Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**914**
Land:	Sudan
Kilde:	Freedom House
Titel:	Freedom on the Net 2024 – Sudan
Udgivet:	16. oktober 2024
Optaget på baggrundsmaterialet:	7. november 2024

Freedom House

FREEDOM ON THE NET 2024

Sudan

NOT FREE

28

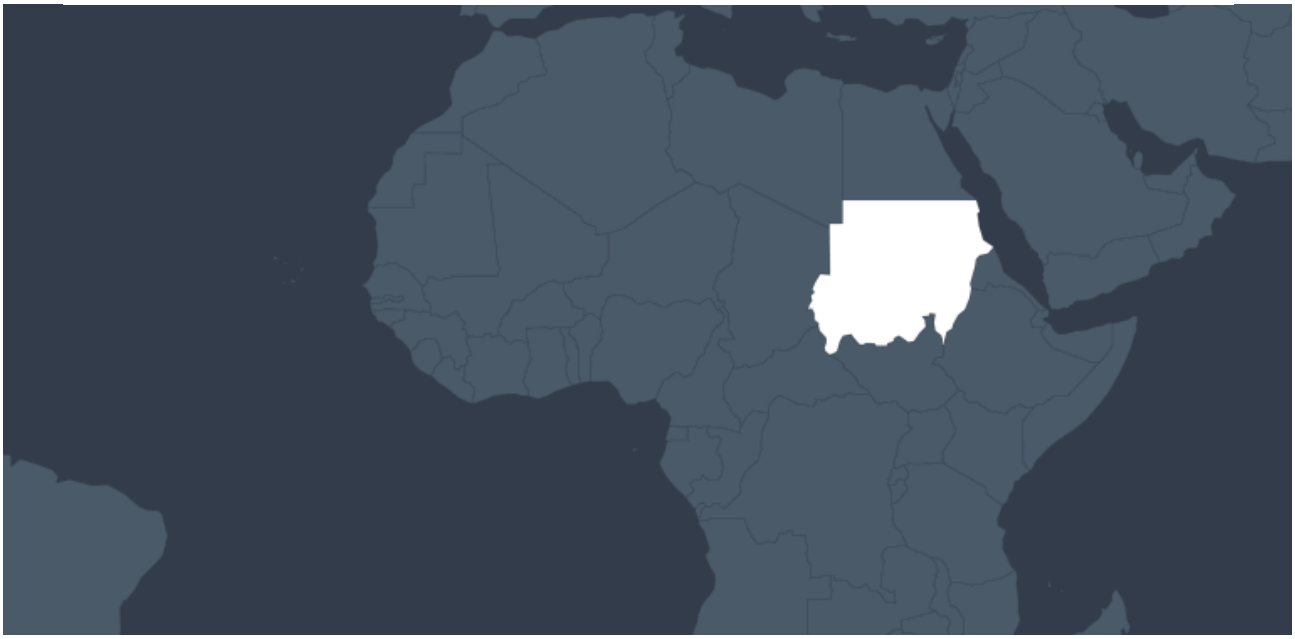
/100

A. Obstacles to Access	5 /25
B. Limits on Content	14 /35
C. Violations of User Rights	9 /40

LAST YEAR'S SCORE & STATUS

30 /100 **Not Free**

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.



Key Developments, June 1, 2023 – May 31, 2024

Internet freedom declined in Sudan, as the civil war between the paramilitary Rapid Support Forces (RSF) and the Sudanese Armed Forces (SAF) caused destruction of internet infrastructure, as well as deliberate internet disruptions that have intensified the country's humanitarian crisis, hampering the delivery of aid and preventing residents from documenting crimes against humanity that have left thousands of people dead and millions displaced. The RSF and SAF seek to manipulate online content to advance their favored narratives of the conflict, and both sides have carried out brutal crackdowns against journalists, activists, and ordinary internet users who cover the war neutrally or report on human rights abuses.

- A nationwide cut to internet access occurred in February 2024, attributed to the RSF's occupation of facilities belonging to major internet service providers (ISPs) in Khartoum. Extremely limited connectivity returned after 10 days as providers shifted their operations to Port Sudan, but service was not restored on all ISPs until May 2024 (see A3).
- Localized internet disruptions in areas of ongoing armed conflict occurred throughout the coverage period, including in Khartoum, Omdurman, and cities across the Darfur and Kordofan regions, with some shutdowns lasting months. Communications disruptions notably occurred in Darfur in November 2023 while the RSF carried out mass atrocities (see A3).
- Faced with frequent connectivity disruptions and damaged or unreliable information and communications technology (ICT) infrastructure, many in Sudan began to rely on Starlink's satellite-based service. Despite aid groups' reliance on Starlink to coordinate humanitarian responses to the civil war, the military-led government attempted to restrict the import and use of Starlink devices due to their extensive use by the RSF (see A3 and A4).
- Both the RSF and the SAF sought to spread propaganda and control the narrative of the conflict online. Networks of bot accounts on X shared pro-RSF messages, while networks of social media users supporting the SAF used inflammatory language to spread prowar messages (see B5).

- Repression of activists since the start of the civil war has sharply curtailed space for online mobilization, though grassroots volunteers continued to use digital platforms to coordinate antiwar activism and mutual aid in the face of restrictions (see B8).
- In January 2024, the military-led government and governors of SAF-controlled states issued decisions prohibiting the use of any means of communication to "disparage the prestige of the state" and state bodies. Rights organizations condemned the decisions as an effort to use the security situation to unfairly restrict freedom of expression (see C2).
- Internet users faced an increase in arbitrary arrest and physical violence, with reports of SAF and RSF combatants beating, torturing, and killing online journalists, activists, and others for their online expression (see C3 and C7).

Political Overview

After military commanders and a prodemocracy protest movement ousted the repressive regime of longtime president Omar al-Bashir and his National Congress Party (NCP) in 2019, Sudan was ruled by a transitional government in which military and civilian leaders agreed to share power until national elections could be held. The process was thrown into turmoil in late 2021 when the military leadership dissolved the transitional government in a coup and cracked down on the ensuing prodemocracy protests. In April 2023, hostilities broke out between the SAF and the RSF, a paramilitary group originally formed by al-Bashir, and the fighting quickly spread across the country. The ongoing conflict has been characterized by extreme levels of violence, including ethnic violence in Darfur, and has led to mass killings and displacement of civilians.

