SMEX

Navigating Fragile Frequencies:

Challenges of Building Resilient ICT Infrastructures in Sudan's Conflict Landscape

Reem Khalil

Sudan

MARIAM AL-SHAFEI

FELLOWSHIP ON TECHNOLOGY AND HUMAN RIGHTS

Acknowledgments

This research was conducted as part of the **2024 Mariam Al-Shafei Fellowship on Technology and Human Rights.** By expanding research on emerging topics within digital rights in West Asia and North Africa, SMEX's inaugural fellowship program invites new minds and voices to address issues at the heart of our internet communities.

Reem Khalil authored the report, overseeing methodology design, compilation of primary and secondary data, and composition of the final document.

Afnan Abu Yahia provided mentorship and editorial support.

Joud Hasan provided coordination within the team at SMEX.

SMEX is a nonprofit dedicated to safeguarding human rights in digital spaces across West Asia and North Africa. We advocate for safe and uncensored access to the internet, mobile services, and networked spaces for people in the region and the diaspora. Recognizing the inseparable link between digital rights and human rights, SMEX focuses on the impact of technology on fundamental freedoms.

Published in May 2025 by SMEX.

Visit www.smex.org to learn more.

This work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.

Executive Summary

This research aims to map the challenges of maintaining resilient telecommunication infrastructures in conflict zones, particularly in Sudan. These challenges include physical destruction to the infrastructure, electricity shortages, maintenance limitations, and communications blackouts, all while limiting access to humanitarian aid. The research highlights the conflict's ramifications on telecommunications and digital humanitarian efforts. As such, it is imperative to identify governance models that can effectively support and ensure the resilience of these systems. We argue that effective governance is a cornerstone of resilient ICT contexts. Conflict zones, with their unique challenges—such as volatile conditions, resource scarcity, and security risks—require corresponding governance strategies to mitigate the impacts on digital infrastructure and actively counteract the effects of conflict to ensure continuous, reliable communication networks.

To explore this topic, this study employs a qualitative method integrating qualitative data from stakeholder interviews and secondary data from relevant industry and media reports.

The study reveals that regulations reform, infrastructural decentralization, and governance structures built around adaptability are commended in sustaining telecommunications services in Sudan's conflict zones. Key findings indicate that traditional governance models, which are often rigid and centralized, fail to provide the necessary flexibility to respond to rapidly changing conditions in conflict settings.

The implications of these findings suggest a need for policymakers and ICT organizations to reevaluate existing governance structures in conflict zones. With insights for similar regions and global policy frameworks on disaster communication and humanitarian response

Dedication

To the sounds that were silenced, and to the voices we couldn’t reach because of a network outage.

To the brave people who made sure we stayed connected, to the souls we lost defending Sudan’s sovereignty.

Abbreviations and Acronyms

Abbreviation	Description
MNO	Mobile Network Operator
ISP	Internet Service Provider
TPRA	Telecommunications Post and Regulatory Authority
NIC	National Information Center
ICT	Information and Communications Technology
SAF	Sudanese Armed Forces
RSF	Rapid Support Forces
IODA	Internet Outages Detection & Analysis
EBS	Electronic Banking Services
ERRs	Emergency Response Rooms
DR	Disaster Recovery
ETC	Emergency Telecommunication Cluster

List of Figures

List of Tables

Introduction

This research explores the role of telecommunications governance in conflict zones, taking Sudan as the case study. It highlights the need for resilient information and communication technologies (ICT) that can maintain functionality during emergencies and crises. This ensures that affected communities and humanitarian organizations can communicate and receive vital information in real time.

Sudan, as a country that has been facing ongoing political instability since 2018 lacks enough research that has been conducted to address these issues. The country presents a composite case for examining the role of the telecommunications infrastructure and governance. Sudan, home to one million refugees and the second-largest refugee population in Africa after Uganda, was severely impacted by the April 2023 conflict, exacerbating existing challenges of conflict, political instability, and humanitarian crises.[1] The April conflict resulted in the forcible displacement of 11 million of the Sudanese population, 8.1 million of whom are internally displaced, making it the largest displacement crisis in the world.[2]

The failure of digital systems in conflict zones undermines communication and the effectiveness of humanitarian interventions, leaving millions of people in vulnerable positions. As such, this study explores the impacts of weak telecom infrastructure in environments where humanitarian intervention relying on such infrastructure is a necessity. Thus, this research seeks to explore the challenges of the conflict on digital infrastructures and the impact of these challenges on human rights and humanitarianism. Accordingly, the research aims to address how governance models can contribute to a more robust and effective ICT infrastructure in such environments.

This research is based on the argument that resilient telecommunication systems are underpinned by effective governance models, which are vital for ensuring that these infrastructures can withstand the challenges of conflict. However, Sudan presents distinctive challenges for digital infrastructure, requiring governance strategies that are specifically designed and tailored to adapt to and mitigate such conditions.

The value of this research lies in its potential to provide actionable insights into strengthening governance frameworks to support more resilient ICT infrastructure in conflict settings. This study's outcomes can inform best practices and policies for

[1] UNHCR, 'Sudan Crisis Explained', 14 November 2024, https://www.unrefugees.org/news/sudan-crisis-explained/.
[2] IRC, 'Crisis in Sudan: What Is Happening and How to Help', 24 October 2024, https://www.rescue.org/article/crisis-sudan-what-happening-and-how-help.

telecommunications governance in conflict settings, contributing to global dialogue on disaster resilience and humanitarian interventions. By defining the boundaries of the research within the context of Sudan, it becomes possible to focus on the particular challenges this region faces in terms of governance and digital resilience while contributing to the broader discourse on disaster communication and digital humanitarianism.

In summary, this study argues that strengthening governance models is critical for improving the functionality and resilience of ICT infrastructure and digital humanitarian platforms in conflict landscapes. It aims to contribute to the broader discourse on disaster communication strategies by offering practical recommendations to stakeholders engaged in both the telecommunications governance sector and humanitarian operations.

This paper is organized as follows: Chapter Two explores the academic and professional body of knowledge, drawing parallels from similar contexts and examining the case of Sudan's telecommunications infrastructure. Chapter Three outlines the research methodology employed in this study. Chapter Four presents the findings and insights derived from the collected data, illustrating the impact of conflict on relevant entities. Chapter Five offers recommendations based on these findings, followed by a conclusion in the final chapter..

Literature Review

National infrastructure planning should be based on national technical capabilities, service provision needs, and informed by changing demands and contextualization. Digital infrastructure is now more than ever, a critical part of any national infrastructure system. It provides a vital channel for different services and needs, particularly during crises. It is considered a fundamental for emergency response and is typically damaged during conflict, which can amount to a war crime and have significant, invoking serious humanitarian, economic, and social consequences[3].

This literature review examines academic and practical products of knowledge on the topics of telecommunication infrastructure in conflict zones and in Sudan.. The review's purpose is to identify and analyse the major challenges to maintaining digital infrastructure during conflict. The two main types of sources the review focuses on are; academic sources and cases of telecommunication resilience in conflict zones and miscellaneous digital humanitarianism sources such as news articles. The review will also include a brief history of the conflict in Sudan with specific focus on the development in the lead up to the current phase of the conflict.

Resilient telecommunications and digital humanitarianism in conflict zones

Disaster resilience is defined by the National Academy of Sciences as "the ability to plan and prepare for, absorb, recover from, and adapt to adverse events." [4] Since the definition's introduction, a number of assessment frameworks on socio-technical systems of resilience have been proposed. The definition also mentions that critical infrastructure, such as national telecommunication systems, should take into account both internal and external threats to the infrastructure system. Other frameworks similarly take the internal and external dynamics into account like anthropogenic and human caused crises such as armed conflict.

Conflicts present both external and internal threats to the telecom infrastructure. Internal threats to the infrastructure typically result from sub-system failures inside the infrastructure ecosystem. For example, cyber attacks or technical system components failing are internal threats. External threats, on the other hand, are caused by failures from outside the infrastructure ecosystem. These failures are exemplified by aircraft or drone attacks. The greatest threat to ICT infrastructure during conflict is physical

[3] Itzhak Aviv and Uri Ferri, 'Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem', *International Journal of Critical Infrastructure Protection* 43 (December 2023): 100637, https://doi.org/10.1016/j.ijcip.2023.100637.

[4] Igor Linkov and José Manuel Palma-Oliveira, eds., *Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains*, NATO Science for Peace and Security Series C: Environmental Security (Dordrecht: Springer Netherlands, 2017), https://doi.org/10.1007/978-94-024-1123-2.

destruction, which is usually caused by external threats. This includes damage to facilities, like telecommunication towers and damages reaching cables and land line topologies. Physical destruction will usually have a direct impact on the availability of telecommunication services and will likely be incredibly expensive to repair.

Yemen is a powerful example of the costs and impact of damages to telecommunication infrastructure due to armed conflict. The overall costs to the telecommunication infrastructure during the Yemeni conflict is estimated to be $4.1 billion U.S.D. as of 2020, according to the Ministry of Telecommunications and Information Technology in Sana'a. In addition to telecom infrastructure, damages to electrical infrastructure like power stations and transmission lines have significant impacts on telecommunications. This is highly evident in the case of Yemen, where the conflict has reportedly led to a reduction of telecom coverage by around 40% [5].
The physical destruction of telecom and electrical infrastructure results in internet shutdowns and communications blackouts, which are characteristically different. An internet shutdown is defined as "the intentional disruption of internet service resulting in the inaccessibility or unavailability of it affecting specific population, location, or mode of access, often to exert control over the flow of information."[6] Whereas communication blackouts are defined as either an intentional suspension of communication channels including telecoms, radio or media or an unintentional stoppage due to damaged communication infrastructure. For example, in the current Gazan genocide, Israel has enforced both an internet shutdown and communications blackouts. The continued Israeli aggression eventually led to the destruction of all the major communication networks in Gaza. As of November 2023, the connectivity rate in Gaza was at 1% leaving almost the entirety of the Gazan population with no access to any telecommunication services.[7] These quantitatively descriptive impacts are more easily identified, unlike intangible factors like regulations.

Palestine is particularly unique due to the dynamic of having the occupying entity being the telecommunications regulator, especially when the conflict between both parties is active. In such a context, their role as regulator becomes fallacious. The telecommunication system in Gaza and the West Bank, is fully under Israel's policy and

[5] Mansoor al-Bashiri, 'Impacts of the War on the Telecommunications Sector in Yemen' (Rethinking Yemens Economy Policy Brief, January 2021).
[6] AccessNow, 'Fighting Internet Shutdowns around the World', *Campaigns / #KeepItOn:* (blog), 2023, https://www.accessnow.org/campaign/keepiton/.
[7] Mais Qandeel, 'Communication Blackouts: Israeli Cyberattacks Against Civilians in Gaza', March 2024, https://opiniojuris.org/2024/03/20/communication-blackouts-israeli-cyberattacks-against-civilians-in-gaza/.

control.[8] Israel has deliberately designed and structured the infrastructure in Gaza and the West Bank over decades to maintain control over it. For example, Palestinian telecom companies, such as Paltel, are not permitted to lay their own international cables nor operate independent frequencies. Thus forcing them to rent infrastructure from Israeli firms. This gives Israel direct access to control, intercept, and manipulate all communications. One such action is shutting down all communications during active-conflict. Furthermore, Israel restricts Palestinian telecom companies from providing more modern mobile internet services. Gaza, for instance, is still limited to 2G services, while the West Bank only gained access to 3G, over a decade after it became the global standard.[9] These policies illustrate how telecom regulations are not merely infrastructural but also deeply political. They have far reaching effects, influencing digital access, economic equity, and sovereignty.

Conflicts show how warring parties can leverage access to digital resources for political gain, especially where the law is rarely enforced. Ideally, the main role of the regulator in the telecom sector is to ensure that it is working properly and that consumer and other stakeholder interests are being protected in a fair and balanced manner.[10] However, in the case of the October 2021 military coup in Sudan, the internet was repeatedly shut down in order to suppress opposition, limit public mobilization, and control the flow of information. These shutdowns allowed the ruling party to assert dominance while obstructing access to external communication and restricting public mobilization.[11] Similarly, in Myanmar, the military used internet shutdowns during its coup to stifle opposition and maintain control.[12] These actions highlight how access to digital resources is a strategic tool in conflicts, where enforcing the rule of law is often sidelined. These scenarios serve as critical examples of digital authoritarianism, where access to information through digital infrastructure is manipulated as a means of power.

---

[8] 'Disconnected: Blackouts and Disruptions to Gaza's Telecommunication Systems during Israel's Assault', *Gisha, Legal Center for Freedom of Movement*, March 2024, https://gisha.org/en/disconnected-blackouts-and-disruptions-to-gazas-telecommunication-systems-during-israels-assault/.

