnected systems within the emergency management cycle. Given this fragmented understanding, this article aims to systematize the DR concept and examine its impact on the emergency management domain, areas scarcely addressed in recent literature.

RESEARCH DESIGN

This study applied systematic literature review (SLR) approach as a way to explore the academic discourse concerning DR that are linking to emergency management and cybersecurity. SLR has been widely used as an approach to derive insights and obtain overview from literature in a specific research domain (Kitchenham et al., 2009; Webster & Watson, 2002). Three digital databases were utilized, i.e., Scopus, AISel and IEEE-Xplore using the following keyword searches:

- "Digital Resilience" AND "Emergency Management" OR "Disaster Management" OR "Crisis Management".
- "Digital Resilience" AND Cybersecurity" OR "Cyber Security"

ISCRAM Digital library was skipped since it did not return the relevant results. All terms were searched based on titles and abstracts. The filtering process did not limit the publication year, as this topic began appearing naturally in the digital library from 2020 during the search. Outlets (conference or journal articles) and citations were not primary filtering considerations to avoid missing valuable insights, while only a limited results were obtained to begin with. Although the search was divided for a clearer overview, the analysis treated the results as an agregate. The following table illustrates the filtering process:

Table 2. Literature Filtering Process

Source	Original	Duplication	Exclusion	Inclusion	Final papers
Aggregated from AISEL, IEEE-Xplore and Scopus	128	76	40	27	17

The exclusion process involved examining the title, while the inclusion process required a careful reading of the abstract to determine if the articles: 1) defines or discusses the DR concept; 2) applies the DR concept to either cybersecurity or crisis management. The final step involved thoroughly reviewing the full-paper. Papers focusing on emotions and sentiment analysis, measurement and operationalization of DR, leaning towards Industry 5.0, financial crises in organizations, and other unrelated topics were further excluded.

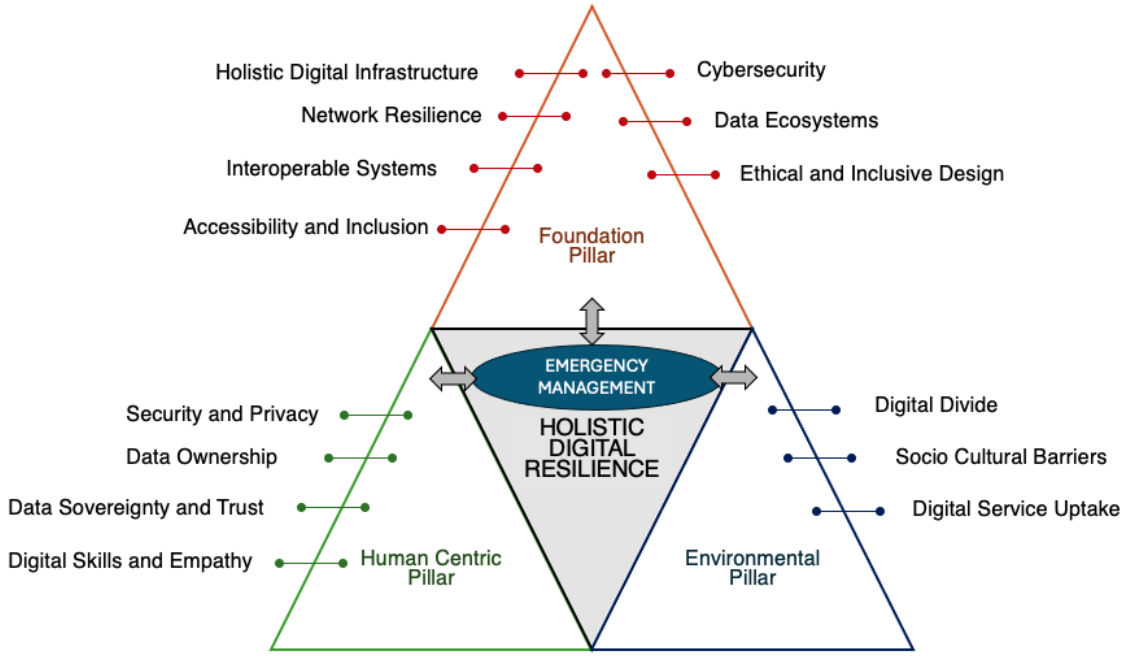

Figure 1. Framework for Analyzing Holistic DR

As a starting point to map DR literature for this purpose and help the coding process, I adapt the following framework (Fig. 1), partly extracted from Abassi (2021), as a quite comprehensive picture of the DR concept. The following definitions in Table 3 are used as basis for extracting information from the articles.