A. Obstacles to Access

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**1** / 6

Internet penetration in Sudan remains low, and connectivity has lacked stability since the civil war began in April 2023. Some 28.7 percent of the population—

representing 14 million people—used the internet as of February 2024 according to DataReportal's *Digital 2024* report. [1] The most recent data from the International Telecommunication Union (ITU), which dates back to 2022, places the internet penetration rate at 29 percent. [2]

According to data from Ookla, the median mobile download and upload speeds for Sudan in January 2024 were 4.82 and 3.75 Megabits per second (Mbps), respectively. Fixed-line median download and upload speeds stood at 8.67 and 7.48 Mbps. [3] ITU data showed that there were less than 30,000 fixed-line broadband connections in Sudan as of 2022. [4]

Conflict has degraded the ICT infrastructure in the country, causing data loss, irregularity in the provision of government services, and network disruptions. Electricity outages, fuel shortages, and difficulties in delivering fuel and maintaining infrastructure due to the security situation have all contributed to service interruptions. [5]

Zain's mobile internet services were inaccessible on January 8, 2024, in cities of central and southern Sudan, including Wad Madani, Sennar, Sinja, Al-Damazin, and Dinder. Zain did not disclose the cause of the interruption. [6]

El Geneina, the state capital of Western Darfur, faced an internet blackout for over six days in November 2023, reportedly as a result of infrastructure failures. [7]

Power outages were frequently reported during the coverage period. A major blackout documented in five states lasted for five days in August 2023, likely caused by an overload and a cable fire. [8]

The Internet Outage Detection and Analysis (IODA) project reported a four-hour outage on August 17, 2023, with only 27 percent of Sudanese networks responding to IODA's internet connectivity test attempts. [9]

An unreliable electricity supply limits internet service in Sudan, including in major cities that have been subject to periodic power rationing. [10] Power cuts, which can last up to 12 hours, usually peak in the summer when demand is highest, especially in Khartoum, where population growth and climate have intensified demand. [11] Khartoum accounted for approximately 70 percent of the country's electricity usage as of 2019; [12] most rural areas have unsteady access to

electricity. In a December 2022 comment, Finance Minister Jibril Ibrahim said that only 40 percent of the Sudanese population had access to the country's power supply. [13] Also in December 2022, the Ministry of Oil and Energy allowed Sudanese to connect small-scale solar-power systems with the national electricity network. [14]

The country's internet infrastructure is generally equipped with backup generators to mitigate internet disruptions, though these generators do not always work. [15] Further, since the outbreak of the civil war, the security situation has inhibited the delivery of fuel for such generators. In May 2023, MTN said that its relay stations in Khartoum were not operating because fuel could not be transported safely through the conflict zone. [16]

Telecommunications companies struggle with endemic corruption and debt to foreign lenders. The resulting lack of investment in infrastructure has caused a degradation in internet service, prior to the outbreak of the civil war. [17]

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	**0**/3

Internet access is prohibitively expensive for many users. Skyrocketing prices for food, fuel, and other essentials, coupled with severe cash shortages resulting from the civil war, have made connectivity even less affordable.

Internet prices continued to rise during the coverage period, with all major providers imposing price increases. [18] As of May 2024, a 1-gigabyte (GB) monthly bundle offered by Zain costs 1,226.39 Sudanese pounds ($2.03). Sudani, a mobile service provider that operates under Sudatel, a partially state-owned entity, charges 1,560.28 pounds ($2.58). [19]

Due to widespread internet infrastructure failures and deliberate disruptions that occurred during the civil war (see A1 and A3), many people began to rely on Starlink to access the internet. [20] In areas under the RSF's control, the paramilitary group has charged residents high prices to connect. The hourly cost of connectivity often exceeds 3,000 pounds ($4.96), and some report costs of up

to $6 per hour. In El Geneina, the city government imposed annual license fees of 150,000 pounds ($248.40) in February 2024 for those who use Starlink for commercial purposes. [21]

Rising prices for connectivity have become even less affordable due to the lack of jobs, a result of the ongoing civil war. A salary crisis resulting from the civil war also affected internet affordability. In February 2024, Finance Minister Ibrahim said that some state employees would receive only 60 percent of their salaries, citing a fall in government revenues. [22]

Since 2011, a sustained petroleum shortage has led to drastically increasing inflation and skyrocketing prices for services, [23] which continued during the coverage period. The country's inflation rate stood at 83.6 percent as of January 2023. [24] In March 2022, the Ministry of Finance raised the telecommunications value-added tax (VAT) by 5 percent, which raised connectivity costs. [25]

Students remain disenfranchised by price increases as education has shifted online following the closure of schools during the civil war. In June 2023, the Ministry of Higher Education directed universities to resume education via digital platforms. [26] The government had employed e-learning during the COVID-19 pandemic, though critics noted that the cost of internet access was a major barrier for students' participation. [27] In October 2021, the Ministry of Education launched a free e-learning platform in collaboration with Ministry of Telecommunications and Digital Transformation (MTDT), Microsoft, the UN Children's Fund (UNICEF), and Sudan's four main ISPs (Zain, MTN, Sudatel, and Canar Telecom). [28] In October 2023, the UNICEF office in Sudan encouraged students to use the same platform to resume their education. [29] Moreover, in February 2024, the Ministry of Education said it had certified the country's first "electronic" school, to operate under the auspices of the Organization of Sudanese Working Abroad. [30]

According to a survey conducted by Afrobarometer in 2021, only 39 percent of women in Sudan reported having mobile internet access, compared to 49.7 percent of men. [31] A 2023 report from the Feminist Internet Research Network noted that social, economic, and legal inequality serve as a barrier to Sudanese women's internet access. [32]

The Universal Service Fund (USF), a government resource designed to ensure that mobile and internet networks are available for rural and lower-income populations who otherwise would be marginalized because of cost, has failed to expand access to rural communities. The USF levies taxes on telecommunications companies, though payment is reportedly an issue. [33] In 2023, the USF failed to engage with any project due to the war. [34]

Sudani provided free mobile internet and phone services during the conflict but announced the end of that practice in January 2024. [35] MTN and Zain provide zero-rating services by offering subscribers free, but sometimes limited, access to Facebook services. [36]

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	**1** / 6

The government has frequently exercised control over the internet infrastructure, and connectivity was regularly restricted as the SAF and RSF targeted internet services locally and nationwide during the ongoing civil war. Such disruptions have complicated efforts to deliver critical humanitarian aid, limited reporting on atrocities perpetrated by armed groups, and prevented people from communicating with family members or using online banking services to purchase food and medicine.

In February 2024, MTN and Sudatel users experienced nationwide service blackouts, following reports that the RSF had occupied those providers' data centers in Khartoum. The RSF initially denied responsibility for the restrictions, but sources including the state-owned Sudan News Agency said the RSF cut access to bolster its demand for services in RSF-controlled Darfur to be restored. [37] The RSF blamed the SAF for the restrictions in Darfur, though ISPs did not confirm the reason for the Darfur outages.

Later in February 2024, Zain's services were disrupted, reportedly after the RSF demanded that Zain halt services in SAF-controlled Port Sudan and Nile River State. After 10 days, extremely limited connectivity was restored on Sudatel's network, after the company established a new data center in Port Sudan. [38] Zain began to gradually restore service in March 2024, [39] while MTN announced that

its services had been restored in May 2024. [40] Despite the reported restoration of connectivity through the first half of 2024, users still experienced unreliable service due to infrastructure failures (see A1).