[9] Reem Almasri and Afnan Abu Yahia, 'Out of Coverage: How Does the Occupation Control Gaza's Communications?', 2023, https://www.7iber.com/technology/%D9%82%D8%B7%D8%B9-%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D9%88%D8%A7%D9%84%D8%A7%D8%AA%D8%B5%D8%A7%D9%84%D8%A7%D8%AA-%D8%B9%D9%86-%D8%BA%D8%B2%D8%A9/.

[10] Blackman Colin and Lara Srivastava, 'The Telecommunications Regulation Handbook' (International Bank for Reconstruction and Development, The World Bank, InfoDev, and The International Telecommunication Union, 2010).

[11] Tessa Knight and Lujain Alsedeg, 'Sudan's Precarious Information Environment and the Fight for Democracy' (Digital Forensic Research Lab (DFRLab), The Atlantic Council of the United States, 2023), https://www.atlanticcouncil.org/wp-content/uploads/2023/08/ENGLISH-Democracy-Derailed-Sudans-precarious-information-environment-2.pdf.

[12] Ben West, 'Building Redundancies in Communications Amidst Growing Threat to Telecoms', 2022, https://www.torchstoneglobal.com/growing-threat-to-telecoms/.

All of these challenges impact digital humanitarianism during conflicts. Digital humanitarianism refers to the use of digital tools and data sources to intervene from the "electronic atmosphere" during times of crisis, providing support that aids in community resilience and recovery.[13] This involves utilizing technology to respond to crises, adapt to changing needs, and strengthen post-crisis rebuilding efforts.

By creating digital channels for immediate intervention, digital humanitarianism expands humanitarian interventions beyond the traditional to include rapid-paced, data-driven insights that enhance response coordination and reach. In Lebanon, satellite imagery was utilized to illustrate the extent of the destruction wrought by the Israeli army on more than a dozen of villages in the south. This mapping occurred in the absence of any response or commentary from the Israeli army.[14] By showcasing the potential of digital tools in documenting and responding to crises, digital humanitarianism also underscores the pressing challenges that arise when deploying these technologies in conflict zones.

Digital humanitarian platforms and digital modes of humanitarian responses in conflict zones face challenges, most notably in terms of technological barriers and accessibility. Digital infrastructure in conflict-affected regions is often fragile, unreliable, or deliberately targeted, which limits the availability of internet and mobile networks. These networks are essential for platform functioning. Such infrastructure limitations hinder both data collection and dissemination, making real-time intervention even more difficult.

Accessibility also is a major issue. If local populations lack access to the necessary devices or digital literacy, difficulties will compound, leading to ineffective utilization of digital platforms. Conflicts exacerbate social inequalities. Marginalized groups have even less access to these digital tools than average, further limiting the inclusivity and reach of digital humanitarian efforts.[15] In a country like Lebanon for example, the digital infrastructure operated in a challenging environment making the accessibility challenge clear, adding to this the inequalities of the geographic distribution of network coverage.[16]

---

[13] Mark Duffield, 'The Resilience of the Ruins: Towards a Critique of Digital Humanitarianism', *Resilience International Policies, Practices and Discourses* 4, no. 3 (2016), https://doi.org/10.1080/21693293.2016.1153772.

[14] Al Jazeera, 'Satellite Images Reveal Israeli Destruction of Villages in South Lebanon', *Israel Attacks Lebanon* (blog), 2024, https://www.aljazeera.com/program/newsfeed/2024/11/3/satellite-images-reveal-israeli-destruction-of-villages-in-south-lebanon.

[15] Saman Rejali and Yannick Heiniger, 'The Role of Digital Technologies in Humanitarian Law, Policy and Action: Charting a Path Forward', *International Review of the Red Cross, Digital Technologies and War*, 2021, https://international-review.icrc.org/articles/digital-technologies-humanitarian-law-policy-action-913.

[16] Mahdi Krayem, 'Can Lebanon Access the Internet through Satellites?', 2024, https://smex.org/can-lebanon-access-the-internet-through-satellites/.

This severely limits the availability of internet and mobile networks, which are essential for digital humanitarian platforms to function.

The crucial issue, when it comes to digital humanitarianism in conflict environments, is that in the same context the traditional ways of assessment would have come short. This is because the access and certainty of information in conflict zones decreases, and as a result a more dynamic and adaptive mode of assessment needs to be adopted. In order to adapt to the continuously changing dynamics of conflict areas, a more flexible mode is required. Hence, the resilience-based management approach of infrastructure management was introduced.

According to Linkov & Palma-Oliveira, the crises or conflict that would require resilience-based management share similar common characteristics. These attributes include:
"(i) yielding unanticipated consequences of significant extent, (ii) spanning the public and private borders of authority, and (iii) they demand the transition into alternative modes where the assumptions that traditional risk-management plans are no longer valid."
All of which are present in the environments of conflict.[17] The definition also stipulates that in similar contexts of crisis, emergency coordination from private organizations as well as public authorities needs to be established in real time to create an effective response.[18]

To conclude, telecommunications infrastructure in conflict zones face significant challenges, including but not limited to, physical damage, regulatory barriers, and governance fragmentation. Such challenges disrupt essential services during crises. These disruptions hinder emergency response efforts, delay humanitarian aid delivery, and limit access to critical information for affected populations. Furthermore, the damaged digital infrastructure limits communication-dependent industries and services like telecommunications and banking. Regulatory barriers and government fragmentation will lead to limited access to services, perpetuating inequality in access. As seen in conflicts such as those in Sudan and Yemen, telecommunication breakdowns will isolate communities, preventing them from accessing essential services, which in turn will intensify social divisions and constrain humanitarian aid. Addressing these challenges requires cooperation, robust policy frameworks, and investment in conflict-resilient infrastructure.

---

[17] Linkov and Palma-Oliveira, *Resilience and Risk*.
[18] Ekundayo Shittu, Geoffrey Parker, and Nancy Mock, 'Improving Communication Resilience for Effective Disaster Relief Operations', *Environment Systems and Decisions* 38, no. 3 (September 2018): 379–97, https://doi.org/10.1007/s10669-018-9694-5.

Sudan’s 2023 ongoing war and political conflict

In 2019, the long authoritarian rule of Sudan’s Omar Al Blashir was ousted by a nation-wide peaceful revolution. Bashir’s dictatorship seized power in 1989 during his service as an officer in the Sudanese Armed Forces through a military coup. His 30 year rule oversaw most of the Sudanese Civil War, the secession of South Sudan in 2011, and the 2003 War in Darfur.

The War in Darfur, which has been condemned as a genocide against the Arab Population in the western region of Sudan, was also when the Rapid Support Forces (RSF) were born. The RSF were officially formed in 2013, by the regime of Omar al-Bashir and placed under the leadership of Mohammad Hamdan Dagalo (also known as Hemedti). The RSF are infamous for evolving from a militia group known as the Janjaweed, which was active during the War in Darfur. The Janjaweed, formally organized as the RSF, were responsible for brutal attacks across the Darfur region including but not limited to; mass displacement, sexual violence, and kidnapping. The Janjaweed group was created to serve as a government-aligned force under Sudan's National Intelligence and Security Services (NISS) and tasked with suppressing rebellions. This positioned the RSF as a paramilitary force with significant autonomy while integrated in the security apparatus. This integration into state security provided the RSF with resources and influence, which led to the expansion of their role in the national power structure.

Following the toppling of Al Bashir, the country was led by a transitional government which put the political atmosphere in an optimistic disposition desiring democratic transition. The transitional government was led by the Sovereignty Council and consisted of a military contingent, the Military Council, and a civilian contingent, the Civilian Council. Each of these contingents hold executive and legal force, respectively, as part of their representative functions. The Military Council was led by the leader of the Sudanese Armed Forces, Abdelfattah Al Burhan, with Hemedti as his deputy. Two years later, in 2021, a military coup led by the leader of the Military Council and his deputy forced the dissolution of the transitional government and left the country in political turmoil. Al Burhan acted as the de facto head of state and, along with Hemedti, was to lead the country’s democratic transition. Throughout 2022, both Al Burhan and Hemedti engaged in negotiations with civilian parties that shared power with the military council in the transitional government. The negotiations were meant to be laying the ground for an agreement that would put the country under another transitional government which would be followed by national elections. The agreement also called for the integration of the RSF into the SAF, and for both to be placed under civilian leadership. The failure of Sudan's military leaders to meet the early 2023 deadline for implementing this power-sharing agreement revealed deep tensions. In particular, it

revealed discontent with the RSF's role, its relationship with the SAF, and how both forces would integrate under a future civilian government. Over time, these events have intensified the tensions and power struggle between Al Burhan and Hemdeti, so much so that by April troops of both entities were lined by the streets of Khartoum and deployed through Sudan.[19]

On April 15th 2023, the violent conflict between the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF) erupted. The armed conflict started in the capital city Khartoum, the most populated city in the country and where the majority of public services are operated. Public services which include banking telecoms, healthcare , ministries and government institutions. The conflict later spread to other states of Sudan including those in the Darfur and Kordofan regions, and the states of Aljazeera and White Nile. Until ultimately, the conflict reached every state in the country, having varying degrees of impact. This has resulted in the world's largest displacement crisis in recent history with 11 million people being displaced as of the writing of this paper. Leaving 25.6 million, more than half of the population, in need of basic necessities.[20] Furthermore, economic entities in urban centers like Khartoum, Aljazeera and Nyala regardless of structure and size were destroyed, looted, burned or forced to close.[21] These include both public and private institutions, such as banks and telecommunications providers.

Sudan's telecom sector at a glimpse

Historically, the telecom sector in Sudan has been heavily politicized, with operating companies including influential government officials on their boards and giving the national intelligence agencies access to the telecom network data.[22] This highlights the importance of regulatory bodies in the context of conflict and security concerns of telecommunications systems.

Sudan's telecom industry as a whole, underwent significant changes during the 1990s, starting with the government ensuring telecom companies' monopoly with limited regulation. Following this, the government brought about the privatization of some national telecom operators with the induction of regulatory bodies ensuring private

[19] Center for Preventive Action, 'Civil War in Sudan', 2024, https://www.cfr.org/global-conflict-tracker/conflict/power-struggle-sudan.
[20] IRC, 'Crisis in Sudan: What Is Happening and How to Help'.
[21] IFPRI and UNDP, 'The Socioeconomic Impact of Armed Conflict on Sudanese Urban Households', November 2024, https://www.undp.org/sites/g/files/zskgke326/files/2024-11/the_socioeconomic_impact_of_armed_conflict_on_sudanese_urban_hh_0.pdf.
[22] Guido Lanfranchi, Moneera Yassien, and Ahmed ElMurtada, 'Internet Lifeline Sudan' (Netherland Institute of International Relations, Clingendael Alert, 2024), https://www.clingendael.org/sites/default/files/CA_Internet_Lifeline_Sudan_Alert_0.pdf.

companies complied with industry rules. In a second wave of liberalization, the government allowed new service providers and services (like mobile and value-added services) to be introduced to the market. This required changes to licensing and regulations. Finally, a full competition model of the telecommunication market was instituted and the regulator's role was realized, ensuring fair competition and consumer protection.[23]

When it comes to the regulatory environment of the telecoms sector in Sudan, the following describes the regulatory agencies and the dynamics at play. The overall responsibility for telecommunication policy and regulation is vested in the Ministry Telecommunications and Digital Transformation. Additionally, two other government bodies in Sudan are entrusted with different responsibilities for the ICT landscape policy and regulations. These entities are: (i) the Telecommunications and Post Regulatory Authority (TPRA) and (ii) the National Information Centre (NIC). TPRA is tasked with planning policies and regulations including regulating tariffs, licensing operators, frequency management and equipment authorizing [24]. NIC is primarily concerned with the use of ICT in government with the overall objective of expanding and managing digital transformation services and projects in the country, in addition to acting as a consulting entity for the governmental ICT-related matters.[25]

Governance in the telecommunications sector involves implementing policies, standards, and regulatory practices that ensure the lawful operation of telecom infrastructures. Telecommunications governance models vary but can typically be characterized as either centralized or decentralized approaches. Both approaches have unique structures and benefits associated with them. Centralized governance is often state-led, in which the regulatory bodies enforce strict and unified standards. This helps maintain control over national telecom assets but sometimes limits flexibility. The decentralized models are characterized by more distributed methods, often leveraging multi-stakeholder environments and regional telecom partnerships that encourage innovation and adaptability to local needs.