Table 3. Holistic Framework Explanation as a basis for coding the literature

Foundation	**Explanation**
The foundational pillar (upper part of Fig.1)	It capture the essential infrastructure and systems necessary to support and ensure holistic DR. This includes building resilient digital infrastructure, ensuring network and information systems resilience, promoting interoperability and compatibility of systems and data, making digital services accessible and affordable, implementing robust cybersecurity measures, establishing digital identity systems, creating integrated data ecosystems, and incorporating ethical and inclusive design principles. Papers will be coded using these component
The human centric pillar (bottom left of Fig. 1)	It encompasses designing and implementing digital technologies that prioritize the safety, security, privacy, and well-being of individuals. It includes developing digital skills, ensuring data ownership (empowering user control over their personal data), data sovereignity (data is subject to the laws and governance structures within the nation where it is collected) and trust, and incorporating empathy to address the diverse needs of users, especially vulnerable communities.
The environmental pillar (bottom right pillar of Fig.1)	addresses the underlying societal and cultural barriers to DR, focusing on issues such as rural-urban and gender divides. It aims to redesign economic and social systems to uproot inequalities and exclusions, ensuring that DR efforts contribute to promoting inclusive and equitable access to digital technologies.

While Abassi (2021) does not list emergency and disaster management as a part of foundation pilar, and rather an example of cross sectoral issues, but in this framework, I suggest to include it as a main feature of holistic DR. The literature analysis and coding will follow the structure of Figure 1. The coding was done using qualitative software Nvivo.

RESULTS

The results is organized based on the coding process using the framework suggested in Figure 1.

Foundation Pillars

On holistic, robust digital infrastructure, network and information systems, Fleron et al. (2022) highlight the essential aspects of digital resilience (DR) in supporting digital transformation within the public sector, using Denmark as an example. This involves constructing resilient digital infrastructure characterized by high-speed broadband connectivity for households and businesses. Doctor et al. (2023) highlight the importance of IT provision, which includes equipping IT workplaces, procurement, infrastructure, service processes, cloud-based services, and ensuring network continuity (Park et al., 2023; Zighan, 2024). Additionally, there is a significant focus on orchestrating digital resources and repurposing existing information systems (Lee et al., 2024; Magutshwa & Radianti, 2022). Abbasi (2021) emphasizes ICT infrastructure resilience, including ensuring redundancy, diversity of network routes and equipment, and rapid resource mobilization during attacks or disasters.

On the interoperability, Fleron et al. (2022) also stress this as important for promoting collaborative strategies and the integrating digital technologies across public sectors, despite inherent technical interoperability challenges (Doctor et al., 2023; Zhang & Wang, 2024). In conflict setting like the Ukrainian war, migrating sensitive data to secure cloud services outside the country (and backing up sensitive data, e.g., in EU servers) is crucial for protecting against cyber and kinetic attacks (Itzhak & Ferri, 2023; Lindström et al., 2024). Reconfiguring and adopting new technologies, such as Blockchain Technology can establish a secure digital environment (Mahmood et al., 2024), complemented by cybersecurity risk management tools, penetration testing, and partnership with external security organizations to strengthen resilience.

On accessibility and digital inclusion: The increased availability of digital public services reflects efforts to make these services accessible to all (Doctor et al., 2023). Digital identities are crucial dor digital identity and transaction systems (Fleron et al., 2022), with an emphasis on utilizing familiar technology afor broad accessibility (Lee et al., 2024; Magutshwa & Radianti, 2022). In conflict situations, maintaining access to essential service like digital identification remains vital (Itzhak & Ferri, 2023). Extending broadband infrastructure to underserved and and developing policies ensure digital access and inclusion (Abbasi, 2021).

