

Flygtningenævnets baggrundsmateriale

Bilagsnr.:	694
Land:	Sudan
Kilde:	Freedom House
Titel:	Freedom on the net 2023. Sudan
Udgivet:	oktober 2023
Optaget på baggrundsmaterialet:	7. marts 2024

NEW REPORT: Visible and Invisible Bars

ENGLISH عربي



FREEDOM ON THE NET 2023

Sudan

NOT FREE

30

/100

A. <u>Obstacles to Access</u>	5/25
B. <u>Limits on Content</u>	15/35
C. <u>Violations of User Rights</u>	10/40

LAST YEAR'S SCORE & STATUS

29 /100 Not Free

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



Overview

Internet freedom remained largely the same in Sudan, with very limited improvements. Sudanese internet users were impacted by the military government's continued efforts to restrict access in response to prodemocracy movements, as well as by restrictive amendments to the Law on Combating Cybercrimes (LCC)—which introduced mandatory prison sentences and fines for defaming public figures—and the conflict between the paramilitary Rapid Support Forces (RSF) and the Sudanese Armed Forces (SAF). Both sides in the armed conflict used inauthentic accounts to control the narrative, and the RSF's import of Predator spyware underlined authorities' growing reliance on tools for digital surveillance and information manipulation. Journalists faced arrests, threats, and in some cases, torture at the hands of belligerents. Social networks remained accessible during the coverage period, however, and activists leveraged social media to document human rights abuses.

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 government began to enact reforms, and space for the exercise of civil liberties slowly opened. However, the process was thrown into turmoil by the late 2021 coup, which led to the dissolution of the transitional government, and the 2023 conflict between the RSF and SAF. Throughout the transition period, violence involving security forces, other armed groups, and rival ethnic communities has persisted in much of Sudan.

Key Developments, June 1, 2022 - May 31, 2023

- Internet services were regularly intermittently disrupted after conflict began between the RSF and SAF in April 2023. Some restrictions were due to government orders, while others were the result of the RSF occupying the Sudan Telecom Company (Sudatel) Khartoum data center and attacks on or

near communications infrastructure in conflict-affected areas (see A1 and A3).

- Authorities enacted nationwide internet restrictions multiple times throughout the coverage period in response to planned protests against military rule (see A3).
- In November 2022, the cabinet passed an amendment to the LCC, under which offenders will receive a mandatory prison term and a fine in cases where they defame a public figure or agency (see C2).
- Violence, online harassment, and arrests targeted at journalists in retaliation for their reporting increased after clashes between the RSF and SAF began, with both sides seeking to control the narrative and conceal human rights abuses (see C3 and C7).
- In July 2022, after tribal conflict erupted in Blue Nile State, telecommunications service providers were ordered to suspend all SIM cards not registered with a national ID number (see C4).
- In November 2022, a foreign news outlet reported that the RSF had acquired Predator, spyware that can access a target smartphone's camera, microphone, and other features (see C5).

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 remains low, with 28.4 percent of the population—representing 13.5 million people—using the internet as of January 2023 according to the *Digital 2023* report. ¹ The most recent data from the International Telecommunication Union (ITU), which dates back to 2020, places the internet penetration rate at 28 percent. ²

According to data from Ookla, the median mobile download and upload speeds for Sudan in March 2023 were 18.98 and 10.62 Megabits per second (Mbps), respectively. Fixed-line median download and upload speeds stood at 5.23 and 3.97 Mbps. ³ ITU data showed that there were 30,426 fixed-line broadband connections in Sudan as of 2021. ⁴

Mobile service provider Sudani, which operates under the partially state-owned Sudatel, became the first provider to begin 5G trial operations in Khartoum in February 2022. ⁵

In December 2022, service provider Zain disclosed a plan to spend \$800 million to upgrade its infrastructure in Sudan. ⁶ In February 2023, Zain paid the Telecommunications and Post Regulatory Authority (TPRA), Sudan's telecommunications regulator, \$37 million in spectrum license fees to improve service quality. ⁷

In January 2023, Canar Telecom signed a \$15 million, six-year strategic partnership agreement with YahClick to provide satellite broadband services in Sudan. ⁸

An unreliable electricity supply limits internet service in Sudan, ⁹ including in major cities that have been subject to periodic power rationing. Power cuts, which can last up to 12 hours, ¹⁰ usually peak in the summer when demand is highest, especially in Khartoum, where population growth and climate have intensified demand. In a December 2022 comment, Finance Minister Jibril Ibrahim said that only 40 percent of the Sudanese population enjoyed access to the country's power supply. ¹¹ In March 2023, the Power Distribution Company declared planned power cuts for six hours a day two working days per week, and three hours per day on Saturdays. ¹² In December 2022, the Ministry of Oil and Energy allowed Sudanese to connect small-scale solar-power systems with the national electricity network. ¹³

Khartoum accounted for approximately 70 percent of the country's electricity usage as of 2019; ¹⁴ most rural areas have unsteady access to electricity. The country's internet infrastructure is generally equipped with backup generators to mitigate internet disruptions, though these generators do not always work. ¹⁵

The internet infrastructure has been impacted by the armed conflict between the RSF and the SAF. Electricity outages, a lack of fuel, and inability to deliver fuel due to the security situation have led to service interruptions. ¹⁶ In late April 2023, a nationwide power outage affected multiple internet service providers (ISPs). ¹⁷ In early May 2023, MTN issued a statement that its relay stations in Khartoum were not operating because fuel could not be transported safely through the conflict zone. ¹⁸