The Sudanese telecom sector can be described as an oligopoly with four main companies (Canar, MTN, Sudani and Zain) dominating the market. Originally, the telecommunication sector operated under unique conditions such as international sanctions and several social conflicts. Despite these shortcomings, Sudan is still considered to have a well-equipped telecommunication sector with infrastructure meeting regional standards. These include a national fiber optic backbone, wireless

[23] Colin and Srivastava, ‘The Telecommunications Regulation Handbook’.
[24] ‘The Telecommunication and Post Regulatory Authority’, Website, 2023 2018, https://tpra.gov.sd/en/english-home/.
[25] ‘The National Information Center’, 2024, https://nic.gov.sd/public/home.

fixed-line networks with limited fiber to the home connections.[26] The dial-up internet was introduced in Sudan in 1998 as a joint attempt between Sudan Telecommunications Company (SUDATEL) and the Sudan Corporation of Broadcasting and Television. In 2007, the internet service providers were upgraded to wireless 3G technologies, overcoming the 2G technology limitations that were mentioned earlier.[27]

Three Mobile Network Operators (MNOs) provide mobile-cellular and mobile broadband services in Sudan: MTN, Sudani (which is part of Sudatel that is partially owned by the state), and Zain. The main Internet Service providers (ISPs) in Sudan are Canar and Sudatel, with Sudatel owning the majority of the national backbone infrastructure when compared to Canar, creating a concentrated dependency on these actors particularly Sudatel.[28]

By the year 2022, it was reported that 91.6% of the Sudanese population had access to at least 2G connectivity. In that same year, 78.6 % had access to at least 3G connectivity and 35% had access to LTE 4G connectivity. These rates are somewhat lower when compared to 93.3%, 83.6% and 64.3% respectively for the same type of connectivity on average in Africa.[29] The figure below provides a visualization of the percentage of the Sudanese population that is covered by the mobile networks connectivity compared to the average of all African nations from 1960 to 2023.

[26] ITU, 'Sudan ICT Country Profile', 2018, https://www.itu.int/en/ITU-D/LDCs/Documents/2017/Country%20Profiles/Country%20Profile_Sudan.pdf.
[27] WFP Logistics Capacity Assessment, 'Sudan Telecommunications', 2024, https://lca.logcluster.org/34-sudan-telecommunications.
[28] Lanfranchi, Yassien, and ElMurtada, 'Internet Lifeline Sudan'.
[29] ITU DataHub, 'Sudan Population Coverage', Population Coverage, by Mobile Network Technology, 2023, https://datahub.itu.int/data/?e=SDN&i=100095&v=chart&c=1&s=19306.

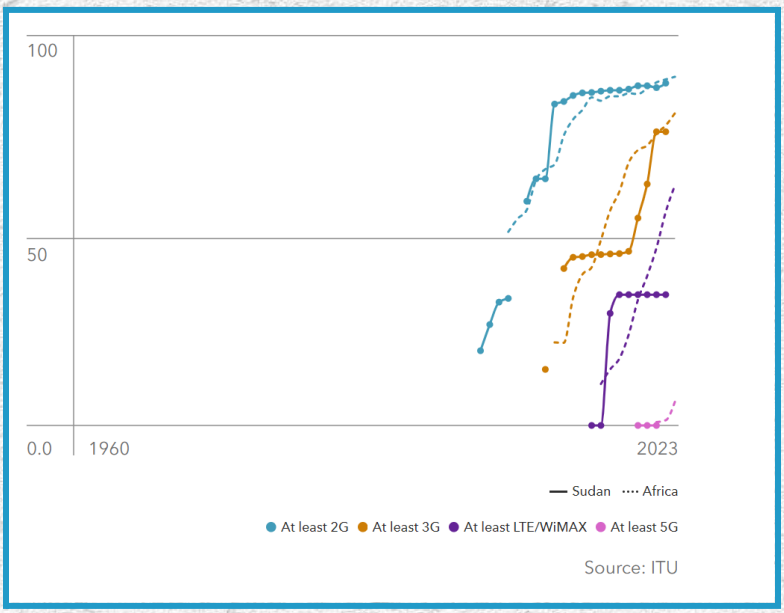


Figure 1: Percentage of the Sudanese population covered by network connectivity compared to Africa from 1960 to 2023.[30]

The number of subscribers for each MNO according to the latest published report by the Telecommunication and Post Regulatory Authority [31] is as follows:

Operator	Number of Mobile Service Subscriber (2017)
Zain	13,572,301
MTN	7,643,356
Sudani	7,428,482
Total	28,644,139

Table 1: Number of Mobile Service Subscribers per Mobile Network Operator

[30] ITU DataHub.
[31] TPRA Yearly Report, 'The Telecommunication and Post Regulatory Authority', 2017, https://tpra.gov.sd/wp-content/uploads/2023/12/annual-report-2017.pdf.

The geographic distribution of the telecom infrastructures is shown in the figure. It is adapted from data in the same report.[32]

The data demonstrates the level of telecom coverage in Sudan and the population's reliance on it. Furthermore, it briefs about the ramifications on the humanitarian situation during the conflict of 2023. It will provide the basis of the analysis findings and presentations.

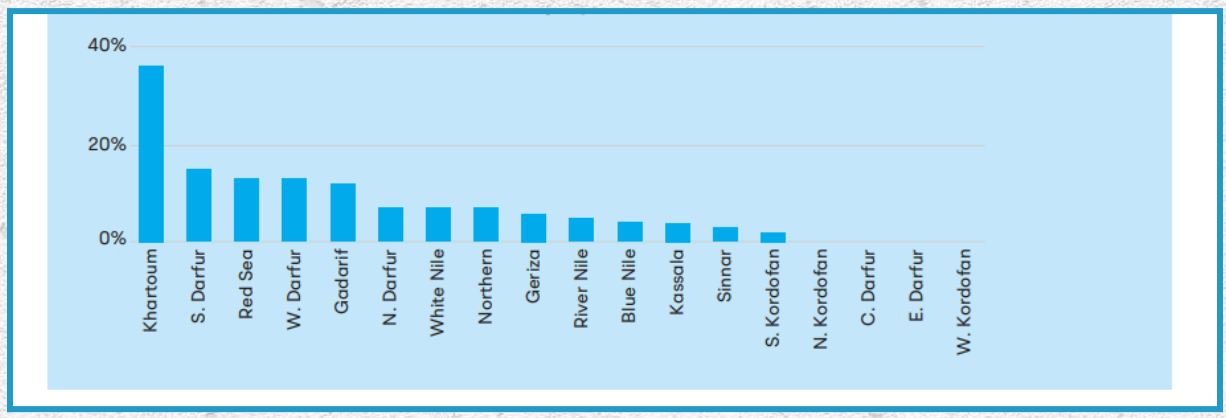


Figure 2: The percentage of network coverage in Sudan by State

Focusing on the telecom regulations scene, we can observe that the regulatory environment in Sudan complicates telecommunications management. In large part, this is due to fragmented governance and political conflicts preventing the establishment of a unified strategy for protecting and rebuilding critical infrastructure. Sudan has a history of frequent destabilizing crises and major disruptions in the telecommunications infrastructure. In addition to this, the telecommunication landscape has become heavily politicized over the last few years with government interventions resulting in telecoms blockade and internet shutdown. For example, the internet has been shut down multiple times to control and prevent the public from organizing during the Al Bashir autocracy. Moreover, internet throttling and censorship was evident during the aforementioned regime. For example, access to social media websites such as Facebook, Twitter, and Instagram was banned during the uprising against the Bashir government.[33] Likewise, the transitional military council ordered the shutdown of the internet after the dispersal of the military headquarters sit-in that was demanding full civilian rule in an attempt to cover the corresponding human rights violations.[34] Additionally, internet shutdowns were implemented in 2020 during the national exams, in 2021 during the October Military

[32] Lanfranchi, Yassien, and ElMurtada, 'Internet Lifeline Sudan'.
[33] Khattab Hamad, 'The Socio-Economic Impact of the Internet Shutdown in Sudan', n.d., https://internews.org/wp-content/uploads/2022/08/Socio-Economic-Impact-of-Shutdowns-in-Sudan.pdf.
[34] Digital Rights Lab, 'Internet Shutdowns in Sudan Allow the Bypass of Regulations', 2024, https://advox.globalvoices.org/2024/08/14/internet-shutdowns-in-sudan-allow-the-bypass-of-regulations/.

Coup, and in at least four other instances during protests in 2022.[35] All of these actions hinder the stability of communications which further erodes digital resilience.
Moreover, the significant logistical obstacles to providing telecommunications services in conflict affected regions, such as the scarcity of reliable electricity, hinder the capability to keep communication networks operational.[36] In Sudan, the telecommunications sector faces unique challenges that hinder digital resilience, particularly during periods of conflict. It is worth noting that many of the risks associated with digital infrastructure are shared among other sectors, such as the humanitarian, the financial, and energy sectors.

The cumulative effect of these increased risk factors influences the effectiveness of telecommunications and hinders the Sudanese population's ability to access essential services and reliable communication channels.

To conclude, the telecommunications infrastructure in conflict zones faces significant challenges, which include physical damage, regulatory barriers, and fragmented governance. These result in disrupted essential services during crises, and the case of Sudan currently under study is no exception. While traditional governance models struggle in these environments, adaptive approaches coupled with digital humanitarian tools offer promising solutions for building resilience.[37] The following section will explore the research design needed to examine *how effective governance models can be established to create more resilient telecommunications infrastructure and digital humanitarian platforms in conflict zones like Sudan.*

Research Design and Case Description

The theme that has clearly emerged throughout the research is that unique governance models and technological architectural settings are needed to address the distinctive challenges presented by environments of conflict.

The research is framed around a main question and a sub-question. The main question will be concerned with unravelling how to work towards more resilient telecommunications infrastructure in conflict zones. The latter will be concerned with how digital humanitarianism is affected by the deterioration in telecommunications arising from wars. It is drawn from the fact that stable connectivity is essential for digital humanitarian operations which operate extensively during emergencies. As such, answering the first part of the research question will feed into answering the second.

---

[35] Knight and Alsedeg, 'Sudan's Precarious Information Environment and the Fight for Democracy'.
[36] al-Bashiri, 'Impacts of the War on the Telecommunications Sector in Yemen'.
[37] Ekundayo Shittu, Geoffrey Parker, and Nancy Mock, 'Improving Communication Resilience for Effective Disaster Relief Operations', *Environment Systems and Decisions* 38, no. 3 (September 2018): 379–97, https://doi.org/10.1007/s10669-018-9694-5.

The research question is framed as follows:

How can effective governance models be established to create more resilient telecommunications infrastructure and digital humanitarian platforms in conflict zones like Sudan?

Consequently, the purpose of exploring this question will enable us to: (i) investigate how governance models and institutional arrangements affect the effectiveness of telecommunications and digital platforms. (ii) Contribute to model developing recommendations for fostering digital resilience strategies and governance models in conflict. (iii) Contributing to the ongoing dialogue on and informing best practices for disaster communication.

Research Design

This section will present the data collection and analysis strategy conducted during this research, and it will provide a description of the case of Sudan.

Qualitative research is the methodology adopted in this study. It is based on the understanding that unique contextualities similar to the one under investigation, requires a tailored way of exploring those contextualities. Given the nature of qualitative research that provides a way of understanding how a process unfolds giving insights into a unique phenomenon,[38] it is methodologically fit. Additionally, the framing of the research question being exploratory and open-ended provides a way to capture detailed data that can be organized into coherent stories of experience. Furthermore, a case study was chosen to identify the boundaries of the research. So while it is fixated on an event in real life, it is also enabling the controlled emphasis for a better understating. Lastly, semi-structured interviews were carried out in order to provide an insight into local voices. This provided a better understanding of experiences, systems, and practices. All of these factors make the qualitative research taking a specific case study fit for the purposes of this research.

Data Collection Strategy

Researcher-generated data was the primary data for this study and collected through semi-structured interviews. In addition, resources on the telecommunication landscape

[38] Amy C. Edmondson and Stacy E. Mcmanus, 'Methodological Fit in Management Field Research', *Academy of Management Review* 32, no. 4 (October 2007): 1246–64, https://doi.org/10.5465/amr.2007.26586086.

in Sudan were used, with a particular focus on the 2023 April conflict's impact. The following subsection will convey the particularities of each data collection strategy.

Secondary Data: Emerged from an analysis of the existing literature and academic product, the review of industry reports, concerned multilateral organizations reports and media articles. Adding to this, other related resources giving an overview of the telecommunications ecosystem in Sudan were used, including publicly available government reports and archives.

Primary Data: Semi-structured interviews were chosen to provide an intimate understanding of the particularities of telecoms and digital humanitarianism in Sudan during the conflict. Interviews blend contextual insights with a purposeful, structured, and analytical research approach to address questions.

The recruitment of interviewees followed a non-random selection which is found to be suitable given the nature of the case study having different entities and actors involved with different perspectives. The interviewees were representative of the key stakeholder groups linked to the subject matter, namely: telecommunication companies, humanitarian aid organizations, independent researchers and advisory groups in Sudan. This is to ensure a richer data set is available for analysis that covers multiple aspects to reach interview saturation.