On cybersecurity, DR literature highlights IT security management, identity and access management, stressing adherance to standards for high-security levels. Zhang and Wang (2024) discuss risks like digital malfunctions, vulnerabilities and cyberattacks. Spagnoletti and Za (2021) examine digital technologies´dual role in introducing new risks and enhancing performance during accidents. Garcia-Perez et al. (2023) highlight cyber resilience, while Mahmood et al. (2024) suggests robust cybersecurity measures, including awareness programs, and role redefinition. Zighan (2024) advocates advanced measures (Magutshwa & Radianti, 2022), including threat intelligence, and real-time response mechanisms. Overall, the article stresses the adoption of security-by-design and privacy-by-design principles to protect digital systems and build trust (Abbasi, 2021).

On data ecosystems, Doctor et al. (2023) emphasize integrated IT systems for seamless data ecosystems, ensuring control, error control, and simplified communication across department and organizations. Lee et al. (2024) stress integrating data sources for a comprehensive crisis response. In war situation, data migration to cloud services and creating private clouds in allied countries support integrated data ecosystems (Itzhak & Ferri, 2023). Zighan (2024) mentions the importance of cybersecurity integration and recognizing supply chain interdependence.

On ethical and inclusive design principles, Doctor et al. (2023) address focus on stakeholder orientation and societal impacts, including privacy, in e-government. Spagnoletti and Za (2021) discuss design´s role in deploying, and using information systems to recover from or adjust to major disruptions in complex organizations. Lee et al. (2024) emphasizes balancing data exploitation with privacy and ensuring ethical and inclusive digital interventions. Abbasi (2021) suggest people-centered approach respecting the needs and rights of all people, including marginalized and vulnerable groups and equitable access to digital resources (Shandilya et al., 2024).

Human Centric Pillar

On security and privacy: DR literature emphasize the well-being of individuals by integrating human values such as privacy, care, freedom of movement, and health into digital interventions (Lee et al., 2024; Shandilya et al., 2024). This approach helps reconcile dilemmas and ensures the public acceptance of digital systems.

On data ownership, DR literature underscores the importance of data protection, migrating sensitive data to secure cloud services, ensuring data ownership, and empowering user control over personal data. The relevance of data sovereignty during wartime is particularly emphasized (Itzhak & Ferri, 2023).

On data sovereignty and trust, the literature emphasizes the need for national strategies and local compliance that align with national laws and governance structures (Fleron et al., 2022). Building trust involves setting transparent paths addressing specific institutional requirements (Doctor et al., 2023; Lee et al., 2024).

On digital skills and empathy: DR literature highlights enabling factors such as psychological resilience, community capital, family support, access to technology, digital expertise, and self-efficacy (Al-Abdulghani et al., 2021). Digital literacy, skills, and reskilling for government stakeholders (Garcia-Perez et al., 2023; Zhang & Wang, 2024) and employee training (Doctor et al., 2023) are necessary to tackle digitalization and cyberthreats (Zighan, 2024). Literature stesses developing digital skills through new procedures, cybersecurity awareness programs, workshops, and personalized security sessions (Mahmood et al., 2024). Comprehensive upskilling to ensure citizens can learn safely online, with cybersecurity experts teaching security skills to non-technical individuals (Abassi, 2021; Zighan, 2024). The literature advocates for empathy and addressing diverse needs, emphasizing strategies based on citizen needs and societal impacts (Fleron et al., 2022) while ensuring inclusivity for all, especially vulnerable communities (Lee et al., 2024). Examples include digital caring systems supporting quarantined individuals during COVID-19. Extending broadband infrastructure and developing skills for locally-driven content and applications are crucial for unserved and underserved areas (Abbasi, 2021).

