Clingendael
Netherlands Institute of International Relations

Clingendael Alert

Guido Lanfranchi, Moneera Yassien & Ahmed Elmurtada

APRIL 2024

Internet Lifeline Sudan

Ensuring unhindered internet access is key to helping the Sudanese people survive the war

© REUTERS/El Tayeb Siddig

Starting in the early days of February, a telecommunications shutdown left almost 30 million Sudanese without access to the internet or telephone calls for several weeks.[1] Although the network has been partially restored in the east of the country, large swathes of Sudan – including the capital Khartoum – remain isolated. The large-scale shutdown in February has come on top of several network disruptions over the previous months, particularly in the western region of Darfur, which have kept millions of people isolated for months.[2] These repeated disruptions have taken place against the backdrop of a violent war between the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF), which in their reckless

1 Radio Dabanga. 2024. 'Sudan communications blackout widens amid accusations,' Radio Dabanga, 5 February, Sudan communications blackout widens amid accusations - Dabanga Radio TV Online (dabangasudan.org) (accessed 15 February 2024).

2 Radio Dabanga. 2023. 'Zain restores mobile and internet services in Darfur cities as shelling persists,' Radio Dabanga, 9 November, https://www.dabangasudan.org/en/all-news/article/zain-restores-mobile-and-internet-services-in-darfur-cities-as-shelling-persists (accessed 15 February 2024).

competition for power have dragged the whole country and its 45 million people into an abyss.

Telecommunication shutdowns have a catastrophic impact for the Sudanese people, for whom phone calls and particularly the internet have become a lifeline since the outbreak of the war in April 2023.[3] Far from being simply a tool for communication, in the current circumstances the internet has become a necessary tool for survival, enabling people to avoid armed clashes, procure food and medicines, as well as to transfer and receive money. Internet connectivity also allows the Sudanese diaspora and international aid actors to channel funds into the country, thereby providing life-saving support to millions of people in need, at a time when aid is struggling to reach them.

In this context, **all efforts should be made – inside and outside of Sudan – to ensure unhindered access to phone calls and the internet for the Sudanese population**. To this end, this Alert suggests that:

(1) Humanitarian and political **negotiations should include unhindered access to the internet as a key priority**, given the crucial role that it plays for the population;
(2) Aid actors and donor governments should **promote the availability of multiple ways of accessing the internet**, such as solutions based on **satellite and WiMAX technology**, or the use of **e-SIMs** near the country's borders;
(3) Any solution to the current crisis should also consider how to **increase the resilience of Sudan's telecom sector in the longer term**, for instance by decentralizing its infrastructure and opening up the telecom market to smaller businesses.

The crucial role of the internet in the midst of Sudan's war

Since the outbreak of the war in April 2023, the internet has been a lifeline for a large share of the Sudanese population – not only in Khartoum and in other urban areas, but also in many rural areas across the country. With armed clashes spreading across Sudan, **access to information** through the internet has become more critical than ever. The internet allows people to have access to news about their family and friends, and to retain social connections that become all the more important in times of crisis.[4] In many cases, it can also be a life-saving tool, as people regularly use it to post and receive information about where the fighting takes place or where an attack is impending. The internet is also used to map escape routes towards areas that are less affected by the war, or to share information about the requirements for crossing into neighbouring countries.

In addition, people also use the internet to **mobilize an active response to the crisis**. This includes, for instance, asking individuals to cater for specific emergencies, e.g. by bringing essential items like medicines to areas where these are most needed. In addition, at the collective level, neighbourhood-based Emergency Response Rooms (ERRs) use the internet to share information regarding the availability of basic items such as food and medicines, arrange their procurement, and ensure their distribution to those in need.

Besides granting access to information and communication, the internet also enables **access to key public services**. The issuing of passports – which are needed for people to leave the country through legal channels – is dependent on internet connectivity in Port Sudan, where SAF-controlled authorities have relocated their offices and servers. Moreover, many children and young people have come to rely on the internet to

3 Telecom networks had already played a major role in Sudan's uprising in 2018-19 (Human Rights Watch. 2019. 'Sudan: End Network Shutdown Immediately,' HRW, 12 June, https://www.hrw.org/news/2019/06/12/sudan-end-network-shutdown-immediately (accessed 15 February 2024)).