In November 2023, while the Alfitaihab neighborhood of Omdurman was under siege from the RSF, local resistance committees reported that resulting power shortages had interrupted local telecommunications services. [41] Between November and December 2023, authorities ordered ISPs to restrict connectivity in Omdurman during military operations. Some residents approached cell towers in an effort to connect but were sometimes dispersed and prohibited from connecting by SAF soldiers. [42] In February 2024, the military gave Starlink devices to the Khartoum state government to restore services disrupted by the RSF around Omdurman. [43]

Neighborhoods of Khartoum that saw heavy fighting between the SAF and the RSF during the coverage period experienced intermittent internet disruptions due to fuel shortages, and service remained irregular at the end of the coverage period. Connectivity was effectively nonexistent in Kordofan during the coverage period, according to reports. [44]

The lack of internet access during the midst of escalating conflict in West and Central Darfur has intensified the humanitarian and security crisis, hampered the delivery of humanitarian aid, and made it difficult for residents to report on fighting and crimes against humanity that have led to widespread death and displacement, both internally and in neighboring Chad.

In El Geneina, mobile connectivity was notably disrupted for over a week in early November 2023, [45] while the RSF stepped up abuses and mass atrocities against the Masalit and other non-Arab groups. [46] Sudani and Zain service was restored later in the month.

In May 2023, the city of Zalingei in Central Darfur State was subjected to a complete telecommunications blackout. [47] In July 2023, outages in Zalingei were attributed to an order from the RSF prohibiting maintenance workers from refueling generators to restore connectivity. [48] The blackout lasted for at least five months, and remained ongoing as of October 2023. [49] In November 2023,

after taking control of the city, the RSF said it would restore basic services, including telecommunications. [50]

In Nyala, in South Darfur, communications and internet access were disrupted in May 2023 after a telecommunications tower was targeted and badly damaged during fighting between the RSF and SAF, which limited the ability of residents to report on the conflict as hundreds of civilians were killed, wounded, or missing. [51] Service in Nyala was restored in September 2023. [52]

Ordinary users, aid groups, the SAF, and the RSF have all come to rely on Starlink to varying degrees during the coverage period. The RSF and humanitarian groups have been especially dependent on Starlink in Darfur, where telecommunications services have been heavily restricted. Despite a government-imposed ban on importing the devices (see A4), groups continued to use terminals smuggled in from neighboring countries. [53] Residents in RSF-controlled areas must pay high prices to connect (see A2). [54] In April 2024, Starlink announced it would block service to terminals operating in countries where it did not hold a license, including Sudan, at the end of that month. The blocks would impact terminals smuggled into Sudan that were using the provider's "roaming" feature. [55] Starlink terminals remained operational in Darfur as of May 2024, however. [56]

Sudan is connected to the global internet through international gateways controlled by Sudatel, Zain, and Canar Telecom, which are in turn connected to five submarine cables: Saudi Arabia–Sudan-1 (SAS-1), Saudi Arabia–Sudan-2 (SAS-2), Eastern Africa Submarine System (EASSy), FALCON, and Africa-1. The 2Africa Cable is expected to land in Sudan, though the landing had not been completed as of May 2024. [57]

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**3**/6

Legal and regulatory obstacles have not restricted the diversity of service providers in the past, though economic constraints continue. During the coverage period, the SAF sought to prevent the import of Starlink's portable satellite terminals on which the RSF has relied.

In January 2024, the Telecommunications and Post Regulatory Authority (TPRA) requested that the Ministry of the Interior prohibit any Starlink devices from entering Sudan. [58] Experts said this decision was made due to security concerns given the RSF's reliance on such terminals (see A3) as well as economic pressures from licensed ISPs, who reportedly complained that Starlink was operating without a license. [59] Sudanese authorities reportedly contacted SpaceX, which owns and operates Starlink, and asked for help regulating the satellite service in Sudan—including by requesting that the military be given the ability to disable service in RSF-controlled territory [60]—but said the company had not been responsive to requests to block access to smuggled devices. [61] Although SpaceX announced that roaming services would be turned off in Sudan by the end of April 2024, the service was still accessible as of May 2024 (see A3).

Several licensed telecommunications providers operate in Sudan, with Canar Telecom, Zain, MTN, and Sudatel maintaining significant market shares. The government is due to renegotiate its contracts with MTN and Zain when their licenses expire in 2024 and 2027, respectively. [62] No information was available about the status of MTN's license as of June 2024. In August 2021, the TPRA licensed three companies, Lolo Tech, Vision Valley, and Morgan Zone, to provide fixed wireless access (FWA) service. [63] As of February 2023, Vision Valley and Morgan Zone were operating, while Lolo Tech was using its license for implementing data transmission projects.

According to an August 2022 TPRA report, the most recent information available, Zain holds 49 percent of the mobile-service market, while MTN holds 26 percent and Sudatel holds 25 percent. According to the same report, Thabit, Sudatel's fixed-line brand, holds 79 percent of that market while Canar Telecom holds 21 percent. [64] Zain also holds 40 percent of the mobile internet market, while MTN and Sudatel hold 32 and 28 percent, respectively. [65]

MTN and Zain are primarily foreign owned. [66] The government owns 30 percent of Sudatel. [67] Following the ousting of the al-Bashir regime, the transitional government changed Sudatel's board of directors; for instance, Ibrahim Jaber Ibrahim, who is also a member of the Transitional Sovereignty Council, chairs the board of Sudatel. [68] The al-Bashir regime reportedly had significant sway over the company's board of directors. [69]

The government may also retain a stake in MTN's Sudanese operations, after anticorruption investigators seized assets held by a prominent businessman linked to the al-Bashir regime in 2020. The assets included shares in MTN. [70]

Zain has reportedly maintained links to the government. Hisham Allam was appointed chief executive in 2020. [71]

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	**0** / 4

The regulatory bodies that oversee service providers historically lacked independence, and recent changes indicate no movement toward autonomy. The TPRA, which replaced the National Telecommunications Corporation (NTC) in 2018, [72] is tasked with regulating internet use and telecommunications licensing, facilitating competition, producing statistics, and developing the ICT sector. [73] It has the power to engage in surveillance and restrict internet connectivity; it is also responsible for determining what content is accessible on the internet (see B3). [74]

In February 2021, the transitional government created the MTDT [75] and brought the TPRA under its purview. In October 2021, the coup authorities arrested the MTDT minister. [76] Lieutenant General Abdel Fattah al-Burhan, the military government's leader, named Adel Hassan Mohamed Hussein to the MTDT in January 2022. [77] Major General Sadiq Jamal al-Deen al-Sadig, appointed as head of the TPRA in 2019, was involved in the decision to restrict internet access following the October 2021 coup and directed ISPs to ignore a court order to restore internet service (see A3). [78]

TPRA decisions, including decisions to restrict internet access in recent years, have been seen as political in nature.