Environmental Pillar

On socio-cultural barriers: Abbasi (2021) and others highlight the significant societal and cultural barriers that limit access to digital technologies for women, older adults, persons with disabilities, ethnic minorities, indigenous groups, migrants, refugees, internally displaced persons, and those living in rural or remote areas. As education, work, and public services shift online, these groups are disproportionately left behind. To address these inequalities, Abbasi (2021) calls for the participation of marginalized groups in DR efforts.

On digital service uptake: In line with this, Doctor et al. (2023) and Lee et al. (2024) emphasize the importance of involving citizens in decision-making processes and government-citizen collaboration to develop inclusive digital solutions that address diverse needs. They stress advocate the policies and investments to enhance access to digital technologies and propose building digital skills through employee involvement and training to reduce digital literacy disparities.

On digital divide: Lindström et al. (2024) discusses implementing support measures for vulnerable employees, such as providing psychological support and encouraging volunteering, to foster an inclusive and equitable digital environment. These combined efforts aim to bridge digital divides and ensure that digital advancements benefit all population segments.

Beyond these pillars, literature also pointed out the environmental consideration such as data centres and energy-intensive digital operations and how to be more environmentally advantegeous practices, (Shandilya et al., 2024), whci can be additional consideration under this environmental pillar.

Emergency Management

Emergency management is closely linked to DR concerning the use of digital technologies to anticipate, prepare for, and mitigate disasters. DR ensures that networks and information systems remain operational and can recover swiftly from disruptions caused by natural disasters, health crises, and cyberattacks. Table 4 shows the themes on **Pre-Crisis Digitally resilient Emergency Management,** in the relationship with holistic framework:

Table 4. Pre-Crisis Digitally resilient Emergency Management

Themes	Description	Relations to the Holistic Framework
Risk Assessment & Early Warning Systems:	Digital technologies enable data collection, processing, mapping, and visualization of disaster risks, enhancing early warning systems and multi-stakeholder engagement (Magutshwa & Radianti, 2022).	Holistic Digital infrastructure/ **Foundation Pillar**
Smart Logistics onboarding process & Resource Allocation:	Integrated logistics and supply chains ensure timely delivery of critical supplies during crises. Centralized IT systems facilitate smooth organizational coordination and resource prioritization. While onboarding is to make people familiar with working from offline to online (Neumannova et al., 2023a; Park et al., 2023)	Holistic Digital infrastructure/ **Foundation Pillar**
Cybersecurity Preparedness	Organizations must ensure cybersecurity resilience by maintaining compliance with legislative requirements, allocating sufficient budgets for cyber response, and establishing robust cybersecurity frameworks to prevent cyber threats (Fernandes et al., 2023; Garcia-Perez et al., 2023).	Cybersecurity/ **Foundation Pillar**
Cloud Migration & Data Protection:	Rapid cloud migration protects data from cyber and kinetic attacks, ensuring security and continuity of essential services. Digital sovereignty and self-reliant digital ecosystems are vital for securing critical infrastructure (Itzhak & Ferri, 2023).	Data ecosystems/ **Foundation pillar**
Communication, Continuity Planning and Risk Management	High-reliability organizations emphasize flexible decision-making and communication in emergencies (Spagnoletti & Za, 2021). Strategies include telecom backups, reliance on high-capacity batteries, internal roaming, and satellite telecommunications (e.g., SpaceX's Starlink) to maintain connectivity when infrastructure is damaged (Fernandes et al., 2023; Itzhak & Ferri, 2023; Lindström et al., 2024).	Holistic Digital infrastructure, Network Resilience, Interoperable systems/ **Foundation Pillar**
DR Framework	Zighan (2024) suggests of "sense, resist, and react" model, which integrates threat intelligence, advanced cybersecurity measures, and real-time response mechanisms Fernandes et al. (2023) suggest Resistance, Absorption, and Restoration.	Holistic Digital infrastructure/ **Foundation Pillar**

Post-Crisis digitally resilient Emergency Management: During and after a crisis, DR supports emergency management by providing infrastructure, data, and tools for rapid response, adaptation, and recovery. The following themes appear in the literature (Table 5).