The interview guide was developed allowing for coverage of each aspect of the research question. The interview guide was developed in English and translated into Arabic for Arabic speaking participants. It explored the existing telecommunication governance models, the challenges imposed by the 2023 conflict in Sudan, and how humanitarian aid was affected. The interviewees explored how the conflict impacted telecommunication infrastructure, the importance of establishing governance during similar conditions, and the impact on humanitarian work.

Data was collected in 6 interviews conducted by covering key actors in three groups: Telecommunication Companies in Sudan, national and international nongovernmental organizations working in direct aid and relief during the conflict, and researchers who are subject matter experts. This is detailed in Table (1) below:

Affiliation or Organization	Participant Code	Date	Number of interviews

Telecommunications Companies in Sudan	Int.Telco(1)	July 27th, 2024	2
	Int.Telco(2)	August 31st, 2024	
National and International Nongovernmental Aid Organizations	Int.NGO(1)	July 11th, 2024	2
	Int.NGO(2)	August 5th, 2024	
Researchers and Subject Matter Experts	Int.Res(1)	August 20th, 2024	2
	Int.Res(2)	August 23rd, 2024	

Table 2: Listing of interviews conducted

The duration of the interviews ranged from 15 minutes to almost an hour (53 minutes) and were conducted online via Google Meet. All interview audio was recorded after obtaining consent and saved on SMEX secure drive and transcribed. The majority were translated from Arabic (Sudanese dialect) to English, two were conducted in English and one participant preferred to answer interview guide questions in writing. Another 10 potential interview participants were approached from backgrounds in government agencies, regulatory entities, and additional telecom companies in Sudan. However, the interviews were ultimately not conducted, as some individuals either ceased responding or declined to participate.

Overall, this mixed approach of data collection is likely to enable the empirical material to develop. This is considered an important aspect in creating an improved understanding of the research.

Data Analysis Strategy

Thematic analysis was the method used by the researcher to analyze the transcripts of interviews. It is found to be methodologically fit, as it enables the research to identify patterns of meaning through the narrated data. The descriptive unit developed was a code of meaning that was found in the perspectives of participants. Codes were further grouped thematically, with each theme representing a conceptual interpretation and pattern finding in the data. This process of analysis carried out was a bottom-up approach of thematic analysis. As such, the analysis included; (i) selecting narratives related to telecommunication resilience and governance models, (ii) selecting narratives related to the challenges faced by telecommunications during conflicts and lessons learned from corresponding experience, and (iii) selecting narrative-related impacts on humanitarian operations relying on the telecoms connectivity. Table (2) provides examples of themes identified through the thematic analysis.

Stage of Analysis	Identified Themes
The telecommunication resilience and governance models	Disaster Recovery, National Emergency Response
challenges faced by telecommunications during conflicts and lessons learned from corresponding experience	Physical Infrastructure destruction, telecom employee safety, Risk management, regulatory reform
impacts on humanitarian operations relying on the telecoms connectivity	Improvised operations, Starlink internet reliance, limited and total operations blockade

Table 3: Examples of themes identified in the analysis

The following subsection called Case Description will present an overview of the telecom sector in Sudan with a lens focusing on the April 2023 Conflict's impacts on telecommunication.

Findings and Analysis

This section will present the findings discovered through the thematic analysis of the narrated data. It is organized by theme, presenting each found theme of meaning. As such, it will illustrate the challenges faced by telecom infrastructure and digital humanitarianism interventions during the conflict, as well as the impacts of conflict on the telecommunications infrastructure and Sudanese population.

Challenges Faced by Telecom Infrastructure During Conflict

1.1 Physical Destruction of the Telecom Infrastructure

The physical destruction of the telecom infrastructure is typical of aggressors because it causes rival factions to fall-behind and can be utilized in political gains for the aggressor. Physical destruction of telecom infrastructure includes but is not limited to the bombing of buildings and premises, data centers, switches and fiber cuts. A prominent officer in a telecom company in Sudan told us that:*"The first thing that*

happened at the time of the conflict is the physical damage to these areas…. The buildings were shelled and bullets entered them."

It was evident through our research that Sudan's telecoms infrastructure has faced severe physical damage, even reaching main components of the telecommunications technical ecosystem. For example, telecom towers and fiber-optic cables have been damaged due to airstrikes and ground battles. This resulted in the disruption of communication services across large parts of the country. Major cities like Khartoum and Nyala have experienced extended network blackouts, further isolating their populations.[39] Nyala, which came under RSF control in late October, and other cities of Darfur completely lost all connections following the end of hostilities. Such challenges require both technical, organizational and regulatory bolstering to ensure the availability of telecom services during conflicts.

The cable lines of telecom operators were not spared from the physical destruction. Zain, for example, had its cables destroyed by the air bombardment of the Shambat bridge that links the cities of "Omdurman and Bahri." Additionally, the cable in the area between "Mershing and Damma" north of the city of Nyala was also damaged badly.[40] This level of damage requires the presence of maintenance personnel in order to restore services.However, this was also challenged by war-specific risks.

These risks don't just threaten the physical infrastructure, but also the life and safety of tech workers who are an essential part of the telecom system. Maintenance personnel and tech workers' roles are essential to service restoration, which includes conducting repairs on damaged towers, replacing destroyed cabling, or reestablishing power supplies often using backup systems. They also deploy and configure alternative connectivity solutions, such as mobile base stations or satellite links that reconnect towers, cables and servers. One of the sources said that "it *was documented that these shells penetrated the offices where employees are usually present, so they could have caused damage to employees and human lives. There was a need to evacuate the…. employees. There was a general issue from that time until now, related to the arrival of the specialized maintenance teams and data centers and telecom teams, for the equipment, systems and services."*

In addition to the above, it was evident that maintenance personnel navigated hazardous conditions and life threatening situations during the conflict. Telecom employees had to work while being displaced and living in unstable conditions. As per

[39] Dabanga, 'War Plunges South Darfur Communications into "Medieval Abyss"', 2023, https://www.dabangasudan.org/en/all-news/article/war-plunges-south-darfur-communications-into-medieval-abyss.
[40] Dabanga.

our resource, "*Also, the employees were in a state of displacement and instability. During the displacement, not all of them had access to electricity and a network at the same time, which affected the operations. Even if one were able to work and the infrastructure was available for us to do it. There was some fluctuation in the work progress.*" Furthermore, telecom companies had personnel who lost their lives while performing their duties.

The killing and displacement of workers, coupled with the challenging working conditions, hindered the functionality of networks. There was also a significant impact on maintenance ability due to personnel needing to be physically present in the affected areas where there is active conflict. Maintenance is critical in ensuring infrastructure does not degrade and remains resilient. This is in addition to the essential and consistent upkeep, repair, configuration and upgrades of equipment and systems. A resource added: *"There were always maintenance problems because fiber cuts in conflict areas are severe with projectiles and so on."*

1.2 Electricity shortages and Access to Fuel

The conflict has caused major disruptions to the supply of electricity and fuel for backup generators, both of which are necessary for telecom data centres to function. Local supply chains of fuel were disrupted by the war, forcing reserves to be depleted. Key infrastructure such as refineries, fuel storage facilities, and transportation networks (which include pipelines and roads) has been damaged or rendered inoperable due to targeted attacks or collateral destruction. Additionally, sanctions and blockades imposed by warring factions have constrained fuel imports. These disruptions have created severe challenges for civilians. Critical services, including transportation, electricity generation, and humanitarian aid delivery are being hampered, which is exacerbating the already dire humanitarian crisis.[41]

It was evident that there were repeated country-wide electricity outages between May 2023 and March 2023. The largest outage occurred on 15 May 2023, when electricity levels in the country were brought to their lowest [42]. It is vital to have a stable and reliable back up power supply to ensure that telecommunications can operate as normal. Our resource at a telecom company in Sudan mentioned this, saying:

"There were fuel supply problems and they were not only at the headquarters, in addition to it there were fuel problems on the telecom sites (towers) and across any

[41] STPT and New Features Multimedia, 'Fueling Sudan's War How Oil Exports, Imports, and Smuggling Are Prolonging the Conflict', *Sudan Transparency And Policy Tracker*, July 2024, https://sudantransparency.org/wp-content/uploads/2024/07/FuelingSudansWarEN.pdf.

[42] Zhizhin Mikhail et al., 'Satellite Data Captures Power Outages in Sudan's Civil War', *The Payne Institute Commentary Series* (blog), May 2024, https://payneinstitute.mines.edu/satellite-data-captures-power-outages-in-sudans-civil-war/.

area where there is a dispute, whether in Khartoum or other states, the fuel supply is critical for the sites and the data centers.
Among the damages are power outages and damage to the supply of electricity for headquarters and the sites and the backup generators"

The power shortages amidst the conflict have exacerbated the communication disruptions, marking a new period of network instability. MTN, Sudan's major network, was affected by power outages in Khartoum due to fuel delivery issues, which the company confirmed in an official announcement on its platforms.[43] A telecom Engineer at Zain Sudan mentioned that "the solutions to the problems of the companies Sudani and MTN depend on saving fuel and protecting them from theft.[44]

These fuel shortages impacted people's ability to access electricity for everyday necessities. Ranging from charging phones and laptops to hindering the operations of the remaining health care centers. With the electricity grid frequently offline, many individuals turned to alternative solutions such as car batteries and small solar panels. However, these solutions were not sustainable for prolonged use. The scarcity of fuel led to a sharp increase in prices, making generators prohibitively expensive for most households. This left communities and communications reliant on inconsistent power sources, significantly reducing the ability to stay connected, access information, and maintain livelihoods. All of which compounded the hardships of living in a conflict zone.[45]

1.3 Internet shutdowns and communications blockouts

Since the onset of the 2023 conflict, Sudan has experienced several internet and communication blackouts, particularly during periods of intensified military engagements. In February 2024, all three major internet operators—Zain, MTN Sudan, and Sudani—were taken offline, resulting in a near-total communication blackout that affected over 14 million users nationwide.[46]

The durations of these shutdowns have varied, with some lasting several days to some lasting weeks. Geographically, the blackouts have been widespread, impacting both urban centers like Khartoum and remote regions. They have hindered communication

[43] MTN Sudan, 'MTN Sudan Announcement', 2023, https://www.facebook.com/mtnsudan1/posts/pfbid0S4dEQxKkXq71hNgJhYisyCgcZPZHFFuqyRpfB3eMaydYXtPV7AcSi3sR5wFncn3Bl.
[44] Dabanga, 'War Plunges South Darfur Communications into "Medieval Abyss"'.
[45] Al Rayah Al Rehima, 'Electricity Shortage Aggravates the Suffering of Sudanese Amidst the Ongoing War', October 2023, https://andariya.com/post/electricity-shortage-aggravates-the-suffering-of-sudanese-amidst-ongoing-war.
[46] Digital Rights Lab, 'Internet Shutdowns in Sudan Allow the Bypass of Regulations', 2024, https://advox.globalvoices.org/2024/08/14/internet-shutdowns-in-sudan-allow-the-bypass-of-regulations/.

and access to information across the entire country. Both sides of the conflict have been accused of deliberately disrupting communication networks to control information flow and impede the coordination of opposing forces. In some instances, the RSF have been reported to seize data centers, leading to service disruptions.[47]

The primary reasons behind these shutdowns have been linked to political motivations and pressuring the opposing party. These manifest as deliberate damage to telecoms infrastructure, purposefully constraining fuel and power supplies, and forcibly shutting down telecommunications data centres as in the aforementioned incident.

The quality of internet connections has typically returned to pre-shutdown levels when connection is restored. Restoration efforts have involved re-establishing data centers in safer regions, such as Port Sudan, to circumvent areas of active conflict. However, the exact processes and timelines for restoration have varied depending on the security situation and control over infrastructure.[48]

The table below summarizes the internet and communication disruptions in Sudan since the 2023 conflict.

Date	Responsible Party	Affected Area(s)	Duration	Reason
16th April, 2023	TPRA	All MTN Coverage	Few Hours	Orders of the government's telecommunications regulator.
23rd April, 2023	indefinite	Nation-wide	Days	indefinite
5th May, 2023	RSF	All MTN Coverage		Electricity and power supply shortages
June 2023	RSF	Khartoum, Nyala	Several days	Fuel shortages and bombing

[47] Dabanga, 'Communications Blackout Continues in Large Parts of Sudan', February 2024, https://www.dabangasudan.org/en/all-news/article/communications-blackout-continues-in-large-parts-of-sudan?utm_source=chatgpt.com.
[48] Dabanga.