Unlike decisions made by the TPRA or other government authority, the internet shutdown attributed to the RSF in February 2024 was not justified using any legal framework (see A3). [79]

In October 2022, the government cancelled the registration of the Sudanese Consumers Protection Society, an organization with a history of advocating against internet shutdowns. [80]

B. Limits on Content

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content, particularly material that is protected by international human rights standards?	**5**/6

Sudanese authorities are known to block and filter websites and social media. No new blocks on social media platforms or websites were carried out during the coverage period; however, the government continues to block websites it considers "negative."

Websites hosting pornography reportedly became accessible in Sudan in 2019; authorities under the al-Bashir regime had previously openly blocked most pornographic and other "negative" content. [81] In July 2021, however, the TPRA announced that it would continue to block pornographic websites, citing the Telecommunications Law of 2018. [82] Users attempting to access such sites are directed to a TPRA block page. [83]

Many internet users access social media through virtual private networks (VPNs). Many users without VPNs on their phones pay specialists at technology shops throughout Sudan to install them. While the 2020 regulations on internet filtering mandate that VPN websites be blocked (see B3), [84] VPNs remained accessible through the coverage period. [85]

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content, particularly material that is protected by international human rights standards?	**2**/4

The Sudanese government does not systematically use legal or administrative means to force publishers and content hosts to delete legitimate content. Instead, authorities use intimidation to coerce internet users to delete content. The General Intelligence Service (GIS), as well as individuals affiliated with the military and the RSF, harass and intimidate users to delete content they object to in Facebook groups (see C7). [86]

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	**2**/4

Under the TPRA Act of 2018, the TPRA is mandated to protect the national security of Sudan, which is vaguely defined. [87] Furthermore, the law allows the TPRA to shut down any wireless device, wireless station, or broadcast station if these stations are violating rules and regulations outlined in other laws. The TPRA Act has been used to justify internet restrictions following the October 2021 coup, as well as to restrict the importing of Starlink devices during the coverage period (see A4).

In December 2020, the TPRA approved regulations on content filtering and website blockage. [88] The regulations give TPRA the mandate to block certain categories of websites including: gambling sites, peer-to-peer file sharing websites, VPN websites, websites which call for atheism, and websites of "any additional classifications that the authority considers." Under Article 8 of the regulations, ISPs must immediately block websites once they receive a TPRA notice or face fines of up 300,000 pounds ($496.79). [89]

The TPRA's website gives users the opportunity to submit requests to unblock websites "that are deemed to not contain pornography," [90] but it does not specify whether the blocking of political websites can be appealed. In addition to the TPRA, the prosecutor general has the power to block any website that threatens national security or violates social mores. [91]

In the past, the ISPs were transparent in communicating when websites were blocked due to the filtering directives of the former NTC. [92]

Little is known about the procedural aspects of the Sudanese government's restrictions of online content. In December 2018, Salah Abdallah, head of the now-defunct National Intelligence and Security Service (NISS), admitted that the government was responsible for blocking social media platforms, but the NTC did not provide further information about the decision. **93**

Under the al-Bashir regime, the TPRA managed online censorship through its internet service control unit. The regulator previously claimed that 95 percent of blocked material was related to pornography, **94** though it also acknowledged that it had not succeeded in blocking all "negative" sites in Sudan. **95** The TPRA additionally requires cybercafé owners to download blocking and filtering software. **96**

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	**1** / 4

Government threats against online journalists and internet users have led to growing self-censorship in recent years. Recent laws and directives restricting online speech have increased the risk of criminal prosecution, leading many people to self-censor (see C2). Widespread intimidation and violence targeting journalists covering the civil war from both the RSF and SAF has further restricted the environment for free expression online (see C7). **97**

In November 2023, after the SAF's Military Intelligence (Mi) in Kassala State interrogated journalist Haider Idris on charges of publishing RSF-issued statements, in connection with his coverage of the trial of someone accused of collaborating with the RSF, Idris stopped writing on his Facebook page (see C3).

Journalists have been unable to work due to targeting and harassment from belligerents, and have had to halt their reporting or leave Sudan entirely. Reports Without Borders said it had helped at least 40 journalists flee the country as of July 2023. **98**

Ordinary internet users have become more inclined to self-censor to avoid government surveillance and arbitrary legal penalties. They also rely on anonymous communication to speak candidly. Many journalists writing for online

platforms publish anonymously to avoid prosecution. After the October 2021 coup, protesters and activists relied on individuals living outside of Sudan to upload content they collect to avoid surveillance and arrest. [99]

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	**0** / 4

Manipulation and control of the online information environment has been a key tactic of both the RSF and the SAF throughout the civil war. Political actors frequently manipulate internet content to advance their agendas, and issue directives to media to control the public narrative.

Networks of accounts identified during the coverage period sought to generate support for each conflict party in the civil war. Beam Reports, a Sudanese fact-checking agency, identified disinformation narratives that targeted and promoted both the SAF and the RSF during the war, often relying on decontextualized images of atrocities or military craft. [100]

In December 2023, Beam Reports identified a network of inauthentic accounts on X that shared RSF propaganda, celebrated official occasions in Saudi Arabia, and published content about relations between the SAF and Iran. [101] Another investigation by Beam Reports the same month revealed that pro-RSF accounts were targeting SAF in a campaign to manipulate public opinion by publishing inauthentic official documents portraying the army and its supporters in a negative light. [102]

The RSF had previously reportedly used inauthentic X accounts to promote its activities; [103] prior to the outbreak of the civil war, in April 2023, the Digital Forensics Research Lab reported on two networks of inauthentic accounts promoting the RSF and its commander, Mohamad Hamdan Dagalo. One of the networks was comprised of newly created accounts, [104] while the other was comprised of accounts that may have been hijacked. [105]

Pro-SAF social media users known as the *Balabsa* post prowar content, often using hate speech and ethnically and regionally divisive, inflammatory language to

reject any negotiated end to the civil war. Reporting has noted links between the Balabsa and members of the ousted al-Bashir regime. [106]

In July 2023, a page linked to the SAF noted that its authors provided support to the SAF's intelligence operation, for the purpose of "cyber war" and armed media rooms. [107]

In March 2024, Muammar Musa, a politician who was a member of the NCP, and who currently leads efforts to support the SAF in Gezira State, called on people to join the "Electronic Deterrence Brigade" to confront the RSF's disinformation and propaganda. Whether this brigade would work as a fact-checking entity or would spread counterpropaganda was unclear. [108]

In December 2023, the Ministry of Culture and Information in Nile River State established a "unified media room" to combat rumors and limit the spread of RSF propaganda. [109]

Authorities in SAF-controlled areas have issued directives to media organizations covering the civil war. In January 2024, the acting minister of federal government and the governors of several states under the military's control issued decisions prohibiting the publication of any information that "disparages the prestige of the state" or of state bodies, including the military, using any means of communication (see C2). A coalition of digital rights organizations condemned the moves, calling on the government not to exploit the security situation to repress human rights. [110] In May 2024, the governor of Khartoum State issued a decision prohibiting publishing anything that leads to discouragement or creates discontent among the SAF, or which raises the morale of the RSF. [111] Military officials previously imposed editorial directives following the 2021 coup, which indicated that media outlets should refer to the coup as an "action" or "decision;" [112] authorities also pressure news outlets operating online and offline to avoid using negative language to describe the government.