Table 5. Post-Crisis digitally resilient Emergency Management

Themes	Description	Relations to the Holistic Framework
Crisis Response, Reacting Capability & Coordination:	Digital platforms enhance coordination by fostering information sharing, collaboration, and collective action. Digital twins simulate complex system behaviors to improve crisis decision-making (Spagnoletti & Za, 2021). Moreover, creating incident response strategies, ongoing testing, and ensuring a rapid and well-coordinated plan to contain and mitigate damages from an attack is crucial to is to minimize downtime and a swift return to normal operations (Zighan, 2024)	Holistic Digital infrastructure, interoperable systems/ **Foundation Pillar**
Remote Operations & Business Continuity:	Organizations must prepare for rapid transitions to remote work, ensuring continuity by providing technical support and maintaining business functions during disruptions (Fernandes et al., 2023; Garcia-Perez et al., 2023; Lindström et al., 2024; Neumannova et al., 2023a; Park et al., 2023).	Holistic Digital infrastructure/ **Foundation Pillar**
Cyber Resilience in Crisis Management:	Cyber resilience involves absorbing and overcoming cyberattacks while maintaining core operations. This includes response plans, cybersecurity training, and investment in mitigation strategies (Garcia-Perez et al., 2023; Lindström et al., 2024).	Cybersecurity/ **Foundation Pillar, Human Centric Pillar**

Themes	Description	Relations to the Holistic Framework
Workforce Safety & Mobility:	In conflict zones, organizations should consider pausing activities, relocating to safer areas, and ensuring continuous communication to track employee movements (Lindström et al., 2024).	Holistic Digital infrastructure/ **Foundation Pillar**
Adaptability, Exaptation & Learning:	Organizations must remain adaptable, employing flexible decision-making and agile coordination among frontline operators. Digital technologies support organizational learning and adaptation to changing crisis conditions, repurposing of traits, technologies, processes, skills, and resources for emergent uses that they were not initially designed for (Magutshwa & Radianti, 2022; Spagnoletti & Za, 2021).	Digital skills and emphathy/ **Human Pillar**

DISCUSSIONS AND RESEARCH AGENDA

DR is not an easy concept to entangle, as it is multidimensional. The proposed framework helps to tailor different opinions on what is considered as DR. This concept shows also the potential as a framework for mitigating (pre-crisis), recovering from, and adapting to (post-crisis) threats to digital infrastructure versus threats to physical and social infrastructures. Importantly, resilience to disruptions to digital infrastructure likely involve cyber-physical-social aspects that relate to the different pillars in Figure 1. Using the framework illustrated in Figure 1, we observe the most obvious gap, where most of literature leans toward emphasizing the digital technologies as enablers for digital resilience. Moreover, while we have discovered some useful link between DR and emergency management, it has not yet been concreted enough to be adopted directly and adapted into different crisis scenarios. Some identified gaps and future possible DR research direction are as follows:

- ***Integration of Cybersecurity and Emergency Management****:* Research should focus on integrating cybersecurity measures with emergency management strategies to enhance digital resilience (DR) by combining cybersecurity protocols with disaster response and recovery plans.
- ***Human and Environmental Pillars****:* Current DR suggestions often overlook human and environmental aspects. Incorporating these pillars is essential for achieving holistic DR, and thus opportunities for further research.
- ***Holistic Cybersecurity Approaches****:* Limited research exists on holistic cybersecurity approaches that include social, economic, and cultural dimensions. Understanding how cybersecurity threats impact various communities and sectors is crucial for developing inclusive strategies.
- ***Cross-Sectoral Collaboration****:* More research is needed on effective cross-sectoral collaboration between cybersecurity experts and emergency management professionals to enhance DR. This includes fostering partnerships and coordination among stakeholders and exploring how responders can coordinate with cybersecurity experts on potential cyber attack events.
- ***Cybersecurity and Data Privacy****:* Research should explore the balance between cybersecurity measures and data privacy, especially during emergencies, to ensure individuals' privacy rights are protected while implementing cybersecurity protocols in crisis situations.
- ***Use of Emerging Technologies****:* Investigating the use of AI, blockchain, and IoT in enhancing cybersecurity and emergency management is necessary. Research should explore how these technologies can improve DR, detect and respond to cyber threats, and support disaster response and recovery efforts.
- ***Long-Term Adaptation****:* Understanding how individuals and organizations can sustain resilience over extended periods and through multiple crises is crucial for long-term DR research.
- ***Interdependencies between Critical and Digital Infrastructure****:* Research is needed to understand the consequences and mitigation measures due to the integration of ICTs into the operations of critical infrastructure. The Digital Operational Resilience Act (DORA) in Europe, for example, aims to safeguard ICT-based operations in finance, indicating a need for similar measures in other critical infrastructures.