Date	Responsible Party	Affected Area(s)	Duration	Reason
October 2023	Indefinite	Western Sudan	Months	Seizure of data centers
2nd, February 2024	RSF	Nation-wide	Nearly 10 days	physical control

Table 3: Major internet disruptions in Sudan in 2023–2024

In March, connectivity levels gradually returned to normal. On the 3rd of March, Zain Sudan successfully restored its services after the company established new data centers in Port Sudan City. Sudatel slowly restored connectivity as it announced a phased return to coverage across regions of Sudan in early March, which became possible by establishing new data centers in Port Sudan.[49]

1.4 Role of warring parties on internet stability

Both warring parties used internet and telecom shutdowns to strategically disrupt the flow of information in territories under the opposing party's control. This tactic worsened an already severe humanitarian crisis. The crisis has resulted in at least 13,000 deaths and the internal displacement of over eight million people, marking it as the largest internal displacement crisis in the world.[50] Through our analysis it became clear that both warring parties impacted access to communications, which is detailed as follows:

A researcher working in the field of ICT resilience in Sudan said:

"The Rapid Support Forces posted on their Twitter page that they are inside the Sudatel data centre, which is the largest data centre in East and Central Africa. It is not a simple matter. It is the one that operates government institutions and operates Bankak (A heavily relied on mobile banking application in Sudan) as the core for all of Sudan."

There have also been reports on the RSF forcing the shutdown of telecom networks. Two of the main major telecom operators, MTN and Sudani, were deemed out of service. This was due to reports confirming that RSF seized their data centres in

[49] Kassem Mnejja, 'The Sudan Conflict: How Internet Shutdowns Deepen a Humanitarian Crisis', AccessNow, 21 March 2024, https://www.accessnow.org/the-sudan-conflict-how-internet-shutdowns-deepen-a-humanitarian-crisis/.
[50] AccessNow, '#KeepItOn in Times of War: Sudan's Communications Shutdown Must Be Reversed Urgently', 2024, https://www.accessnow.org/press-release/keepiton-sudan-shutdown/.

Khartoum, resulting in internet outages in several parts of the country[51]. The seizure and shut down of data centers has also been confirmed by Reuters.[52] The outage has been confirmed by the Internet Outages Detection & Analysis (IODA).[53] In addition, a joint statement by several prominent several civil society organizations, including the Hadhreen Organization, the Sudanese American Physicians Association (SAPA), and the Strategic Initiative for Women in the Horn of Africa (SIHA Network), condemned the RSF and held them accountable for the aforementioned blackout [54]

Further destruction to telecoms equipment by the RSF has been reported by a prominent officer in the telecom industry. Reporting that RSF had sabotaged the infrastructure and switchboards of telecom companies, they said:

"In February of 2024 a shut down for the 3 telecom companies by Rapid Support. So they went to the headquarters of the telecom companies and forced them to shut down the networks."

In June 2023, the RSF took control of a telecommunication tower in eastern Khartoum, which houses multiple data centers and the National Information Center (NIC). The government spokesperson announced on their official account on Facebook that the RSF takeover led to the failure of the telecom tower and the shutdown of its website.[55]

On 16th April 2023, it was reported that MTN telecom company had been ordered by the TPRA to cut off internet access but had been restored shortly.[56] Additionally, the Sudanese Armed Forces (SAF) have reportedly been responsible for the communication blackout in the states of Darfur. [57]

Both factions have severely impacted the telecommunication services that civilian populations rely on, to varying degrees. They have repeatedly damaged telecommunications infrastructure and enforced bureaucratic obstacles, such as banning certain satellite internet devices. Shutting down internet and telecommunication

---

[51] AccessNow.
[52] Reuters, 'Sudanese Telecoms Provider MTN Restores Internet Service - MTN Official', 2023, https://www.reuters.com/article/sudan-politics-internet-idUSL1N36J071/.
[53] Internet Outages Detection & Analysis, 'Internet Connectivity for Sudan', 2024, https://ioda.inetintel.cc.gatech.edu/country/SD?from=1706448584&until=1707053384.
[54] Hadhreen Organization, SAMA, and SIHA, 'Joint Statement', 2024, https://www.linkedin.com/posts/nazim-sirag_joint-statement-we-strongly-condemn-the-activity-7161420470750167040-SOUL/.
[55] Sudan Spokesperson Platform, 2023, https://www.facebook.com/sdspokesperson/posts/pfbid033nXsQxjXxRmyPmAmCR4XDcHa3iNqwaCoEiyJKDH8JrTueG9Q8cyc4PsX8aRTxyral.
[56] Reuters, 'Sudanese Telecoms Provider MTN Restores Internet Service - MTN Official'.
[57] Digital Rights Lab, 'Internet Shutdowns in Sudan Allow the Bypass of Regulations'.

services during armed conflict is considered a crime against humanity, according to the International Criminal Court as had been ruled in 2011.[58]

Impact of conflict on telecommunication infrastructure

2.1 Blocking access to critical information and safe routes

The 2023 armed conflict has led to repeated attacks on physical assets and limited coverage and connectivity. The total effect of these factors has been significantly hindering reliable access to communication channels. which are essential during humanitarian crises. For people to flee areas of conflict, they need access to information about safe routes which the Sudanese collectively reported using social media platforms. A participant in our research shared the following:

"I have a friend who lived through this situation, he wanted to leave Khartoum, he was in Omdurman until February, at that time the bombing began, so he asked about safe paths and inspections, so when the Internet was interrupted, he no longer knew what to do, so he was afraid to go out and find any of the two forces and expose himself to danger or death, this matter even enumerates safety of civilians."

They added:
"I want to tell you one last thing. Interrupting the Internet, it affects your right to life."

The access to information about emergency services and humanitarian aid was also affected. It was clear that the internet and communication outages in Khartoum have hindered the provision of remote healthcare, particularly mental health care. This has been especially challenging as limited communication has hampered the response. This results, sometimes, with tragic consequences for survivors seeking remote psychosocial care. For example, it was reported by a doctor working in an emergency response room in Khartoum that a girl had contacted them through social media to report the rape of another girl in a poor mental state. Due to heavy armed clashes and communication disruptions, they were unable to connect with the victim immediately. Subsequent attempts to locate her were unsuccessful, and it was later confirmed that she had taken her own life[59].

---

[58] ICC Legal Tools Database, 'Decision on the "Prosecutor's Application Pursuant to Article 58 as to Muammar Mohammed Abu Minyar Gaddafi, Saif Al-Islam Gaddafi and Abdullah Al-Senussi"', 2011, https://www.legal-tools.org/doc/094165/pdf.
[59] Human Rights Watch, 'Khartoum Is Not Safe for Women Sexual Violence against Women and Girls in Sudan's Capital', 28 July 2024, https://www.hrw.org/report/2024/07/28/khartoum-not-safe-women/sexual-violence-against-women-and-girls-sudans-capital.

In February 2024, a nationwide telecommunications shutdown left nearly 30 million Sudanese cut off from internet and phone services for over a month. This prevented those facing the consequences of war from reaching their families and loved ones, deepening the isolation and hardship across the country[60]. A participant shared with us:

"I was completely isolated until I reached the borders of the country I went to… Even my family could not be reassured until I reached the borders and found a network and communicated with my family. In Sudan at that time, the network was cut off and it returned a day later, then my messages reached them."

During the nation-wide telecom shutdown, the Keep It On Coalition, a worldwide network of over 300 human rights organizations from 105 countries working to end internet shutdowns, signed a statement urging the warring parties in Sudan to immediately end the disruption of internet access across the country. It stated that internet shutdowns during wars and armed conflicts put lives at risk by blocking access to critical lifesaving information and exacerbating humanitarian emergencies[61].

2.2 Transferring money or using mobile banking

A problem with the cash supply became incredibly severe, particularly during the first days of the conflict. The issue was that cash had become concentrated in the hands of the RSF. This made internet banking a critical service for many in Sudan. The CEO of a national NGO reported that:

"This matter appeared after the communications were cut off because the cash became confined to the Rapid Support Militia in the areas under their control, especially inside the state of Khartoum"

Another contact shared their testimony saying:

"And we saw this in the shutdown [of the network] by the Rapid Support Forces in February, the country came to a complete standstill. First, there were problems with cash, most of the banknotes were stolen and it became circulating in the hands of the RSF. Most people or all people have become dependent on the Bankak application, and even if you provide the Banknote this money is very large with inflation, a person cannot carry it, as most people depend on the Bankak application, so the Bankak application stopped and thus the movement of operations stopped."

[60] NRC, 'Joint Statement: Telecommunications Blackout in Sudan' (Norwegian Refugee Council, 2024), https://www.nrc.no/news/2024/may/sudan-telecommunications-joint-statement/.
[61] AccessNow, '#KeepItOn in Times of War: Sudan's Communications Shutdown Must Be Reversed Urgently'.

Additionally, the damage and disruption to the banking sector's infrastructure -including core banking systems and hardware- have significantly hindered the delivery of financial services. For example, the Electronic Banking Service (EBS), which is the technical arm of the Central Bank of Sudan operating and hosting the national system for payment processing, had been damaged and the system stopped working in the early days of the conflict[62]. The damage to the digital infrastructure directly affected the e-banking service, as was reported to us:

"For example, among the problems in the telecom sector, was that the banking sector was [consequently] damaged. Specifically, the Bank of Khartoum (the bank operating Bankak Application) to stabilize their service which was dependent on Sudatel or Canar, so if there was a problem in the network, all the services of Bankak App stop, which is the main financial service that was available to people."

2.3 The need to find alternative Internet Sources

The instability of the network and the necessity of stable communications compelled many to find workarounds and alternative solutions during Sudan's conflict. The usage of satellite internet (Starlink) in Sudan noticeably increased during the 2023 conflict, by humanitarian organizations and the affected populations. The country director of an international NGO working on immediate relief to the displaced told us that:
"[We used] Starlink through a sort of informal way. We're having to rent locally, but I know there's some regulatory issues, still on their usage. So actually the Starlink just for some of our offices, activities in different parts of the country, for our internal communication and ICT, less so on the … or outreach."

However, the usage of Starlink was challenging due to regulatory issues and the RSF controlling access. Starlink announced in April 2024 that they would be blocking service to terminals operating in countries where they did not hold a license, including Sudan. This would have an impact on the Starlink devices that were smuggled into Sudan and were using Starlink's "roaming" feature [63]. Furthermore, TPRA has officially requested the ban of importing Starlink devices to Sudan [64]. The decision was reportedly made due to the belief that Starlink was used in the Darfur Region that is under RSF control. See Appendix (1) TPRA Letter

---

[62] Sudan Transparency and Policy Tracker, 'The Banking System During and After the War: Challenges and Policy Recommendations', The Economic Impact of the War in Sudan, 2023, https://sudantransparency.org/wp-content/uploads/2023/07/Banking-and-War.pdf.
[63] The Guardian, 'Starlink Internet Shutdown in Sudan Will Punish Millions, Elon Musk Warned', 2024, https://www.theguardian.com/global-development/article/2024/may/16/starlink-internet-shutdown-in-sudan-will-punish-millions-elon-musk-warned.
[64] Digital Rights Lab, 'Internet Shutdowns in Sudan Allow the Bypass of Regulations'.

Our source affiliated with a telecom company elaborated on this matter, saying:

"..the subscribers at the level of the nation lost communications except for a limited number that had access through land lines. And the workaround at that time through which people can access was Starlink, and at that time it was limited to certain people, for example, the army had Starlink in Omdurman after the liberation of Omdurman, for example, not an exact timing, and the Rapid Support Forces had Starlink, and in many areas there was Starlink being smuggled.
We knew people, whether on a personal level or on the level of social media, it was displayed with photos, that we have Starlink service, we can reach your family for a certain amount.
The restrictions that were imposed (by TPRA) , that Communications companies not to utilize Starlink that is smuggled which is logistically available"

Despite a government ban, devices connected to Elon Musk's Starlink satellite internet system have become increasingly common. This highlights the challenges faced by those trying to maintain connectivity amid ongoing disruptions[65]. Satellite internet was portrayed as a feasible solution in the conflict of Sudan since it does not rely on asset-heavy infrastructure on the ground, such as datacenters and telecom towers. This has in turn increased the proliferation of satellite internet devices, most notably in Darfur initially and then to other parts of the country[66].