4 Göransson, M. 2018. *How smartphones help Syrian refugees in Lebanon*, CRU report, The Hague: Clingendael.

access the few online education services that are still being provided by UN agencies or by some universities – a particularly precious service in one of the largest education crises in the world, with 20 million children being unable to attend school.[5]

Perhaps most importantly, the internet allows **access to financial services**, enabling people to receive remittances and to transfer money within the country.[6] Mobile banking applications – most notably the Bank of Khartoum's *bankak*, but also other applications such as Faisal Islamic Bank's *Fawry* , MTN's *MoMo*, *Cashi* and *SyberPay* – are widely used by the Sudanese people, including in hard-to-reach areas. These apps allow people to receive money and to pay for basic needs (e.g. food, medicines, fuel), and are widely accepted for payments, even in the informal market.

The internet also represents a **key channel for aid actors and donor governments to support Sudan's population**. Avenues to provide such support continue to exist, including for instance the transfer of funds to farmers struggling to pay for the inputs needed to produce food, or to consumers who cannot afford to buy the food that is still available in the market.[7] Mobile money and mobile banking applications provide a way for donors to transfer these funds, but their functioning depends on an operational telecom network, including access to the internet.

Finally, internet access is also crucial for **accountability and justice efforts**. Brave human rights monitors and activists continue to risk their lives to document the atrocities perpetrated during the war. However, not being able to share these reports in a timely manner with the outside world means that this documentation can be lost. Saving images and videos of abuses on the phone is too risky, as warring parties target those who document their crimes.

Recurring internet shutdowns and their impact

Since April 2023, the war has had a profound impact on Sudan's telecom sector, which had already been operating for decades in a challenging environment (see Box 1). **The war's impact has varied significantly over time and across regions**. Since early on in the war, many areas of the country – particularly in Darfur – have suffered from repeated network disruptions and internet blackouts, at times enduring for months on end.[8] However, across large parts of the country – including Khartoum and central-eastern Sudan – internet services remained available for several months. This showcased the sector's resilience, the commitment of local communities and technicians to keep the infrastructure running, and potentially an understanding by the warring parties that telecom services should be preserved, even if only in their own interest. Notably, Sudan's main data centre in Khartoum, located in a conflict area, experienced no disruption for months. Continued access to the internet in many areas outside of the capital also suggests that technicians were able to carry out maintenance work and supply fuel to network towers, even in the midst of security concerns affecting transport and fuel availability.

5 UNICEF. 2023. '19 million children in Sudan out of school as conflict rages on – UNICEF, Save the Children,' UNICEF, 9 October, https://www.unicef.org/sudan/press-releases/19-million-children-sudan-out-school-conflict-rages-unicef-save-children (accessed 15 February 2024).

6 Jaspars, S. and Elkreem, T.A. 2023. 'Sudan's crisis: Can cash transfers prevent starvation and state collapse?,' *African Arguments*, 29 August, https://africanarguments.org/2023/08/sudans-crisis-can-cash-transfers-prevent-starvation-and-state-collapse/ (accessed 15 February 2024).

7 Alhag, K. et al. 2024. 'Business and aid: a role for the private sector in Sudan's humanitarian response,' The Conflict Sensitivity Facility, 15 February, https://csf-sudan.org/business-and-aid-a-role-for-the-private-sector-in-sudans-humanitarian-response/ (accessed 25 February 2024).

8 Radio Dabanga. 2023. 'Zain restores mobile and internet services in Darfur cities as shelling persists,' Radio Dabanga, 9 November, https://www.dabangasudan.org/en/all-news/article/zain-restores-mobile-and-internet-services-in-darfur-cities-as-shelling-persists (accessed 10 March 2024).

Box 1: Sudan's telecommunications sector at a glance

Already well before the war, **Sudan's telecommunications sector has traditionally operated in a unique and particularly challenging environment**, marked by international sanctions, infrastructural inequalities, market concentration, and political manipulation.