CONCLUSION

DR is multidimensional and evolving concept that encompasses the ability of systems, organizations and individuals to respond, adapt and recover from digital disruptions, including cyber threats, natural disasters and other crises, such as recent Covid-19 pandemic. DR spans multitiers—individual, organizational, national and communicty levels, highlights the importance of IS and digital technologies to maintain operational stability and continuity during disruptions. The key dimensions of DR encompass the attributes, tools, organizational practices and contextual factors necessary to build resilience in increasingly complex and interconnected environments and involving cyber- physical- social systems. In conclusion, the integration of DR into emergency management is

essential for navigating the challenges posed by increasingly complex and interconnected systems. DR provides the technological tools, organizational practices, and strategic frameworks necessary to anticipate, respond to, and recover from crises effectively. The research in holistic DR is still incomplete, thus opening up opportunities to fulfill existing gaps. By addressing pre-crisis preparedness, enhancing crisis response and coordination, and supporting post-crisis recovery, DR ensures the continuity of critical infrastructure and societal functions. Furthermore, its emphasis on cybersecurity and adaptability highlights its strategic importance in mitigating cascading effects and safeguarding national security. As emergency management evolves, fostering digital resilience will be pivotal in building robust, flexible, and adaptive systems capable of withstanding disruptions and ensuring long-term sustainability.

REFERENCES

Abassi, S. (2021). *Digital Resilience IC Activity: Foundational Principles for Digital Resilience Framework* (Digital Resilience IC Activity, Issue. IEEE.

Abbasi, S. (2021). *Digital Resilience IC Activity: Sustainable, Secure, and Inclusive Digital Resilience (DR)* (Industry Connections Report, Issue.

Abbasi, S., & Jung, B. K. (2023). *Mapping of Key Digital Health Initiatives Building Resilience for Current and Future Pandemics* (Industry Connections Report, Issue.

Al-Abdulghani, Y., Vatanasakdakul, S., & Aoun, C. (2021). Tough as Nails? An Individual Perspective to Digital Resilience During a Pandemic. AMCIS,

Atif, A., & Qureshi, M. A. (2024, 4-8 Aug. 2024). Enhancing Digital Resilience through AI in Industry 5.0: A Technology Management Perspective. 2024 Portland International Conference on Management of Engineering and Technology (PICMET),

Boh, W., Constantinides, P., Padmanabhan, B., & Viswanathan, S. (2023). Building digital resilience against major shocks. *MIS quarterly*, *47*(1), 343-360.

DIVD-CSIRT. (2024). DIVD-2024-00011 - Six Vulnerabilities in Enphase IQ Gateway Devices.

Doctor, E., Eymann, T., Fürstenau, D., Gersch, M., Hall, K., Kauffmann, A. L., Schulte-Althoff, M., Schlieter, H., Stark, J., & Wyrtki, K. (2023). A maturity model for assessing the digitalization of public health agencies: Development and evaluation. *Business & Information Systems Engineering*, *65*(5), 539-554.

Dzandu, M. D., Cesare, S. D., Evans, R., & Tang, Y. (2024, 15-18 Dec. 2024). Mitigating Pandemics Through the Adaptation of Digital Technologies – Towards a Digital Resilience Framework. 2024 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM),

Fernandes, A., Mira da Silva, M., & Pereira, R. (2023). Digital Resilience in Critical Infrastructures: A Systematic Literature Review. In M. M. d. S. A. R. da Silva, J. Estima, C. Barry, M. Lang, H. Linger, & C. Schneider (Ed.), *Information Systems Development, Organizational Aspects and Societal Trends* Instituto Superior Técnico.