Another alternative source of internet connectivity was emergency telecommunications. On May 25th 2023, the Emergency Telecommunications Cluster (ETC) was activated in Sudan to provide essential ICT services to emergency response humanitarian organizations. ETC is a global network, offering shared communications services during humanitarian crises. While this is considerable progress for providing network accessibility, the ETC serves limited parts of the country and humanitarian organizations working in emergency response[67]. See appendix (1) ETC Sudan Response

The role of multilateral and neutral agencies in advocating for equitable access and connectivity has remained ambiguous during the conflict in Sudan. A high ranking employee at a telecom company:

---

[65] Reuters, 'Sudanese Left in the Dark by RSF-Imposed Telecoms Blackout', February 2024, https://www.reuters.com/world/africa/sudanese-left-dark-by-rsf-imposed-telecoms-blackout-2024-02-12/.
[66] Guido Lanfranchi, Moneera Yassien, and Ahmed ElMurtada, 'Internet Lifeline Sudan' (Netherland Institute of International Relations, Clingendael Alert, 2024), https://www.clingendael.org/sites/default/files/CA_Internet_Lifeline_Sudan_Alert_0.pdf.
[67] ETC, 'Sudan Country Profile', *Emergency Telecommunications Cluster (ETC) Activities* (blog), 2024, https://www.etcluster.org/country/sudan.

“There was no support or clear directions from any party such as ITU or any other party although Sudan has membership in the ITU through TPRA. I don't recall that ITU in any platform addressed the issues of Sudan like in public platforms. There was negligence at this point”

Furthermore, alternative sources for the internet were expensive,making it accessible only to the few that can afford it. The high cost and strict import restrictions on satellite services make them inaccessible to most civilians, despite the fact it is essential for international humanitarian groups and local responders. An interviewee shared with us:

“My sister who was in PortSudan during the internet shutdown and had to use a Starlink connection in a hotel to communicate with us here in Egypt. And, it was very expensive. I think one hour was 10K then.”

Another interviewee mentioned that:

“I do not know anyone who can adapt to the internet outage easily even if they have access to internet points. Not everyone can use them because they are expensive and require the person to travel long distances. This matter consumes time and the cost of transportation in addition to the risk for the person to be in a place with an internet connection, most of these places have surveillance. So this is my testimony”

In areas controlled by the RSF, their troops utilized Starlink internet to sell access to citizens at higher prices. The RSF troops used Starlink as a source of profit, which reportedly motivated the government to ban its use[68]. However, this made it riskier for citizens to use Starlink even though it was the sole source of network connectivity in some areas.

2.4 Impact on humanitarian operations

The digital infrastructure was operated in a challenging environment, which made the accessibility challenge clear. Add to this the inequitable geographic distribution of network coverage[69], the availability of internet and mobile networks were severely limited..
The head of a national NGO told us that:

“The Internet outage caused a complete paralysis 100% for this matter (i.e. humanitarian operations). For example, at that time, we had about 25 kitchens in

[68] Lanfranchi, Yassien, and ElMurtada, ‘Internet Lifeline Sudan’.
[69] Lanfranchi, Yassien, and ElMurtada.

Khartoum State, and communication with them was completely cut off. We no longer knew anything about them.

The Internet outage led to complete paralysis. We lost communication with these kitchens, and this made people go through a very hard time until we resumed communication.

It was very disastrous because the teams could not manage anything because the money in the "Bankak" application cannot be withdrawn or transferred to cash. One cannot buy (aid materials) through Bankak because there is no Internet. This created a gap in managing materials for the kitchens. This is for us and the rest of the organizations. Even in terms of families who transferred money from outside Sudan or who receive aid through international and international organizations, it has completely stopped."

Another participant from an international NGO said:

"It's been challenging because, not only is this a major conflict, but, It's the capital city. It's also become a battle zone. That means that a lot of the national political infrastructure and social and economic infrastructure has also been extremely damaged. Telecoms are a part of that, banking systems too. So, it's really had a very deep impact on us in being able to have normal operations in this situation too amongst most other things."

They added:

"So whilst our offices can be connected with fiber optics or in some areas with 3G or 4G, and with Starlink in some places, in many parts, there's very poor connectivity for field work. So when you're out of the office, for example, around cities with displacement sites or in refugee camps or other places, it means that there are very limited ways to maintain contact with others."

The ability to connect with vulnerable communities and secure funding for essential humanitarian operations, are heavily reliant on telecommunications. Local aid groups and Emergency Response Rooms (ERRs) turn to informal Starlink connections to maintain communication[70]. Alternatively, one can travel a significant distance to get internet access or communication. The head of Hadhreen Organization told us that:

[70] NRC, 'Joint Statement: Telecommunications Blackout in Sudan'.

"The team in Omdurman was the first to make these solutions when communications started to return outside Khartoum. They would go out and travel to the city of Atbara and try to communicate with us from there. Then the needs would be raised and we would transfer them money. Then they would buy the materials and come back (to Omdurman) with them."

The necessity of network connection to humanitarian work was put by one of our research participants as:
"[The internet shutdown] was a death sentence for these central kitchens"

It was also reported that the shutdowns had also forced many ERRs to stop functioning, depriving the population of their only providers of food and health assistance [71]

2.5 Reporting and documenting casualties and human rights abuses.

Technologies like satellite imagery have been used in conflict-afflicted regions to monitor displacement patterns and assess the extent of destruction. Additionally, crowdsourced data from social media has provided real-time insights into the needs of displaced populations, and facilitated the coordination of humanitarian aid despite communication barriers[72]. However, constant network instabilities and limited communications accessibility limit this technology's application.

The main obstacles to data collection in Sudan are the restrictions on humanitarian access. Challenges such as violence, bureaucratic obstacles, logistical issues, and communication difficulties force humanitarian organizations to rely on inconsistent remote data collection methods. Unstable communication systems in conflict zones impede the implementation of humanitarian interventions and disrupt contact between communities and humanitarian actors. This instability further complicates the efforts to provide necessary support and assistance to the affected populations[73]. Mass atrocities, such as those taking place in al-Geneina, have been underreported. The same applies to ongoing atrocities in other regions, such as Al Jazirah, up until the date of writing this study.

Studies have highlighted that the scale of deaths caused by the Sudan war is likely to be significantly underreported. Research conducted by the London School of Hygiene & Tropical Medicine (LSHTM) found that over 61,000 people died of various causes in the

[71] Lanfranchi, Yassien, and ElMurtada, 'Internet Lifeline Sudan'.
[72] Tessa Knight and Lujain Alsedeg, 'Sudan's Precarious Information Environment and the Fight for Democracy' (Digital Forensic Research Lab (DFRLab), The Atlantic Council of the United States, 2023), https://www.atlanticcouncil.org/wp-content/uploads/2023/08/ENGLISH-Democracy-Derailed-Sudans-precarious-information-environment-2.pdf.
[73] USAID and iMMAP Inc.'s partners, 'Sudan Crisis Information Landscape Report', SUDAN CRISIS| Information Landscape| 19 January 2024, 2024.

state of Khartoum State within the first 14 months of the conflict, which marked a 50% increase in the pre-war death rate. Around 26,000 deaths were directly attributed to violence, surpassing the 20,178 violent deaths reported for the entire country by the Armed Conflict Location and Event Data (ACLED). This disparity is indicative of a major gap in casualty reporting, which is further compounded by the limited access to raw data and the difficulty of collecting it during the conflict. These findings highlight how fragmented reporting has masked the broader humanitarian catastrophe[74].

It is worth noting that the scale of atrocities in Sudan's conflict has been classified as war crimes. This includes the targeting of civilians through indiscriminate attacks in densely populated areas. In Darfur, the RSF and allied militias committed ethnically motivated killings, and displaced millions by targeting communities such as the Masalit ethnic group. Further starvation of civilians and widespread sexual violence were also prevalent. The RSF terrorized women and girls by committing acts of sexual violence such as rape and gang rape. Militants would attack victims in their homes, kidnap them, and target those attempting to flee across the border. [75] [76]

Moreover, the conflict severely disrupted the transmission infrastructure of the country's communication systems, including radio stations and state television, reinforcing the existing information vacuum. The RSF reportedly took over the headquarters of the Public Authority for Radio and Television to broadcast propaganda and declare supposed victories. Meanwhile, the Armed Forces seized control of Sudan TV's satellite transmission. As a result, residents turned to documenting events by themselves. However, many faced harassment, phone searches, and violence, particularly at the hands of the RSF.[77]

The underreporting of deaths and atrocities in Sudan's war undermines efforts to ensure accountability and drive meaningful change. Accurate casualty data is essential for exposing the scale of human suffering, holding perpetrators accountable, and mobilizing effective response mechanisms. The absence of reliable figures has impeded advocacy groups, humanitarian organizations, and policymakers from fully assessing the crisis and applying necessary pressure on warring parties. This gap in the data has also complicated efforts to document war crimes. The instability of telecom infrastructure, a

[74] Al Monitor, 'Sudan Conflict Deaths "Substantially Underreported": Study', 15 November 2024, https://www.al-monitor.com/originals/2024/11/sudan-conflict-deaths-substantially-underreported-study.
[75] 'Situation of Human Rights in the Sudan', Report of the United Nations High Commissioner for Human Rights, *Sudan: Horrific Violations and Abuses as Fighting Spreads - Report* (blog), 23 February 2024, https://www.ohchr.org/en/press-releases/2024/02/sudan-horrific-violations-and-abuses-fighting-spreads-report.
[76] Secretary of State Antony J. Blinken, 'War Crimes, Crimes Against Humanity, and Ethnic Cleansing Determination in Sudan', Press Statement, 6 December 2023, https://www.state.gov/war-crimes-crimes-against-humanity-and-ethnic-cleansing-determination-in-sudan.
[77] DR Lab, 'Internet and Telecom Shutdowns in Sudan: Who Is Responsible?', 8 May 2023.

key contributing factor in underreporting, highlights the importance of maintaining resilient telecom infrastructure in conflict zones.

Recommendations

A number of recommendations and proposed solutions emerged after engaging with the subject matter experts in our interviews. These recommendations can be categorized under technical, organizational, policy, and regulatory reforms.

Technical/Architectural

The proper establishment of disaster recovery (DR) sites and backup networks would ensure high availability and consistent reliability of connectivity. A well-designed disaster recovery strategy is characterized by DRs being in distant geographic locations. As such, a subnetwork is always available in the case of bombing or damages. In addition, DR sites should hold a full backup system and data back-up so that in the event of one failing, an alternative and adequate solution is already available and functioning.
Another recommendation was the decentralization of data centers and telecom operations. It was also suggested to consider the use of cloud technologies for critical services, while ensuring the development of accurate and credible resilience indices that offer metrics across various dimensions.

It is important to highlight that technical resilience specifically focuses on improving the level of resilience of infrastructure by adding redundancy, geographical isolation, and backups. However, the concept of resilience evolved into what is known as 'full spectrum resilience' which is a broader concept. This more comprehensive model of resilience includes organizational resilience (covering strategic, operational, and tactical levels of intra- and inter-organizational coordination and collaboration) and societal resilience (including the preparedness of authorities , emergency plans, business continuity plans, evacuation plans, and alternative resources.[78]

Organizational

The restructuring of entities and groups that govern and regulate telecom sector practices is essential for ensuring digital infrastructure resilience. For example, a source in the telecom sector shared that the TPRA established a committee with members from each telecom company. This committee was tasked with addressing

[78] Igor Linkov and José Manuel Palma-Oliveira, eds., *Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains*, NATO Science for Peace and Security Series C: Environmental Security (Dordrecht: Springer Netherlands, 2017), https://doi.org/10.1007/978-94-024-1123-2.

telecom sector disruptions during the conflict and developing recommendations for improved emergency governance. This initiative is invaluable as it creates a platform for real-time public-private organization coordination[79]. However, it is recommended that this committee be expanded by appointing a dedicated officer in each organization who is responsible for managing similar crisis responses to ensure coordination amongst the various stakeholders. This is related to the notion discussed earlier of making adaptations to the continuously changing flow of information in conflict areas, which requires a more flexible modality like the resilience-based approach of infrastructure management.[80]

Among the other suggested organizational reforms is the establishment of an independent entity to ensure the neutrality of telecom regulation. Such an independent legal body must guarantee adherence to the national constitution and international humanitarian laws and agreements. This would include adherence to laws related to accessibility, connectivity, and refraining from indiscriminately targeting civilian infrastructure.[81]

Policy and Regulatory

On the national level, it was found through this research that a unified national policy for disaster risk management is crucial. This national strategy must include policies and regulations focused on disaster risk management, business continuity, data classification, data retention, and backups alongside proper enforcement. As such, implementing a decentralized structure will enhance the emergency response plan and relief efforts of government agencies across all sectors and levels. This approach will also promote disaster management as a multi-sectoral effort, rather than the responsibility of a single agency.

Telecommunications companies and internet service providers must respect human rights by preventing and mitigating potential harms, while remedying any and all harms. This principle is stated in the UN Guiding Principles on Business and Human Rights[82],

---

[79] Ekundayo Shittu, Geoffrey Parker, and Nancy Mock, 'Improving Communication Resilience for Effective Disaster Relief Operations', *Environment Systems and Decisions* 38, no. 3 (September 2018): 379–97, https://doi.org/10.1007/s10669-018-9694-5.