To begin with, the **sanctions regime imposed by the United States on Sudan has for a long time restricted the import of necessary technology**.[9] This has compelled the Sudanese government and telecom companies to find creative solutions to import technology, often at higher costs, thus complicating efforts to develop the sector. Nevertheless, Sudan's telecom sector has demonstrated remarkable resilience and growth, offering internet services to the population at low prices for sub-Saharan standards.[10]

Although efforts have been made to extend coverage across the country, the sector has traditionally featured **evident inequalities in the geographic distribution of infrastructure**. While Khartoum and many urban areas have benefited from a more developed network, peripheral and especially rural areas have lagged behind (see the Figures below).

Figure 1 Internet users, % of the population[11]

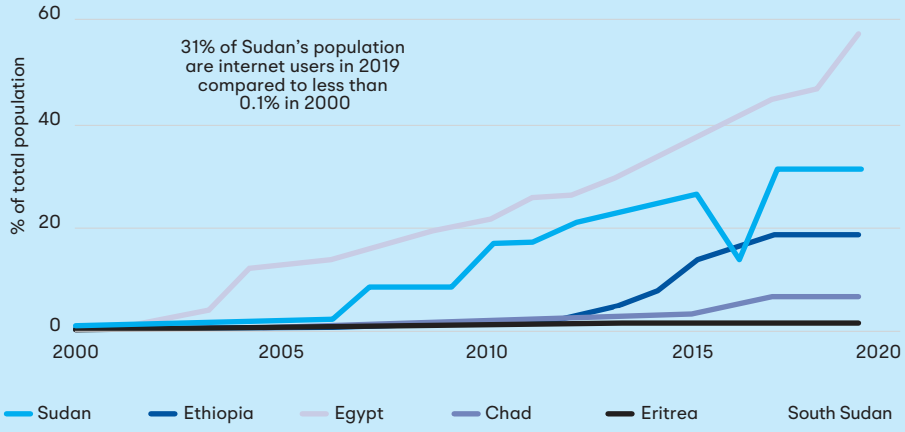
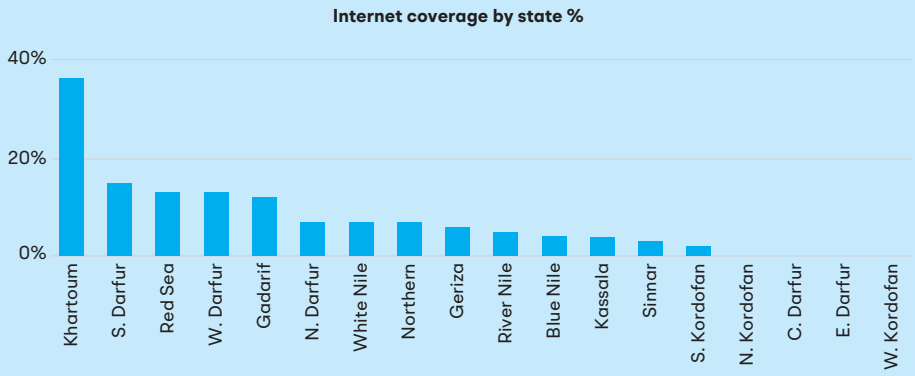


Figure 2 Internet coverage by state[12]



9 The sanctions targeted technology with more than 10% of components made in the United States. This made it very complicated for Sudanese telecom actors to import much of the critical technology normally used in the sector.

10 International Telecommunication Union. 2024. 'The affordability of ICT services 2023,' ITU, March, https://www.itu.int/en/ITU-D/Statistics/Pages/ICTprices/default.aspx (accessed 10 March 2024).

11 Source: World Bank Sudan Country Private Sector Report, May 2022.

12 Source: Telecommunications and Post Regulatory Authority (TPRA) Sudan.

From a market perspective**, Sudan's telecom sector can be characterized as an oligopoly, dominated by four companies**: Sudani (part of the Sudatel Group, a telecom conglomerate partially owned by the government), Canar (established by Emirati investments and then purchased by the Bank of Khartoum), MTN (South African), and Zain (Kuwaiti). While all four companies offer telecom services, most of the infrastructure is owned by Sudatel and (to a lesser extent) Canar, creating a strong dependency on these actors (particularly Sudatel).