Fleron, B., Pries-Heje, J., & Baskerville, R. (2021). Digital organizational resilience: A history of Denmark as a most digitalized country. Proceedings of the Annual Hawaii International Conference on System Sciences,

Fleron, B., Pries-Heje, J., & Baskerville, R. (2022). Becoming a most digitalized country: a history of digital organizational resilience in Denmark. *Communications of the Association for Information Systems*, *51*(1), 16.

Garcia-Perez, A., & Sallos, M. P. (2023). Knowledge Management, Digital Transformation and the Resilience of the Firm. In *Knowledge Management and Organizational Learning* (Vol. 12, pp. 205-223). https://doi.org/10.1007/978-3-031-38696-1_11

Garcia-Perez, A., Sallos, M. P., & Tiwasing, P. (2023). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective [Article]. *Journal of Intellectual Capital*, *24*(2), 465-486. https://doi.org/10.1108/JIC-06-2021-0166

Gevers, V. (2024). From Sun to Sabotage. *Medium*.

Gooding, K., Bertone, M. P., Loffreda, G., & Witter, S. (2022). How can we strengthen partnership and coordination for health system emergency preparedness and response? Findings from a synthesis of experience across countries facing shocks [Article]. *BMC Health Services Research*, *22*(1), Article 1441. https://doi.org/10.1186/s12913-022-08859-6

Holling, C. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, *4*(1), 1-23.

Itzhak, A., & Ferri, U. (2023). Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem [Review]. *International Journal of Critical Infrastructure Protection*, *43*, Article 100637. https://doi.org/10.1016/j.ijcip.2023.100637

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Information and software technology*, *51*(1), 7-15.

Kohn, V. (2020). *How the coronavirus pandemic affects the digital resilience of employees* ICIS Conference,

Kohn, V. (2023). *Operationalizing digital resilience–A systematic literature review on opportunities and challenges* The Proceedings of the 58th HICSS Conference,

Lee, J. Y. H., Chou, C. Y., Chang, H. L., & Hsu, C. (2024). Building digital resilience against crises: The case of Taiwan's COVID-19 pandemic management [Article]. *Information Systems Journal*, *34*(1), 39-79. https://doi.org/10.1111/isj.12471

Li, X., Kotlarsky, J., & Myers, M. (2024). *Expect the Unexpected: Digital Resilience During Disasters* ICIS 2024 Proceedings,

Lin, J., & Tao, J. (2024). Digital resilience: A multiple case study of Taobao village in rural China [Article]. *Telematics and Informatics*, *86*, Article 102072. https://doi.org/10.1016/j.tele.2023.102072

Lindström, N. B., Razmerita, L., Prokopenko, S., & Popovich, N. (2024). Building Digital Resilience in Major Shocks: How Ukrainian Organizations Enact Digital Transformation in Times of War. Proceedings of the Annual Hawaii International Conference on System Sciences,

Magutshwa, S., & Radianti, J. (2022). Is this Digital Resilience? Insights from Adaptation and Exaptation of a Cyber-Physical-Social System. Proceedings of the Annual Hawaii International Conference on System Sciences,

Mahmood, S., Chadhar, M., & Firmin, S. (2024). Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector [Article]. *Journal of Contingencies and Crisis Management*, *32*(1), Article e12549. https://doi.org/10.1111/1468-5973.12549

Manyena, S. B. (2006). The concept of resilience revisited. *Disasters*, *30*(4), 434-450.

Marana, P., Eden, C., Eriksson, H., Grimes, C., Hernantes, J., Howick, S., Labaka, L., Latinos, V., Lindner, R., & Majchrzak, T. A. (2019). Towards a resilience management guideline—Cities as a starting point for societal resilience. *Sustainable Cities and Society*, *48*, 101531.