[80] Igor Linkov and José Manuel Palma-Oliveira, eds., *Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains*, NATO Science for Peace and Security Series C: Environmental Security (Dordrecht: Springer Netherlands, 2017), https://doi.org/10.1007/978-94-024-1123-2.

[81] ICRC, 'The Principle Of Distinction', Cyber Operations During Armed Conflict, 2023, https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf.

[82] AccessNow, '#KeepItOn in Times of War: Sudan's Communications Shutdown Must Be Reversed Urgently', 2024, https://www.accessnow.org/press-release/keepiton-sudan-shutdown/.

which makes it clear that they shall take the necessary measures to avail quality and secure access to the internet and digital communication tools.

In the same vein, external entities should work on removing obstacles in the way of achieving this. One of the most important and critical aspects that experts highlighted is the safety of telecom personnel during such crises. It was revealed that telecom workers involved in site maintenance, and guarding or providing fuel to data centers were exposed to theft, harassment, and threats. Some personnel were even arrested by warring parties, according to a source in a telecommunications company in Sudan. Ensuring the safety and protection of telecom personnel, as well as granting privileged access to specific geographic areas heavily impacted by conflict during peak of attack periods must be treated with more seriousness.

It is crucial that the policies and the regulations be tailored to the context and the level of emergency, and place the interests of the Sudanese citizens as the top priority. One research participant told us:

“Our recommendation is that the National Telecommunications Authority should put the interests of the Sudanese people before narrow interests [...] What we see is that the National Telecommunications Authority shall serve the interests of the Sudanese people [...] and give authorization to Starlink to operate in Sudan.”

While this research does not specifically aim to advocate for the authorization of particular technologies, the findings lead me to recommend that regulatory frameworks consider the unique characteristics of each context. Regulations should be designed primarily to benefit citizens and address their needs effectively.

While this complex web of governance frameworks may succeed in normal operations, large-scale crisis scenarios often expose mismatches in decision-making authority and expertise, which can exacerbate negative consequences. In crises, localized failures can cascade and compound across infrastructures, cities, and states to render services unavailable. Cascading and compounding failures are typically unforeseen and therefore difficult to prepare for. These failures also have far-reaching effects that involve multiple parties that are private and public across sectors. This high level of complexity and the involvement of a wide variety of stakeholders requires all parties to coordinate and collaborate that may never have before. Existing policies and protocols for this collaboration require local expertise within horizontal governance systems to

align with bureaucratic processes, enabling information-sharing and decision-making across infrastructures and sectors.[83]

Lastly, the improvement of digital infrastructure can be incorporated further into a country's strategic plans. Coupling this with rigorous sustainability and feasibility assessments, the deep study of digital solutions that may offer alternatives to physical infrastructure assets.[84]

As for humanitarian organizations that wish to overcome these challenges, it is essential that they consider local contexts, adapt technology to low-resource settings, and work with on-the-ground stakeholders to bridge these digital divides.

The implementation of these recommendations is hindered by several key limitations. Indices and other quantitative measures have shown themselves to be limited at capturing the full impact of disasters on building-back processes, leading to a partial understanding of their long-term effects. Additionally, the absence of clear implementation guidelines can severely hinder the practical application. This can result in policies being formally recognized, but remain under-resourced, inconsistently applied, and considered secondary by relevant actors, which ultimately undermines its intended impact.

Conclusion

In conclusion, the conflict in Sudan has left a significant mark on telecommunications infrastructure, digital humanitarian efforts, and the everyday lives of civilians. The findings revealed significant damage to telecom infrastructure, disruptions in essential services like banking and emergency support, and barriers to humanitarian operations caused by communication shutdowns and infrastructure damage. Moreover, the absence of clear guidance from governmental bodies,multilateral organizations, and restrictive regulatory measures has intensified the challenges faced by affected populations.

---

[83] Blackman Colin and Lara Srivastava, 'The Telecommunications Regulation Handbook' (International Bank for Reconstruction and Development, The World Bank, InfoDev, and The International Telecommunication Union, 2010).

[84] 'Digital Infrastructure Improvements For Connectivity And Resilience In Afghanistan', GUIDING PRINCIPLE 2: RESPONSIVE, RESILIENT, AND FLEXIBLE SERVICE PROVISION (Green Policy Platform, 2021), https://www.greenpolicyplatform.org/sites/default/files/downloads/best-practices/Digital%20Infrastructure%20Improvements%20For%20Connectivity%20And%20Resilience%20In%20Afghanistan.pdf.

To address the research question on establishing resilient telecommunications infrastructure and digital humanitarian platforms in conflict zones like Sudan, this study recommends establishing decentralized disaster recovery sites, enhancing coordination between telecom providers and government agencies, and implementing context-sensitive policies. Addressing these recommendations would allow for a governance model capable of creating resilient telecom infrastructure in Sudan and similar regions, supporting uninterrupted digital humanitarianism despite the challenges posed by conflict.

Future research could explore strategies for building resilient digital infrastructure in conflict zones, focusing on alternative connectivity solutions. Additionally, examining the role of multilateral organizations in safeguarding equitable access to digital resources during crises could provide valuable insights for improved humanitarian response.

References

AccessNow. ‘Fighting Internet Shutdowns around the World’. *Campaigns / #KeepItOn:* (blog), 2023. https://www.accessnow.org/campaign/keepiton/.

———. ‘#KeepItOn in Times of War: Sudan’s Communications Shutdown Must Be Reversed Urgently’, 2024. https://www.accessnow.org/press-release/keepiton-sudan-shutdown/.

Al Jazeera. ‘Satellite Images Reveal Israeli Destruction of Villages in South Lebanon’. *Israel Attacks Lebanon* (blog), 2024. https://www.aljazeera.com/program/newsfeed/2024/11/3/satellite-images-reveal-israeli-destruction-of-villages-in-south-lebanon.

Al Monitor. ‘Sudan Conflict Deaths “Substantially Underreported”: Study’, 15 November 2024. https://www.al-monitor.com/originals/2024/11/sudan-conflict-deaths-substantially-underreported-study.

Al Rehima, Al Rayah. ‘Electricity Shortage Aggravates the Suffering of Sudanese Amidst the Ongoing War’, October 2023. https://andariya.com/post/electricity-shortage-aggravates-the-suffering-of-sudanese-amidst-ongoing-war.

Almasri, Reem, and Afnan Abu Yahia. ‘Out of Coverage: How Does the Occupation Control Gaza’s Communications?’, 2023. https://www.7iber.com/technology/%D9%82%D8%B7%D8%B9-%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D9%88%D8%A7%D9%84%D8%A7%D8%AA%D8%B5%D8%A7%D9%84%D8%A7%D8%AA-%D8%B9%D9%86-%D8%BA%D8%B2%D8%A9/.

Antony J. Blinken, Secretary of State. ‘War Crimes, Crimes Against Humanity, and Ethnic Cleansing Determination in Sudan’. Press Statement, 6 December 2023. https://www.state.gov/war-crimes-crimes-against-humanity-and-ethnic-cleansing-determination-in-sudan.

Aviv, Itzhak, and Uri Ferri. ‘Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem’. *International Journal of Critical Infrastructure Protection* 43 (December 2023): 100637. https://doi.org/10.1016/j.ijcip.2023.100637.

Bashiri, Mansoor al-. ‘Impacts of the War on the Telecommunications Sector in Yemen’. Rethinking Yemens Economy Policy Brief, January 2021.

Center for Preventive Action. ‘Civil War in Sudan’, 2024. https://www.cfr.org/global-conflict-tracker/conflict/power-struggle-sudan.

Colin, Blackman, and Lara Srivastava. ‘The Telecommunications Regulation Handbook’. International Bank for Reconstruction and Development, The World Bank, InfoDev, and The International Telecommunication Union, 2010.

Dabanga. ‘Communications Blackout Continues in Large Parts of Sudan’, February 2024. https://www.dabangasudan.org/en/all-news/article/communications-blackout-continues-in-large-parts-of-sudan?utm_source=chatgpt.com.
———. ‘War Plunges South Darfur Communications into “Medieval Abyss”’, 2023. https://www.dabangasudan.org/en/all-news/article/war-plunges-south-darfur-communications-into-medieval-abyss.
‘Digital Infrastructure Improvements For Connectivity And Resilience In Afghanistan’. GUIDING PRINCIPLE 2: RESPONSIVE, RESILIENT, AND FLEXIBLE SERVICE PROVISION. Green Policy Platform, 2021. https://www.greenpolicyplatform.org/sites/default/files/downloads/best-practices/Digital%20Infrastructure%20Improvements%20For%20Connectivity%20And%20Resilience%20In%20Afghanistan.pdf.
Digital Rights Lab. ‘Internet Shutdowns in Sudan Allow the Bypass of Regulations’, 2024. https://advox.globalvoices.org/2024/08/14/internet-shutdowns-in-sudan-allow-the-bypass-of-regulations/.
DR Lab. ‘Internet and Telecom Shutdowns in Sudan: Who Is Responsible?’, 8 May 2023. https://smex.org/internet-and-telecom-shutdowns-in-sudan-who-is-responsible/.
Duffield, Mark. ‘The Resilience of the Ruins: Towards a Critique of Digital Humanitarianism’. *Resilience International Policies, Practices and Discourses* 4, no. 3 (2016). https://doi.org/10.1080/21693293.2016.1153772.
Edmondson, Amy C., and Stacy E. Mcmanus. ‘Methodological Fit in Management Field Research’. *Academy of Management Review* 32, no. 4 (October 2007): 1246–64. https://doi.org/10.5465/amr.2007.26586086.
ETC. ‘Sudan Country Profile’. *Emergency Telecommunications Cluster (ETC) Activities* (blog), 2024. https://www.etcluster.org/country/sudan.
Gisha, Legal Center for Freedom of Movemen. ‘Disconnected: Blackouts and Disruptions to Gaza’s Telecommunication Systems during Israel’s Assault’. March 2024. https://gisha.org/en/disconnected-blackouts-and-disruptions-to-gazas-telecommunication-systems-during-israels-assault/.
Hadhreen Organization, SAMA, and SIHA. ‘Joint Statement’, 2024. https://www.linkedin.com/posts/nazim-sirag_joint-statement-we-strongly-condemn-the-activity-7161420470750167040-SOUL/.
Hamad, Khattab. ‘The Socio-Economic Impact of the Internet Shutdown in Sudan’, n.d. https://internews.org/wp-content/uploads/2022/08/Socio-Economic-Impact-of-Shutdowns-in-Sudan.pdf.
Human Rights Watch. ‘Khartoum Is Not Safe for Women Sexual Violence against Women and Girls in Sudan’s Capital’, 28 July 2024.

https://www.hrw.org/report/2024/07/28/khartoum-not-safe-women/sexual-violence-against-women-and-girls-sudans-capital.
ICC Legal Tools Database. ‘Decision on the “Prosecutor’s Application Pursuant to Article 58 as to Muammar Mohammed Abu Minyar Gaddafi, Saif Al-Islam Gaddafi and Abdullah Al-Senussi”’, 2011. https://www.legal-tools.org/doc/094165/pdf.
ICRC. ‘The Principle Of Distinction’. Cyber Operations During Armed Conflict, 2023. https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf.
IFPRI, and UNDP. ‘The Socioeconomic Impact of Armed Conflict on Sudanese Urban Households’, November 2024. https://www.undp.org/sites/g/files/zskgke326/files/2024-11/the_socioeconomic_impact_of_armed_conflict_on_sudanese_urban_hh_0.pdf.
Internet Outages Detection & Analysis. ‘Internet Connectivity for Sudan’, 2024. https://ioda.inetintel.cc.gatech.edu/country/SD?from=1706448584&until=1707053384.
IRC. ‘Crisis in Sudan: What Is Happening and How to Help’, 24 October 2024. https://www.rescue.org/article/crisis-sudan-what-happening-and-how-help.
ITU. ‘Sudan ICT Country Profile’, 2018. https://www.itu.int/en/ITU-D/LDCs/Documents/2017/Country%20Profiles/Country%20Profile_Sudan.pdf.
ITU DataHub. ‘Sudan Population Coverage’. Population Coverage, by Mobile Network Technology, 2023. https://datahub.itu.int/data/?e=SDN&i=100095&v=chart&c=1&s=19306.
Knight, Tessa, and Lujain Alsedeg. ‘Sudan’s Precarious Information Environment and the Fight for Democracy’. Digital Forensic Research Lab (DFRLab), The Atlantic Council of the United States, 2023. https://www.atlanticcouncil.org/wp-content/uploads/2023/08/ENGLISH-Democracy-Derailed-Sudans-precarious-information-environment-2.pdf.
Krayem, Mahdi. ‘Can Lebanon Access the Internet through Satellites?’, 2024. https://smex.org/can-lebanon-access-the-internet-through-satellites/.
Lanfranchi, Guido, Moneera Yassien, and Ahmed ElMurtada. ‘Internet Lifeline Sudan’. Netherland Institute of International Relations, Clingendael Alert, 2024. https://www.clingendael.org/sites/default/files/CA_Internet_Lifeline_Sudan_Alert_0.pdf.
Linkov, Igor, and José Manuel Palma-Oliveira, eds. *Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains*. NATO Science for Peace and Security Series C: Environmental Security. Dordrecht: Springer Netherlands, 2017. https://doi.org/10.1007/978-94-024-1123-2.
Logistics Capacity Assessment, WFP. ‘Sudan Telecommunications’, 2024. https://lca.logcluster.org/34-sudan-telecommunications.
Mikhail, Zhizhin, Bazilian Morgan, Elvidge Christopher, and Ziv Kristin. ‘Satellite Data Captures Power Outages in Sudan’s Civil War’. *The Payne Institute Commentary Series* (blog), May 2024.