Numerous entities spread disinformation in Sudan. Key foreign players in manipulating the information space in Sudan are based in Russia, Egypt, Ethiopia, and the United Arab Emirates. In October 2022, former MTDT minister Hashim Hassab al-Rasoul claimed that four foreign platforms linked with Russia were working to spread disinformation against the democratic transition. [113] Domestic

actors who spread disinformation include the SAF, the RSF, the GIS, Islamist parties, and parties opposed to military rule. Prior to the outbreak of the civil war, common disinformation narratives sought to generate support for the 2021 coup, launder the reputations of individuals and institutions with poor human rights records, discourage people from participating in protests, and discredit secular or feminist groups. [114]

The al-Bashir regime spread disinformation and manipulated social media discussion through the so-called cyberjihad unit, [115] which was established under the NISS's purview in 2011. Though its harassment of opposition figures and protesters and its coordinated disinformation efforts decreased after al-Bashir's ouster in 2019, the cyberjihad unit reportedly remained operational on social media. [116] Some politicians and activists have claimed that the cyberjihad unit targeted them with technical attacks and hacking attempts (see C8).

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**0**/3

The sharp contraction of Sudan's economy due to the ongoing civil war—which has placed 25 million people at risk of starvation according to a UN expert group's statement made just after the coverage period, in June 2024—has also negatively affected users' ability to publish content online. [117] For years, tight government control of the media environment prevented independent online news outlets and journalists from becoming economically viable. Political polarization further constrains the development of sustainable independent journalism. [118]

In January 2024, journalist Shamael al-Nour described facing constant communication problems with the SAF regarding how it deals with the press. [119] She had previously criticized the government for its lack of transparency, stating in January 2023 that the country had "become run by espionage" and that acquiring information from the government was nearly impossible. Another journalist said the government sent information to specific journalists via instant messaging apps, limiting the viability of outlets without such connections. [120]

The cost of issuing a license to establish any media services center, including a news site, is 400,000 pounds ($662.39). [121] In a country where the average annual

salary stood at 436,200 pounds ($722.38) in 2024, [122] these fees, which are imposed under the Press and Publication Act of 2009, severely restrict the media environment. The national Ministry of Culture and Information has also revoked accreditations of journalists and media outlets in retaliation for their coverage in recent years. [123]

Funding constraints limit the survival of online news outlets. Al-Taghyeer, for example, relies on donor funding, while Baj News relies on funding from a businessman. In December 2023, Lukman Ahmed, the former director of the Sudanese Radio and TV Corporation, announced the establishment of a US-based digital news platform affiliated with the US National Endowment for Democracy. [124]

Numerous news sites are funded by affiliates of the former al-Bashir government. The government has previously withheld advertisements from media outlets, leading to at least one closure. [125]

B7 0-4 pts

Does the online information landscape lack diversity and reliability?	**2** / 4

Sudan's civil war has fostered a highly polarized environment between the SAF and the RSF, further eroding the reliability of online information. Though diverse, the reliability of Sudan's online information space has also been hampered by a lack of editorial standards from online outlets, online misinformation, and manipulation by political actors (see B5).

Compared to the highly restrictive traditional-media environment, which is marred by prepublication censorship, confiscations of entire press runs of newspapers, [126] and warnings from GIS agents against reporting on certain taboo topics, [127] the internet remains a relatively open space for freedom of expression. Online news outlets such as Al-Taghyeer, [128] Radio Dabanga, [129] and Al-Rakoba cover controversial topics such as corruption and human rights violations. Other news sites, like Darfur24, the Nuba Times, and Sawt al-Hamish, cover regions that have been underrepresented in Sudanese media. [130]

Facing heavy censorship in print media, residents have increasingly relied on online outlets and social media for uncensored information in recent years. [131] The movement of newspapers from print to digital publication was accelerated by ongoing armed conflict during the coverage period, which has caused the cessation of issuing print newspapers in the country. [132]

Citizen journalism has contributed to increasing diversity of the media space by offering multiple sources of information in recent years. [133] Blogging is also popular, allowing journalists and other writers to publish commentary free from the restrictions leveled on print newspapers while providing women and ethnic and religious minorities a platform to express themselves. The more active Sudanese bloggers write in English.

The online landscape's diversity is impacted by how difficult it is to submit online payments for domain and hosting service providers abroad. The civil war has seriously affected the banking sector, to the point that even paying service fees via the black market is a challenge. [134] There are some service providers in Sudan, but security concerns also stand as a barrier to establishing new online media outlets. The January 2023 closure of BBC Arabic's radio service triggered concerns about the diversity of sources of information, especially because the internet penetration rate is low. [135]

The online media landscape lacks reliability, in part because the dozens of new media outlets that emerged after al-Bashir's ouster failed to demonstrate strong editorial policies and practices. Some media websites do not share basic information, such as the names of their reporters, editors, and leadership, or the source of their funding. [136] Government officials reportedly attributed the June 2021 blocking of news sites to the spread of online rumors from "unregistered sites and pages." [137]

As the civil war has continued, the online space is muddied with misleading content that undermines access to accurate and reliable information, and in some cases leads to offline harms. In August 2023, the International Committee of the Red Cross's Facebook page for Sudan posted to call on individuals to stop sharing unverified information and hate speech. [138] In April 2023, during the previous coverage period, following the removal of legacy verification checks on what was then known as Twitter, a Twitter Blue account claiming to represent the RSF

disseminated false information that Dagalo of the RSF had died from combat injuries. [139]

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	**2** / 6

Score Change: The score declined from 3 to 2 because significant repression from belligerent forces sharply contracted the environment for online activism, though some continued to rely on social media for advocacy and mutual aid.

The internet remained an important tool for mobilization during the coverage period, despite the connectivity disruptions and limits on online speech stemming from the civil war hampered free association online.