Sudan's telecom sector has traditionally been heavily politicized.[13] Companies have often incorporated influential political figures onto their boards, and intelligence agencies have enjoyed access to the networks of the various telecom providers. This intertwining of business and politics has led to the manipulation of public funds. Moreover, the presence of security actors in the telecom sector has also been used to control and shrink civic space in the country, helping al-Bashir's autocratic regime to covertly monitor its citizens.[14]

Over time, however, **Sudan's generals increasingly weaponized access to the internet**. According to most reports, the large country-wide shutdown in February started when the RSF forced Sudan's main telecom providers to cut off their services, demanding the restoration of internet access for Darfur.[15] Different theories exist as to whether the network disruptions in Darfur were a result of the conflict or of deliberate sabotage by the SAF.[16] Over time, the network was partially restored – although with limited geographical coverage (mostly in the country's east) and reduced quality – thanks to the efforts of Sudani engineers, who quickly operationalised a new data centre in Port Sudan.[17] However, internet access remains weak or absent in many areas of the country, including in Khartoum and Al Jazirah.

The impact of the telecom shutdowns has been devastating.[18] In areas without a connection, people cannot be in touch with their families and friends, and hence cannot access any support networks. Unable to use their mobile banking apps, people cannot pay for their basic needs, including food. The shutdowns have also forced many ERRs to halt their activities, thus depriving the population of their only effective providers of food and health assistance.[19] The (already difficult) access to key services was halted, with online education coming to an end, and people unable to obtain their passports until the internet was restored in Port Sudan. Moreover, large-scale atrocities such as those happening in al-Geneina have for a long time

13 Hamoda, A. 2017. *Beyond Coverage, Corruption and Lack of Transparency in the Telecommunications Sector in Sudan*; Sudan Transparency Initiative.

14 For instance, the National Telecommunications Corporation has been accused of linking data SIM cards with national IDs, raising serious privacy concerns.

15 Ayin Network. 2024. 'Sudan conflict monitor #10,' Ayin Network, 17 February, https://3ayin.com/en/scm10/ (accessed 10 March 2024). The RSF has denied these accusations.

16 For instance, Zain General Manager Alfatih Arwaa has claimed in a public interview that the network's failures in Darfur were due to the inability to ensure access for engineer and fuel supplies, and that the internet was restored when the RSF eventually agreed to cooperate (Aktham. [@ragnarkov1]. 2024. 'This is the talk of Fateh Orwa about cutting the internet and he said there is no problem,' X, 8 February, https://twitter.com/ragnarkov1/status/1755682348031504537 (accessed 10 March 2024). By contrast, according to some civil society groups, the network disruptions in Darfur (as well as in Kordofan) were not due to technical problems).: Sudan comms shutdown 'ordered by army command,' Radio Dabanga, 25 February, https://www.dabangasudan.org/en/all-news/article/hadhreen-sudan-comms-shutdown-ordered-by-army-command (accessed 10 March 2024).

17 Sudan Tribune. 2024. 'Sudan's internet partially restored,' Sudan Tribune, 12 February, https://sudantribune.com/article282223/ (accessed 10 March 2024); Sudanese Affairs. 2024, 'Speech of the CEO of Sudatel Group, Eng. Magdy Mohamed Abdullah Taha, on the return of Sudani network to work,' YouTube, 13 February, https://www.youtube.com/watch?v=5jzx7olxg0M (accessed 10 March 2024).

18 Nasir, R. 2024. 'We are on the edge': Communication blackout thwarts mutual aid efforts in besieged Khartoum,' *The New Humanitarian*, 4 March, https://www.thenewhumanitarian.org/news-feature/2024/03/04/sudan-communication-blackout-mutual-aid-efforts-besieged (accessed 10 March 2024).