https://payneinstitute.mines.edu/satellite-data-captures-power-outages-in-sudans-civil-war/.
Mnejja, Kassem. ‘The Sudan Conflict: How Internet Shutdowns Deepen a Humanitarian Crisis’. AccessNow, 21 March 2024. https://www.accessnow.org/the-sudan-conflict-how-internet-shutdowns-deepen-a-humanitarian-crisis/.
MTN Sudan. ‘MTN Sudan Announcement’, 2023. https://www.facebook.com/mtnsudan1/posts/pfbid0S4dEQxKkXq71hNgJhYisyCgcZPZHFFuqyRpfB3eMaydYXtPV7AcSi3sR5wFncn3Bl.
NRC. ‘Joint Statement: Telecommunications Blackout in Sudan’. Norwegian Refugee Council, 2024. https://www.nrc.no/news/2024/may/sudan-telecommunications-joint-statement/.
Qandeel, Mais. ‘Communication Blackouts: Israeli Cyberattacks Against Civilians in Gaza’, March 2024. https://opiniojuris.org/2024/03/20/communication-blackouts-israeli-cyberattacks-against-civilians-in-gaza/.
Rejali, Saman, and Yannick Heiniger. ‘The Role of Digital Technologies in Humanitarian Law, Policy and Action: Charting a Path Forward’. *International Review of the Red Cross, Digital Technologies and War*, 2021. https://international-review.icrc.org/articles/digital-technologies-humanitarian-law-policy-action-913.
Reuters. ‘Sudanese Left in the Dark by RSF-Imposed Telecoms Blackout’, February 2024. https://www.reuters.com/world/africa/sudanese-left-dark-by-rsf-imposed-telecoms-blackout-2024-02-12/.
———. ‘Sudanese Telecoms Provider MTN Restores Internet Service - MTN Official’, 2023. https://www.reuters.com/article/sudan-politics-internet-idUSL1N36J071/.
Shittu, Ekundayo, Geoffrey Parker, and Nancy Mock. ‘Improving Communication Resilience for Effective Disaster Relief Operations’. *Environment Systems and Decisions* 38, no. 3 (September 2018): 379–97. https://doi.org/10.1007/s10669-018-9694-5.
STPT, and New Features Multimedia. ‘Fueling Sudan’s War How Oil Exports, Imports, and Smuggling Are Prolonging the Conflict’. *Sudan Transparency And Policy Tracker*, July 2024. https://sudantransparency.org/wp-content/uploads/2024/07/FuelingSudansWarEN.pdf.
Sudan: Horrific violations and abuses as fighting spreads - report. ‘Situation of Human Rights in the Sudan’. Report of the United Nations High Commissioner for Human Rights, 23 February 2024. https://www.ohchr.org/en/press-releases/2024/02/sudan-horrific-violations-and-abuses-fighting-spreads-report.

Sudan Spokesperson Platform, 2023. https://www.facebook.com/sdspokesperson/posts/pfbid033nXsQxjXxRmyPmAmCR4XDcHa3iNqwaCoEiyJKDH8JrTueG9Q8cyc4PsX8aRTxyral.
Sudan Transparency and Policy Tracker. ‘The Banking System During and After the War: Challenges and Policy Recommendations’. The Economic Impact of the War in Sudan, 2023. https://sudantransparency.org/wp-content/uploads/2023/07/Banking-and-War.pdf.
The Guardian. ‘Starlink Internet Shutdown in Sudan Will Punish Millions, Elon Musk Warned’, 2024. https://www.theguardian.com/global-development/article/2024/may/16/starlink-internet-shutdown-in-sudan-will-punish-millions-elon-musk-warned.
‘The National Information Center’, 2024. https://nic.gov.sd/public/home.
‘The Telecommunication and Post Regulatory Authority’. Website, 2023 2018. https://tpra.gov.sd/en/english-home/.
TPRA Yearly Report. ‘The Telecommunication and Post Regulatory Authority’, 2017. https://tpra.gov.sd/wp-content/uploads/2023/12/annual-report-2017.pdf.
UNHCR. ‘Sudan Crisis Explained’, 14 November 2024. https://www.unrefugees.org/news/sudan-crisis-explained/.
USAID, and iMMAP Inc.’s partners. ‘Sudan Crisis Information Landscape Report’. SUDAN CRISIS| Information Landscape| 19 January 2024, 2024.
West, Ben. ‘Building Redundancies in Communications Amidst Growing Threat to Telecoms’, 2022. https://www.torchstoneglobal.com/growing-threat-to-telecoms/.

Appendices

Appendix (1) - Graphs

Figure 3: Fiber Optics Topology in Sudan

Source: [85]

[85] TPRA Yearly Report, 'The Telecommunication and Post Regulatory Authority', 2017, https://tpra.gov.sd/wp-content/uploads/2023/12/annual-report-2017.pdf.

Figure 4: TPRA Starlink Devices Ban Letter.

جمهورية السودان
Republic Of The Sudan

جهاز تنظيم الاتصالات والبريد
TELECOMMUNICATIONS AND POST REGULATORY AUTHORITY

الرقم: ج ت أ ب/م ع/50/أ/3/6/ 800
التاريخ: 23 جمادى الأول 1445هـ
الموافق: 7 ديسمبر 2023

السيد/ المدير العام لقوات الشرطة

السلام عليكم ورحمة الله وبركاته

حظر استخدام أجهزة ستار لينك

المرجع:
أ. خطاب الأمين العامة لمجلس السيادة بالنمرة: م س/أ ع/51/9/23 بتاريخ 19 سبتمبر 2022

1. في البدء يهديكم جهاز تنظيم الاتصالات والبريد أطيب التحايا متمنين أن تكونوا بخير وأمن وسلام.
2. بالإشارة إلى الموضوع أعلاه وبموجب احكام المادة 18 البند (2) من قانون جهاز تنظيم الاتصالات والبريد لسنة 2018 والتي تنص على انه " لا يجوز لاي شخص حيازة محطة او اجهزة لاسلكي، او تركيبها أو استخدامها أو تشغيلها او إدارتها داخل أراضي السودان أو أجوائه أو مياهه الاقليمية أو على سفينة او طائرة مسجلة مسبقاً أو مرخصة في السودان، ما لم يحصل على ترخيص بذلك من المجلس "والمجلس مقصود به مجلس إدارة جهاز تنظيم الاتصالات والبريد.
3. بناء على مخاطبة الأمين العام لمجلس السيادة للجهاز بقرار المجلس الخاص بحظر امتلاك أجهزة ستار لينك بحسب توجيه السيد/ رئيس مجلس السيادة (المرجع (أ)) واستناداً على المادة المشار إليها أعلاه نرجو كريم تفضلكم بتنبيه جميع منسوبي قوات الشرطة بحظر امتلاك هذه الأجهزة واتخاذ ما يلزم من إجراءات لمنع تداولها واستخدامها.
4. مرفق صور لنماذج هذه الأجهزة.

ولكم وافر الشكر والتقدير،

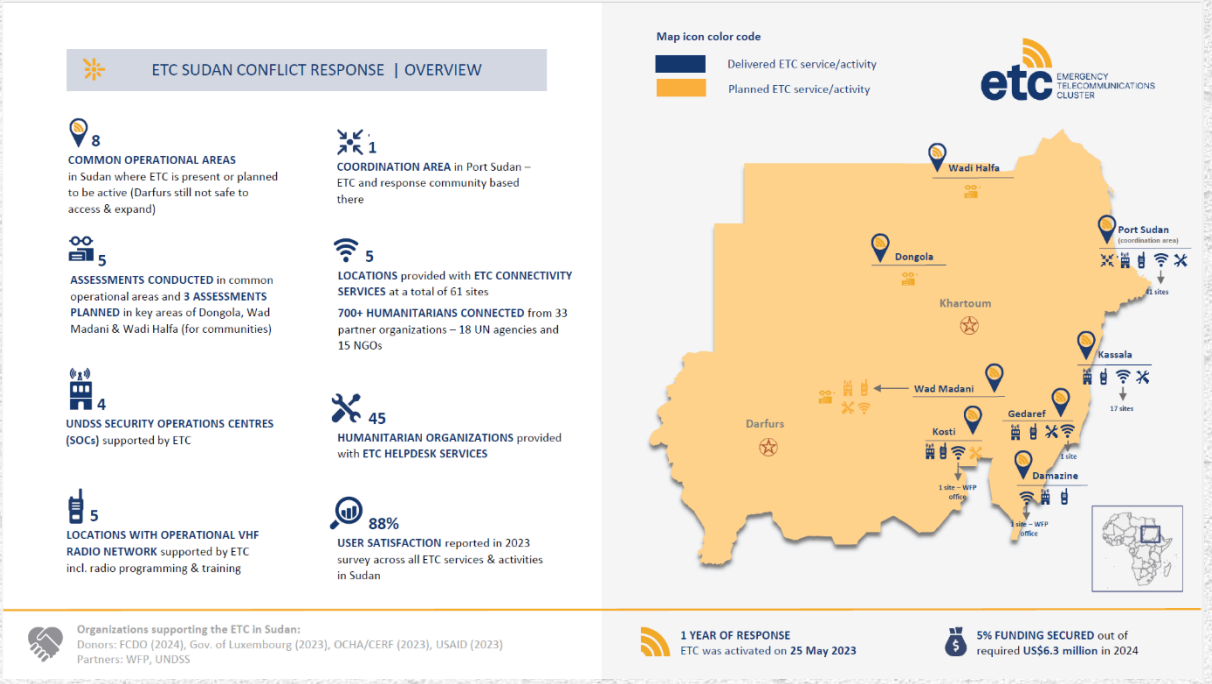
مهندس مستشار دكتور
الصادق جمال الدين الصادق
المدير العام

Khartoum - Buri - Itisalat Tower
E-Mail:itisalat@tpra.gov.sd
Web Page:www.tpra.gov.sd
el :+249 187 171144
ax :+249 183 562355
.O.Box :0869 Code:11111

الخرطوم - بري - برج الإتصالات
البريد الإلكتروني: itisalat@tpra.gov.sd
الموقع الإلكتروني: WWW.tpra.gov.sd

Figure 5: ETC Sudan Conflict Response [86]

[86] ETC, 'Sudan Country Profile', *Emergency Telecommunications Cluster (ETC) Activities* (blog), 2024, https://www.etcluster.org/country/sudan.



Appendix (2) – Interview Guide

Interview guide:

The following will be the guide for the interviews, that demonstrates the topics intended to be covered and the nature of the open-ended questions that will be asked to the interviewees

Introduce yourself and the position you hold (If you would like to)

Topic 1: Telecoms/ICT Governance

What are the governance and regulatory compliance the organization is required to comply with

How are governing framework/law are formulated, agreed upon and disseminated

To which extent were the specific organization(s) included in the formulation of such governing framework/law

What types of services shall the telecom refer back to the TPRA for

Topic 2: Challenges imposed during conflict on National ICT infrastructure

How has the conflict affected the specific organization's work

What functions/bodies the specific organization had in place prior to the conflict to handle similar disruptions, if any

What improvisations or newly emerged functions/ bodies has been created to handle these challenges

Topic 3: The Governance models' facilitation or hindering role for resilient telecom infrastructure

What support was provided by the governing bodies for the operating entities using telecom infrastructure, if any

How was the SPACEX internet service been governed by the government and how it affected the work of your organization

What restrictions were imposed provided by the governing bodies on the operating entities using telecom infrastructure, if any

What intervention from external bodies and INGO(s) did the specific organisation perceive, if any

How has the specific organization handled such interventions

What are the lessons learned and recommendations you would suggest from your experience working in your organization during the conflict to handle telecom disruption