Sudanese authorities have exploited the fluidity of the security situation to crack down on the online activities of resistance committees, groups of grassroots activists who played a large role in organizing protests against al-Bashir in 2019 and against the coup in 2021 (see C3). Despite such restrictions, since the start of the civil war, activists and volunteers have created local, decentralized "emergency response rooms" that have relied on Starlink to access social media, engage in antiwar advocacy, and coordinate humanitarian aid in areas that would otherwise be unreachable. Volunteers use Facebook and WhatsApp to share requests for funds with donors, banking and money-transfer apps to provide money to emergency response rooms in the country, and messaging services to communicate with other volunteers at soup kitchens and schools. [140]

Activists previously relied on Facebook and Twitter to mobilize protests before the October 2021 internet shutdown. When internet services were restored in November 2021, people took to social media to circulate images and footage from a clash that took place in Khartoum that month, to call for accountability, and to organize subsequent protests. [141] Security forces allegedly surveilled and physically inspected protesters' mobile phones to delete evidence of human rights abuses (see C5). In November 2021, after accounts of security officers' practices spread online, an anonymous team of digital security experts created a guide for protesters to secure their devices if they faced inspection. [142]

C. Violations of User Rights

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	**0** / 6

In October 2021, Lieutenant General al-Burhan dissolved the transitional government in a military coup and suspended some of the 2019 interim constitution's articles. Al-Burhan specifically suspended articles related to the government's composition—namely the TSC, the cabinet, and the Transitional Legislative Council—creating "a legal conundrum" in enforcing other provisions and jeopardizing the constitution's freedom-of-expression protections. **143**

In August 2019, the military junta that overthrew the al-Bashir regime and the Forces of Freedom and Change (FFC), a coalition of civilian organizations, signed the interim constitution, the Draft Constitutional Charter for the 2019 Transitional Period, to serve as Sudan's legal framework until a new constitution is drafted. **144** The interim constitution includes a Rights and Freedoms Charter, which focuses on human rights, including those already specified in international agreements ratified by Sudan. The charter also enshrines the freedom of expression, freedom of the press, and access to the internet. **145** In addition, the interim constitution restructures Sudan's national judiciary and mandates that the transitional government ensures the judiciary's independence. **146**

Before the civil war, political and military actors were negotiating a new interim constitution following the dissolution of the transitional government in October 2021, which would underpin a future democratic transition. The leaked draft of the proposed interim constitution included the right to access the information using any means, including the internet. **147** However, this draft was not finalized before the conflict began in April 2023.

In August 2022, journalists established a new union to improve wages and their work environment. **148** The last independent journalists' union was dissolved in

1989. Sudan's registrar of labor organizations refused to recognize the new union in a February 2023 decision, however. [149]

Sudanese courts sometimes issue rulings that affirm freedom of expression online. In November 2021, the Khartoum District Court ordered telecommunications providers to resume internet services. [150] After ISPs failed to execute the court's decision, arrest warrants were issued for their managers; [151] an inside source later claimed that telecommunications providers restored internet access due to political and economic pressure, not because of the court decision. [152] In the past, the Constitutional Court has ruled in favor of prepublication censorship if it is deemed in the interest of national security.

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?	**1** / 4

Sudanese law can be used to penalize online activists, journalists, and ordinary users in retaliation for publishing legitimate online content.

In January 2024, the acting minister of federal government and governors of several states under the military's control issued decisions prohibiting the publication of any information that "disparages the prestige of the state" or state bodies, including the military, using any means of communication. Punishments for violations include fines of up to three million pounds ($4,970) and prison terms up to five years. A coalition of digital rights organizations condemned the moves, calling on the government not to exploit the security situation to repress human rights. [153]

Article 23 of the Law on Combating Cybercrimes (LCC) imposes sanctions such as "imprisonment for less than one year, flogging, or paying a fine" for "anyone who uses the internet, or any means of communications, information or applications to disseminate any news, rumor or report, knowing it's fake, to cause public fear or panic, threaten public safety and offend the reputation of the state." [154]

In July 2020, then prime minister Abdulla Hamdok signed amendments to 2018 LCC, which introduced criminal penalties for the spread of false news online. [155]

The law is based on the Informatic Offenses (Combating) Act of 2007, which criminalizes the establishment of websites that publish defamatory material and content that disturbs public morality or public order. [156] Those found in violation of the 2007 law face fines and two-to-five-year prison sentences. [157]

The July 2020 amendments to the LCC increased the penalties for many activities specified in the original law, including online defamation, online extortion, hacking of government websites, and sharing false information on social media. For instance, Article 24 of the amended LCC imposes a penalty of up to one year in prison and a fine for those who knowingly share false information online with the intention of "fear to the people or threatening the public peace or decreasing the prestige of the state." [158] The July 2020 amendments were reportedly supported by almost the entirety of the TSC. [159]

In November 2022, the cabinet passed an amendment to the LCC that criminalizes insulting state leaders and agencies or otherwise disseminate purportedly false news, [160] though its full text was not released. Under the amendment, authorities were obliged to impose imprisonment and a fine against offenders. [161]

Amendments to the criminal code in July 2020 also carry implications for online activities. Article 153, which criminalizes "material that violates public morals," was amended to remove the punishment of flogging. The provision still imposes penalties of up to one month's imprisonment and a fine for possession of such materials. [162] Osman M. Khartoum, a human rights lawyer, believes that the amended provision may still lead to broad arrests because of the nature of online communications, like WhatsApp group messages. Khartoum also holds that the provision, which permits a court to order "the confiscation of devices and equipment" [163] used to display the materials, may be used for abusive searches and seizures of electronic devices (see C5). [164]

National security imperatives have also opened journalists up to arrest. The 2010 National Security Act gave the NISS immunity from prosecution and the ability to arrest, detain, and censor journalists under the pretext of national security. [165] While amendments in 2020 reformed that law, the military government amended the GIS Law as part of a constitutional decree issued in May 2024, restoring many arrest and inspection powers, as well as immunity, to the GIS (see C5). [166]

C3 0-6 pts

Are individuals penalized for online activities, particularly those that are protected under international human rights standards?	3/6

Arrests and interrogations for online activities continued during the coverage period. Though prosecutions were reported less frequently than in previous years, both the SAF and RSF arbitrarily detained, questioned, and threatened journalists and activists who covered the conflict online.

In May 2024, the SAF's Mi arrested four activists in Gedaref State, Ezzedine Hassan, Ali Hassan Ali, Adil Hassan Fadlallah, and Omar al-Jamri Mohamed Ahmed, after they posted antiwar messages on Facebook. [167] They were taken to an undisclosed location—suspected to be army headquarters—along with five other Gedaref residents who had made posts calling for an end to the war, and were reportedly subjected to torture in detention (see C7).

SAF Mi personnel investigated and interrogated journalist Haidar Idris for "publishing news and statements issued by [the] RSF" on social media platforms in November 2023. The Mi commander threatened Idris with arrest if he continued to publish on WhatsApp about conflict in the region, and implied that Mi was surveilling the journalist. [168]

In August 2023, the GIS arrested Ali Tariq al-Arsh after publishing an investigation about security forces' harassment of displaced people. [169] Al-Arsh was released after five days and subsequently went into hiding. Mi later arrested his brother, who was still in detention as of April 2024, to force Ali to surrender himself, per a statement from the Emergency Lawyers group. That group claimed that the arrest was linked to an ongoing campaign of intimidation against activists. [170]

In July 2023, military personnel surrounded the home of activist Mohamed Ahmed Abdel Rahman, beat him (see C7), and brought him to SAF Mi headquarters; he was accused of operating a Facebook page called Al-Badiri, which hosted pro-RSF content. Abdel Rahman was released the same day, after an investigation proved he did not manage the page. [171]

Also in July 2023, Suleiman Mohammed Talli, a political activist and member of the Communist Party, was arrested over his Facebook posts covering events in North

Kordofan State. He was detained for two days in a Mi prison without an explanation of the reasons for his arrest. [172]

Also in July 2023, the SAF's Mi arrested Sharif al-Hamdabi, a prominent politician who was streaming live videos on Facebook calling people to stand against the conflict and call for peace. The SAF accused him of supporting the RSF. Emergency Lawyers said that the SAF had tortured al-Hamdabi (see C7). [173] Al-Hamdabi was detained for over 45 days; the exact date of his release was unclear.