19 See, for instance, the case of Bahri's ERRs: Bahri Emergency Room. [@ba7riemrg]. 'Bahri Emergency Response Room Food is a right for everyone,' X, 19 February, https://twitter.com/ba7riemrg/status/1759518297614172645 (accessed 10 March 2024).

been underreported, and the same applies to ongoing atrocities currently taking place in other regions, such as Al Jazirah.[20]

Ensuring unhindered access to the internet

Given the critical, life-saving role that the internet currently plays for the Sudanese population, **ensuring unhindered internet access for as many people as possible should be a key priority for all actors** – both inside and outside of Sudan. To this end, this Alert provides the following recommendations:

(1) Prioritize access to the internet as part of any negotiation process

Almost one year into the war, there are a multitude of local, regional and international efforts aimed at addressing Sudan's crisis.[21] In mid- April, France will host a humanitarian conference for Sudan in Paris, while the United States plans to resume direct negotiations between the SAF and the RSF in Jeddah. Earlier rounds of talks in Jeddah have shown that the warring parties' commitment to ceasefires and humanitarian measures is not credible.[22] Nevertheless, **as the country's humanitarian crisis continues to deteriorate, Sudanese and international actors may be able to effectively pressure the warring parties to abide by a minimum standard of humanitarian commitments**.

Negotiation efforts – whether they concern political, military, or humanitarian issues – should **put forward the immediate restoration of access to the internet across all regions as a key priority**. When pushing for the unhindered delivery of humanitarian aid, mediators should include access to the internet in the discussions, reflecting the life-saving role that the internet plays for the population. As the warring parties' commitments cannot be trusted, mediators should push for concrete actions, such as a complete reversal of any remaining shutdowns and the restoration of damaged telecom infrastructure.

To increase pressure on the warring parties, international actors should explicitly **highlight the deliberate internet shutdowns as a denial of humanitarian aid** – and hence as a violation of international law, liable to international prosecution.[23] On the other hand, they could **frame the restoration of internet access as a way for the warring parties to gain legitimacy** among the Sudanese population, as well as towards the international community. Such a commitment would stand in stark contrast to current practices, whereby SAF and especially RSF officers have reportedly profited from the war economy.[24]

(2) Support multiple mechanisms for internet provision, including satellite connection, WiMAX, and e-SIMs

Besides pressuring the warring parties to restore the telecom services under their control, donor governments and aid actors should **support the use of multiple ways to access the internet**. These include, for instance, **satellite connection, WiMAX technology, and e-SIMs** (for a brief overview of the functioning of these mechanisms and their pros and cons, see Box 2).

20 Sudan War Monitor. 2024. 'Full Text: UN Panel of Experts Report on Sudan,' Sudan War Monitor, 23 January https://sudanwarmonitor.com/p/full-text-un-panel-of-experts-report (accessed 10 March 2024); Sudan Tribune. 2024. 'Reports emerge of alleged RSF violations in Al-Jazira State, Sudan,' Sudan Tribune, 20 February, https://sudantribune.com/article282465/ (accessed 10 March 2024).

21 These range from talks between Sudanese political and military actors, to a host of foreign-backed efforts to convene the warring parties and to address the deteriorating humanitarian crisis. See, for instance: Radio Dabanga. 2024. 'Hamdok to Dabanga: 'We are still waiting for a meeting with Sudan army leadership,'' Radio Dabanga, 21 February, https://www.dabangasudan.org/en/all-news/article/hamdok-to-dabanga-we-are-still-waiting-for-a-meeting-with-sudan-army-leadership (accessed 10 March 2024); Chughtai, A. and Murphy, T. 2023. 'Conflict and interests: Why Sudan's external mediation is a barrier to peace,' *European Council on Foreign Relations*, 8 September, https://ecfr.eu/article/conflict-and-interests-why-sudans-external-mediation-is-a-barrier-to-peace/ (accessed 10 March 2024).

22 Radio Dabanga. 2023. 'Sudan ceasefire: SAF and RSF swap accusations of violations,' Radio Dabanga, 24 May, https://www.dabangasudan.org/en/all-news/article/sudan-ceasefire-saf-and-rsf-swap-accusations-of-violations (accessed 10 March 2024).