Neumannova, A., Bernroider, E., & Obwegeser, N. (2023a). *Digital Operational Resilience: The Role of Non-routine Responses in Crisis Situations* ECIS 2023.

Neumannova, A., Bernroider, E. W., & Obwegeser, N. (2023b). Conceptualizing Digital Resilience: An Intellectual Capital Perspective.

Pan, J., Lu, A., & Fang, Y. (2024). From Profitability to Sociability: Digital Resilience of the Sharing Economy. 30th Americas Conference on Information Systems, AMCIS 2024,

Park, J., Son, Y., & Angst, C. M. (2023). The Value of Centralized IT in Building Resilience During Crises: Evidence from US Higher Education's Transition to Emergency Remote Teaching. *MIS quarterly*, *47*(1).

Penadés, M. C., Núñez, A. G., & Canós, J. H. (2017). From planning to resilience: The role (and value) of the emergency plan [Article]. *Technological Forecasting and Social Change*, *121*, 17-30. https://doi.org/10.1016/j.techfore.2016.12.004

Radianti, J. (2016). Towards European Dimensions of City Resilience. International Conference on Information Technology in Disaster Risk Reduction,

Radianti, J. (2024). Vision for Emergency Management: Conceptualizing Mission-Critical Ecosystems. Proceedings of the International ISCRAM Conference,

Radianti, J., & Gjøsæter, T. (2021). Metrics for Ensuring Security and Privacy of Information Sharing Platforms for Improved City Resilience: A Review Approach. *Research Anthology on Privatizing and Securing Data*, 911-932.

Sarker, M. N. I., Islam, M. S., Huq, M. E., Alam, G. M., & Raihan, M. L. (2020). Big data-driven disaster resilience. In *Information and Communication Technologies for Humanitarian Services* (pp. 165-185). https://www.scopus.com/inward/record.uri?eid=2-s2.0-85104430716&partnerID=40&md5=f59579b06412e9e20d3c942694c63a33

Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024). Digital Resilience: Navigating Disruption and Safeguarding Data Privacy. In *EAI/Springer Innovations in Communication and Computing* (Vol. Part F2609, pp. 1-552). https://doi.org/10.1007/978-3-031-53290-0

Sharma, M. K., Anand, N., Roopesh, B. N., & Sunil, S. (2022). Digital resilience mediates healthy use of technology [Article]. *Medico-Legal Journal*, *90*(4), 195-199. https://doi.org/10.1177/00258172211018337

Son, C., Sasangohar, F., Neville, T., Peres, S. C., & Moon, J. (2020). Investigating resilience in emergency management: An integrative review of literature [Article]. *Applied Ergonomics*, *87*, Article 103114. https://doi.org/10.1016/j.apergo.2020.103114

Spagnoletti, P., & Za, S. (2021). Digital Resilience to Normal Accidents in High-Reliability Organizations. In *Engineering the Transformation of the Enterprise: A Design Science Research Perspective* (pp. 339-353). https://doi.org/10.1007/978-3-030-84655-8_21

Tim, Y., & Leidner, D. E. (2023). Digital Resilience: A Conceptual Framework for Information Systems Research [Article]. *Journal of the Association for Information Systems*, *24*(5), 1184-1198, Article 11. https://doi.org/10.17705/1jais.00842

Toulas, B. (2023). Hackers breach US water facility via exposed Unitronics PLCs. https://www.bleepingcomputer.com/news/security/hackers-breach-us-water-facility-via-exposed-unitronics-plcs/

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii-xxiii.

Zhang, Y., & Wang, F. (2024). Theoretical Connotation and Improvement Path of Government Digital Resilience-A Case Study Based on the Practice of Urban Emergency Management Digital Transformation in China. International Conference on eDemocracy and eGovernment, ICEDEG,

Zighan, S. (2024). Navigating the Cyber Landscape: A Framework for Transitioning from Business Continuity to Digital Resilience. 2nd International Conference on Cyber Resilience, ICCR 2024,

Zubok, V. (2023). Assessment and improvement of digital resilience in the energy crisis caused by missile strikes. IOP Conference Series: Earth and Environmental Science,