The RSF arrested Abdelrahman Warab, a Sudan News Agency journalist, in June 2023. [174] Warab's subsequent fate is not yet known (see C7).

On May 30, 2023, journalist Nader Shulkawi, who posted clips of his reporting on YouTube, was detained in the city of Omdurman by the RSF and was being held in an RSF detention camp as of June 1, 2023. [175] He was later freed following calls for his release from family, friends, and the journalists' union. [176]

Salem Mahmoud, a correspondent for Al-Arabiya, was live-streaming via Facebook in April 2023, during the previous coverage period, when RSF personnel interrupted his reporting to question him about his work. [177]

The government places legal pressures on journalists using the vague terms in the LCC, often relying on criminal defamation charges under Article 25. Following the July 2020 amendments to the LCC (see C2), military officials announced that a cybercrime commissioner would monitor and prosecute "insults" lodged against the army. [178] In October 2022, the police announced that it would take legal action against those who "defame its work and spread rumors." [179]

Authorities have pursued online activists based outside Sudan. In March 2023, the GIS sued Dalia al-Tahir, a diaspora Sudanese journalist based in Libya, claiming that she published "fake news" regarding tension between the RSF and GIS. [180]

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	**3**/4

The government does not directly restrict encryption, but SIM card registration requirements limit anonymous communication. Social media blocks in past years

drove users toward VPNs and facilitated the use of encrypted communication tools like Signal and Telegram.

Article 9 of the NTC's General Regulations 2012, based on the 2001 Communications Act, obligates mobile service providers to keep a complete record of their customers' data, and authorities began enforcing mandatory SIM card registration in late 2017. Subscribers were required to register their phone numbers using their national identity cards, which include detailed personal information such as their home address and birthplace. These requirements enable the government to access mobile user information, limiting anonymity.

After the nationwide telecommunications shutdown attributed to the RSF in February 2024 (see A3), ISPs reportedly lost access to significant amounts of user data. Since then, ISPs began allowing users to use their services without using identity documents to reregister. [181]

In July 2022, after tribal conflict took place in Blue Nile, the Technical Committee of the Council of Security and Defense in Sudan ordered service providers to suspend all SIM cards that were not registered with a national identification number. [182] Service providers would be held legally responsible for any violations of the order.

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	**1** / 6

Unchecked communications surveillance is a grave concern in Sudan, where the government is known to actively monitor communications on social media platforms and surveil online activists and journalists during politically sensitive periods. The government still enjoys broad authority to conduct surveillance despite legal reforms, though the extent of the security forces' technical capacity to surveil is unclear.

According to a November 2022 report by LightHouse Reports, the RSF imported Predator, a spyware application produced by Intellexa; Predator can access a smartphone's camera, microphone, files, and other features after the target user

clicks a URL. [183] In April 2023, the Greek government admitted to allowing Predator's export to Sudan. [184]

Politician Mubarak Abdel Rahman Ahmed said on Facebook in October 2023 that the RSF had compromised his phone using spyware shortly before the outbreak of the conflict. [185]

In May 2023, SMEX reported that the RSF has been inspecting the contents of individuals' phones since the outbreak of armed conflict in Khartoum the month before. [186] While torturing and interrogating freelance photojournalist Faiz Abubaker (see C7), RSF members examined his Facebook account before releasing him.

Reports have also indicated that the SAF has surveilled journalists' online activities since the outbreak of the civil war. While threatening journalist Haidar Idris with arrest over his reporting in November 2023 (see C3), an Mi officer implied they were closely watching his posts.

Sudanese authorities used their access to mobile networks to trace the locations of and arrest some activists after the October 2021 coup. [187] In late 2022, the Emergency Lawyers Committee disclosed to SMEX that security forces subpoenaed phone histories and tracked the mobile phones of number of anticoup protesters who had been arrested. [188] Additionally, during the October 2021 protests, security forces allegedly inspected participants' mobile phones to delete evidence of rights abuses committed by security officers. [189]

In July 2020, the TSC amended the 2010 National Security Act; Article 25 of the law previously granted the NISS broad authority to surveil, interrogate, and arrest people in Sudan. While the amendments included several important reforms, Article 25 of the amended law still grants the GIS "the right to request information, data, documents or things from any person and view or keep them." [190] A former telecommunications engineer suggests that the amended version of Article 25 has been interpreted to permit security services to "lawfully violate a citizen's privacy without asking for any permission." [191] The GIS gained further search powers in May 2024, when the military government amended the GIS Law to reverse preexisting restrictions on the agency (see C2). [192]

The NISS regularly intercepted private email messages with the aid of sophisticated surveillance technologies. An industry source believed it likely that the NISS purchased surveillance equipment to facilitate interception at the landing stations in Port Sudan, though it remains unclear if the implementation was a success and whether the current authorities have access to the equipment. **193** Another pressing issue is the lawful interception clause in the contracts users sign with telecommunications companies, which is intentionally broad and gives the authorities the right to tap one's phone without clear evidence of criminal conduct or an ongoing investigation. **194**

According to 2013 research published by Citizen Lab, a Canadian digital rights organization, Sudanese authorities possessed high-tech surveillance equipment produced by the American technology company Blue Coat Systems, which manufactures monitoring and filtering devices. **195** In 2017, NISS agents reportedly planted Blue Coat surveillance software in the phones and laptops of at least 11 activists during an out-of-country meeting and training. **196**

C6 0-6 pts

Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?	**0** / 6

Service providers are required to aid the government in the surveillance of their users. In one 2020 case, such privacy violations may have facilitated an extrajudicial killing.