23 Rottensteiner, C. 1999. 'The denial of humanitarian assistance as a crime under international law,' *International Review of the Red Cross*, 30 September, https://www.icrc.org/en/doc/resources/documents/article/other/57jq32.htm (accessed 10 March 2024).

24 Amin, M. 2024. 'Sudan war: Army and RSF both profiting from smuggling of vital goods,' *Middle East Eye*, 18 March, https://www.middleeasteye.net/news/sudan-war-army-rsf-profit-smuggling-food-fuel-starlink (accessed 20 March 2024).

Box 2: Alternative mechanisms for internet provision

Over the past few months, **satellite technology has emerged as the most widely used alternative** in areas cut off from the country's infrastructure network, as symbolized by Starlink's diffusion in Darfur first, and then across the country.[25] Although satellite technology comes at a very high cost, its key advantage is that it does not depend on asset-heavy infrastructure on the ground (e.g. data centres, telecom towers), which can be damaged or sabotaged in the context of the war. Rather, it only relies on the availability of receiving devices on the ground, which connect directly to the satellites. Nevertheless, this technology is still subject to capture by the warring parties. For instance, in RSF-controlled areas where the network has not been restored, RSF troops have used Starlink not only to obtain internet access for themselves, but also to sell it to citizens (often at high prices).[26] While this mechanism has enabled people to access life-saving services, it has also generated profits for the RSF soldiers. On the other hand, the RSF's use of Starlink has led the SAF to ban this technology in areas under its control, making its use riskier for people – though not uncommon. Despite its abuse by the RSF, for many Sudanese Starlink represents the only way to access the internet, meaning that any crackdown on its usage risks having a disastrous humanitarian impact. At the same time, it should be noted that Starlink is not the only available satellite solution in Sudan: Sudanese companies have been engaged in the provision of satellite services since well before the war, and some of them reportedly continue to be active in certain areas of the country.[27]

Another relevant solution is **WiMAX technology, which has the potential to extend the geographic coverage of existing infrastructure**. This technology carries wireless data over long distances (tens of kilometres), making it possible to tap into the internet in a place where it is available and making it accessible in another location. The only infrastructure required is two antennas, placed in the sending and in the receiving location respectively. The limitation of this technology is that it does not per se ensure access to the internet, but it rather relies on internet availability in the sending location. As a result, a shutdown there would result in a shutdown in the receiving location as well. Despite this limitation, WiMAX technology can still bring the internet to areas that are currently not served by the traditional infrastructure. Several Sudanese businesses were active in the implementation of WiMAX solutions already well before the war, and they could be supported so that they can continue to operate in the current circumstances.[28]

Finally, **e-SIMs have the potential to provide telecom services in the proximity of Sudan's borders**. Recently, e-SIMs have emerged as a useful solution in contexts where telecom infrastructure is damaged – as proven by their use in Gaza.[29] This solution could allow for people located close to Sudan's border (within a maximum of 40-50 km) to have access to the internet, even in cases of a blackout within Sudan. This, however, would require not only the supply of e-SIMs to people along the border, but also cooperation by the telecommunication

25 Ahram Online. 2024. 'Smuggled Starlink dishes throw lifeline to some in war-torn Sudan,' Ahram Online, 3 April, https://english.ahram.org.eg/NewsContent/26/1259/520420/War-in-Sudan/War-in-Sudan/Smuggled-Starlink-dishes-throw-lifeline-to-some-in.aspx. (accessed 5 April 2024). Due to the legacy of US sanctions against Sudan, Starlink devices cannot be activated within Sudan – rather, they are usually activated elsewhere in the region and then smuggled into Sudan.

26 Amin, M. 2024. 'Sudan war: Army and RSF both profiting from smuggling of vital goods,' *Middle East Eye*, 18 March, https://www.middleeasteye.net/news/sudan-war-army-rsf-profit-smuggling-food-fuel-starlink (accessed 20 March 2024).

27 Examples include Sudasat, a joint venture between Sudatel and the Haggar Group, as well as a host of smaller businesses. These businesses usually rely on foreign satellite networks (e.g. Arabsat).

28 Examples include companies like Maxnet and Vision Valley.

29 Aly, R. 2023. 'Palestinians in Gaza using eSim cards to get around communications blackout,' *The Guardian*, 17 December, https://www.theguardian.com/world/2023/dec/17/esim-cards-internet-gaza-palestinians (accessed 10 March 2024).

authorities of Sudan's neighbours to extend as far as possible the coverage of their infrastructure. Despite its limitations, this technology could ensure coverage for the vulnerable population located close to the border – including the many people who have become trapped there while trying to find a way out of the country.[30]

Although none of these solutions is perfect by itself, an increased reliance on multiple solutions has major advantages. First of all, diversifying away from the current dependency on Sudatel's infrastructure (see Box 1) can limit the negative impact of physical damage to such infrastructure – be it as a side-effect of the fighting, or due to active targeting and sabotage. Moreover, relying on different mechanisms can broaden geographical coverage (given that different technologies are available or implementable in different locations), while also pushing down prices (particularly if the number of potential suppliers grows). In addition, this strategy can also reduce risks related to capture by the warring parties: if the SAF or the RSF shut down one mechanism or gain control thereover, the population may still have other alternatives to rely upon.

Support from international actors could take several forms. For instance, donors could provide **financial support to ensure that the costly satellite technology becomes more affordable** for the population. This model has already been pioneered in Ukraine, where the US administration has provided equipment and financial support to ensure internet access.[31] While this experience has elicited its fair share of controversies,[32] it could provide useful learning for any potential similar effort in Sudan. Critically, any such effort should be adapted to Sudan's specific context, accounting for specific risks (e.g. capture by the warring parties) and opportunities (e.g. Sudanese private sector actors already engaged in this sector).

International support for these mechanisms can benefit from **cooperation with the Sudanese private sector**. As noted earlier (see Box 2), many of these solutions have already been implemented in Sudan, including by Sudanese companies. International actors can provide support for these businesses to enable them to provide access to the internet as widely and as cheaply as possible. In addition, **Sudanese businesses may act as hubs for the distribution of internet access**. It is often easier for businesses than it is for private citizens to retain access to the internet – be it through landline connections, which are less subject to damage, or thanks to their ability to pay for and operate alternative technologies (e.g. satellite, WiMAX). International actors should provide incentives for these businesses to share internet access with the communities around

30 See, for instance, an account of the difficult situation along the border with Egypt: Alhaj, E. and Adler, N. 2023. 'Stuck in limbo: Frustration, despair at Sudan-Egypt border,' *Al-Jazeera*, 27 June, https://www.aljazeera.com/news/longform/2023/6/27/stuck-in-limbo-frustration-and-despair-on-the-sudan-egypt-border (accessed 10 March 2024).

31 USAID provided 5,000 Starlink terminals, while the Department of Defense signed a contract with SpaceX on the provision of satellite services. USAID. 2022. 'USAID safeguards internet access in Ukraine through public-private-partnership with SpaceX,' USAID, 5 April, https://www.usaid.gov/news-information/press-releases/apr-05-2022-usaid-safeguards-internet-access-ukraine-through-public-private-partnership-spacex (accessed 10 March 2024); Stone, M. and Roulette, J. 2023. 'SpaceX's Starlink wins Pentagon contract for satellite services to Ukraine,' *Reuters*, 1 June, https://www.reuters.com/business/aerospace-defense/pentagon-buys-starlink-ukraine-statement-2023-06-01/ (accessed 10 March 2024).

32 Marquardt, A. 2022. Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab,' *CNN*, 14 October, https://www.aljazeera.com/news/2024/2/13/elon-musk-denies-selling-starlink-to-russia-after-ukraine-claims-use-in-war; https://apnews.com/article/spacex-ukraine-starlink-russia-air-force-fde93d9a69d7dbd1326022ecfdbc53c2; https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html (accessed 10 March 2024); Al-Jazeera. 2024. 'Elon Musk denies selling Starlink to Russia after Ukraine claims use in war,' Al-Jazeera, 13 February, https://www.aljazeera.com/news/2024/2/13/elon-musk-denies-selling-starlink-to-russia-after-ukraine-claims-use-in-war (accessed 10 March 2024); Copp, T. 2023. 'Elon Musk's refusal to have Starlink support Ukraine attack in Crimea raises questions for Pentagon,' *AP News*, 12 September, https://apnews.com/article/spacex-ukraine-starlink-russia-air-force-fde93d9a69d7dbd1326022ecfdbc53c2 (accessed 10 March 2024).