Reporting from online news outlet Darfur24 implicated communications surveillance in the killing of Baha al-Din Nouri, who was kidnapped and tortured to death by RSF officers in Khartoum in December 2020. According to sources, RSF officers kidnapped Nouri after their monitoring of his calls had not yielded enough information for an arrest warrant. Whether security forces monitored Nouri's call directly, using surveillance technology, or with assistance from a service provider is unclear. **197**

The SIM card registration process links phone numbers to users' personal data, which enables government surveillance (see C4). Mobile service providers are obligated to keep records of their customers' data, including full names, full addresses, other phone numbers, and place of employment. Under the

Telecommunications Law of 2018, telecommunications companies must provide customer data to authorities upon request. [198]

An activist who was summoned for questioning in early 2018 [199] noted that an NISS officer told him that the agency could collect extensive information about mobile users with just their phone numbers because authorities have access to the national identification system and the user information stored by telecommunications companies. A politician arrested after the October 2021 coup claimed that the government traced his location and identified his close contacts based on his SIM card activity. [200]

Though all telecommunications providers can be compelled to aid the government in monitoring the communications of their users, authorities reportedly have a tighter grip on Zain and Sudatel than MTN. The GIS has been closely involved in telecommunication providers' hiring processes in the past, though the practice may have decreased after 2019. [201]

Between January and June 2023, Meta received one request for data for a legal process from the Sudanese government; from July to December 2023, it received three such requests. The company did not turn over data in response to either. [202]

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in relation to their online activities?	**0** / 5

Score Change: The score declined from 1 to 0 as combatants on both sides of the civil war tortured and killed online journalists and ordinary internet users for their online expression throughout the coverage period.

Online journalists and activists often face extralegal intimidation, harassment, and violence in retaliation for their online activities. Violence against both online journalists and ordinary internet users increased following the outbreak of conflict between the SAF and the RSF as both sides have sought to control the narrative of the conflict and cover up human rights abuses.

In October 2023, Halima Idris Salim, a journalist for the YouTube-based outlet Sudan Bukra, was killed in Omdurman while covering the conflict, when an RSF vehicle ran over her. [203]

In June 2023, the RSF arrested Abdelrahman Warab, a journalist with the Sudan News Agency, and detained him at an unknown location without giving a reason for his arrest. As of November 2023, his whereabouts were still unknown, leading a journalists' organization to express concerns that Warab had been forcibly disappeared. [204]

In May 2024, a source reported that five residents of Gedaref who were detained for posting antiwar messages on Facebook (see C3) were subjected to torture while in detention, being beaten and whipped by SAF Mi personnel. [205]

Yasser Jabbara, an online journalist, was arrested in January 2024 by the SAF's Mi, who put him inside a shipping container for four days. [206]

Masa'ad Mohamed, a petroleum engineer in West Kordofan, was killed by "being excessively tortured" in November 2023 by the SAF's Mi. [207] Mohamed was reportedly killed after sharing a voice recording on WhatsApp describing the military situation on the ground. [208]

After detaining Sharif al-Hamdabi, a politician who was streaming live antiwar videos on Facebook, in July 2023, the SAF's Mi reportedly subjected him to torture in detention. [209]

SAF soldiers beat activist Mohamed Ahmed Abdel Rahman while arresting him in July 2023 on allegations of managing a Facebook page supporting the RSF (see C3). [210]

On social media, including WhatsApp and Facebook, lists of names of journalists accused of working for either side in the conflict have been circulated by anonymous accounts, potentially putting their lives in danger. [211] One journalist whose name was among those circulated reported receiving multiple death threats over WhatsApp. [212] A female journalist received threatening WhatsApp messages after she criticized the RSF in a private WhatsApp group for Sudanese media workers. [213] Multiple journalists reported to Al-Jazeera in May 2023 that

they were considering fleeing Sudan due to fears they would be targeted by either the SAF or the RSF. [214]

In May 2023, during the previous coverage period, freelance photojournalist Faiz Abubaker, who frequently posts his photography on Instagram, was shot in the back by the RSF while filming clashes in Khartoum. He was then held at an RSF checkpoint and later reported that RSF fighters assaulted him. [215] The RSF also examined his Facebook account and released him after he was able to prove that he was not affiliated with the SAF. [216] Abubaker fled to Egypt after recovering from his wounds.

Though the civil war sharply restricted the space for protest during the current coverage period (see B8), in previous years, security forces harassed protesters for their online activity, and often subjected online journalists covering protests to physical violence. Reports from activists of violent arrests and torture while in custody are common.

Antiwar politicians and activists, particularly women activists, have faced significant online harassment, bullying, and attempts to discredit them. Hanan Hassan, a lawyer and politician, has been a frequent target for harassment, [217] including gender-based hostility, with her caricature being used as part of a troll campaign against antiwar activists and politicians. [218] Hassan had previously changed her Facebook account after facing a wave of harassment in 2021.

Online harassment and hate speech along ethnic lines from both pro-RSF and pro-SAF accounts increased during the coverage period. Minority groups such as LGBT+ people are also frequent targets of online harassment. [219]

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	**1**/3

During the coverage period, social media accounts of politicians, parties, and other groups, both critical of and providing support for the military, were subject to hacking and cyberattacks.

In April 2024, the Facebook page of the Popular Resistance, a pro-SAF armed group, was hacked. The hackers reportedly posted false and inaccurate information before the administrators restored the page; the perpetrators were unknown. [220]

In March 2024, the X account of Sudanese politician Yasser Arman was hacked and an inauthentic account with his name appeared on the platform. Arman accused NCP remnants and the cyberjihad unit of targeting his account. [221] Arman has been a vocal critic of the war and the deposed al-Bashir regime on social media.

The Facebook pages of the Sudanese Congress Party and its president were hacked for six days in December 2023. The party announced that they restored the pages on December 15, 2023. [222]

In January 2023, the official Facebook page of the Almareikh football club was hacked by the "Sudan Cyber Security" hacking group, [223] after an individual tied to RSF commander Dagalo became the club's president.

In previous years, independent news sites have been subjected to technical attacks, which many believe were perpetrated by the cyberjihad unit. Attacks usually intensify around significant political events and unrest, while some prominent news sites ward off daily distributed denial-of-service (DDoS) attacks. Several online outlets reported technical attacks against their websites in past years but were able to respond by increasing their cybersecurity capabilities.

Footnotes

1 Simon Kemp, "Digital 2024: Sudan," DataReportal, February 23, 2024, https://datareportal.com/reports/digital-2024-sudan.

2 International Telecommunication Union, "Digital Development Dashboard: Sudan," accessed August 18, 2023, https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Develo....

3 "Sudan Median Country Speeds," Speedtest Global Index, accessed May 13, 2024, https://www.speedtest.net/global-index/sudan#mobile.

4 “Digital Development Dashboard: Sudan,” International Telecommunication Union, accessed May 13, 2024, https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Develo....

5 “Sudan Conflict Affects Digital Communications and Critical Services Delivery,” CIPESA, June 5, 2023, https://cipesa.org/2023/06/sudan-conflict-affects-digital-communication....

More footnotes

On Sudan

See all data, scores & information on this country or territory.

See More ›

Country Facts

Population
46,870,000

Global Freedom Score
6 /100 **Not Free**

Internet Freedom Score
28 /100 **Not Free**

Freedom in the World Status
Not Free

Networks Restricted
Yes

Social Media Blocked
No

Websites Blocked

No

Pro-government Commentators

Yes

Users Arrested

Yes

In Other Reports

Freedom in the World 2024

Other Years

2023

Be the first to know what's happening.

Join the Freedom House weekly newsletter

Subscribe

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org