them, wherever possible. This model was used in Khartoum during the 2018-19 protests (some businesses that had retained access to the internet during the shutdowns would open up access to people during certain times, while carefully switching it off when the police would come), and it could be implemented once again – with the necessary adaptations – in the current context.

(3) Build long-term resilience for Sudan's telecom sector

While the priority in the short term is to deliver internet access for the population, any measures undertaken to this end should also **consider how to make Sudan's telecom sector more resilient against shocks in the long term**. Most notably, the current experience during the war (see above) has shown that dependency on centralized infrastructure (e.g. a single, large data centre in Khartoum) exposes the telecom sector to major risks in case of physical damage to such infrastructure. To mitigate these risks, Sudanese and international actors should ride the wave of the current changes in Sudan's telecom sector and **push for a more decentralized infrastructure**. This could entail, for instance, building several smaller data centres around the country.

Similar changes should be adopted regarding Sudan's telecom market. So far, this market has been dominated by a few large companies, with small and medium-sized enterprises often being confined to smaller tasks (see Box 1). By contrast, **increasing the role of smaller businesses in the telecom sector** may provide several benefits – including not only lower prices for customers (if the number of suppliers increases), but also more resilience towards shocks (in case one supplier is not able to deliver its services, others may step in to replace it).

As Sudan's humanitarian crisis continues to deteriorate, no stone should be left unturned to ensure that the population has access to basic needs, such as food, healthcare, and a safe environment. In today's Sudan, **access to these needs largely depends on access to the internet** – making it a lifeline that demands immediate restoration, while also keeping in mind the longer-term needs of a post-war Sudan.

About the Clingendael Institute
Clingendael – the Netherlands Institute of International Relations – is a leading think tank and academy on international affairs. Through our analyses, training and public debate we aim to inspire and equip governments, businesses, and civil society in order to contribute to a secure, sustainable and just world.

www.clingendael.org
info@clingendael.org
+31 70 324 53 84

@clingendaelorg
The Clingendael Institute
The Clingendael Institute
clingendael_institute
Clingendael Institute
Newsletter

About the authors

Guido Lanfranchi is a research fellow at Clingendael's Conflict Research Unit (CRU). He contributes to CRU's Horn of Africa programme, focusing on Sudan, Ethiopia and Somalia. Guido's research interests revolve around the interplay between economic, political and security dynamics, with a focus on how economic interests and business elites shape governance arrangements and conflict patterns. Guido also conducts research on geopolitical dynamics in the Horn of Africa, including the engagement of various foreign powers (Russia, China, Arab Gulf states, etc.).

Moneera Yassien is a junior research fellow with the Conflict Research Unit (CRU) of Clingendael. She contributes to the work of the Horn of Africa team as an economist and data analyst. She is particularly interested in using qualitative and quantitative methods, to research the economic development in fragile states and the role of conflict and fragility in shaping the different elements of country's economic and political development. Moneera's research and analyses benefits from spending over 5 years on-ground experience in the Horn of Africa and MENA region, working with civil society, UN agencies, International organizations and Development Banks on Private Sector development, informality, and economic empowerment.

Ahmed Elmurtada is a cybersecurity engineer with over eight years of experience in Information security, Technology and Start-ups within private sector across Telecom & Fintech Sectors. Currently Managing Partner & Co Founder of 249Startups , leading Business Innovation & Development activities focusing on Business Development, Research, growth, Technology, mentorship, and access to networks and investments. With passion for bringing change through Technology.

Acknowledgements: This report would have not been possible without the financial support of the Dutch Ministry of Foreign Affairs, as well as the insightful inputs and comments from Anette Hoffmann, Jos Meester, as well as a Sudanese telecom expert who preferred to remain anonymous.