When available, internet infrastructure is not always reliable. Citizens of Ghibaish, in North Kordofan State, disrupted local Zain service after protesting in front of communications towers; the protesters said Zain representatives had not responded to calls to maintain or upgrade existing services. ¹⁹

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, exacerbated during the COVID-19 pandemic. ²⁰

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, and the country's economic crisis increased relative prices further during the coverage period. According to the General Commissioner of Social Security, the poverty rate reached 65 percent in 2022. ²¹

Since 2011, a sustained petroleum shortage has led to drastically increasing inflation and skyrocketing prices for services, ²² which continued the coverage period. The country's inflation rate stood at 83.6 percent as of January 2023. ²³ In March 2022, the Ministry of Finance raised the telecommunications value-added tax (VAT) by 5 percent, which raised connectivity costs. ²⁴

Internet prices continued to rise during the coverage period, with all major providers imposing price increases. ²⁵ As of January 2023, a 1-gigabyte (GB) monthly bundle offered by Zain and Sudatel cost 982.65 (\$1.71) and 855.61 Sudanese pounds (\$1.49) respectively, ²⁶ which are unaffordable for most residents. The Ministry of Finance raised the minimum wage to 12,000 pounds (\$20.95) for government employees in January 2021. ²⁷

Students remain disenfranchised by price increases. In July 2020, the higher education minister directed universities to commence e-learning to combat the spread of COVID-19. After critics noted that the cost of internet access is a major barrier for students' participation in e-learning, ²⁸ 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, and Sudan's four main ISPs (Zain, MTN, Sudatel, and Canar Telecom). **29**

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. **30**

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. **31** In July 2022, Sudatel chief executive Magdi Taha said that the USF will start distributing funds to 100 telecommunication towers in the Darfur region. **32**

MTN and Zain provide zero-rating services by offering subscribers free, but sometimes limited, access to Facebook services. **33**

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 frequently exercises control over the internet infrastructure, and internet access was shut down nationwide and locally during the coverage period.

Between June 11 and 22, 2022, the authorities cut internet access nationwide for three hours daily, ostensibly to prevent cheating on national exams. **34** Later that month, internet and phone service was restricted nationwide as protesters in Khartoum rallied against the military government. **35**

In October 2022, authorities in Blue Nile State restricted internet access during a tribal conflict in the Wad al-Mahi area, to curb inflammatory discourse. **36** Also in October 2022, authorities restricted access nationwide for an eight-hour period as protesters marked the one-year anniversary of the 2021 coup. **37**

Telecommunication services were disrupted in the western Darfur village of

Tandalti during an outbreak of communal violence, after a video of two men who had been murdered and mutilated was circulated on social media. **38**

Internet access was disrupted in April 2023 as the armed conflict between RSF and SAF began. **39** On April 16, 2023, a day after fighting began, the TPRA ordered MTN to restrict internet services before reversing itself hours later. **40** While authorities did not issue any further shutdown orders, infrastructure obstacles played a major role in service disruptions in Khartoum after the onset of the conflict (see A1).

Mobile subscribers were affected by outages occurring over four days in April 2023. Canar Telecom's 83-hour outage was the longest, while Sudatel's lasted 40 and Zain's lasted 10. The reason for these disruptions remains unclear as of the end of the coverage period. **41**

The SAF claimed that the RSF seized Sudatel's data center in Khartoum, causing a service outage lasting over 24 hours in late April 2023. **42** A source within Sudatel confirmed this claim. **43**

Internet traffic recovered slightly following the cease-fire between the SAF and RSF in late April 2023, but intermittent disruptions persisted through the end of May 2023. **44**

On May 17, 2023, the cities of El Geneina and Zalingei in West Darfur were subjected to a complete telecommunications and internet blackout. **45** The lack of internet access during the midst of escalating conflict in West and Central Darfur has intensified the humanitarian and security crisis, preventing the delivery of humanitarian aid, and making it difficult for residents to access information and report on fighting in El Geneina, **46** which have displaced thousands of people to neighboring Chad. **47** The communications blackouts in Zalingei and El Geneina were ongoing at the end of the coverage period.

In Nyala, in South Darfur, communications and internet access was also disrupted in May 2023 after a telecommunications tower was 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. **48** Service in Nyala was restored after the end of the coverage period, in September 2023. **49**

Sudan experienced two near-total network shutdowns, lasting 36 days and 25 days respectively, in 2019 and 2021. ⁵⁰ In early June 2019, security forces attacked a peaceful sit-in in Khartoum, killing 127 people, injuring hundreds more, and sexually assaulting dozens. ⁵¹ The timing of the shutdown limited the spread of information about the massacre on the internet, including evidence of abuses perpetrated by security forces. ⁵² During these disruptions, internet services were intermittently available via some Canar Telecom and Sudatel fixed-line connections. ⁵³

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 be operational in Sudan by 2024. ⁵⁴

A4 0-6 pts

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

3/6

There are no legal or regulatory obstacles that restrict the diversity of service providers, though there are economic constraints.

The government is due to renegotiate its contracts with MTN and Zain when their licenses expire in 2024 and 2027, respectively. ⁵⁵ Four licensed telecommunications providers operate in Sudan: Canar Telecom, Zain, MTN, and Sudatel. In August 2021, the TPRA licensed three companies, Lolo Tech, Vision Valley, and Morgan Zone, to provide wireless broadband service. ⁵⁶ As of February 2023, Vision Valley and Morgan Zone were operating, while Lolo Tech was using its license for implementing data transmission projects. ⁵⁷

According to an August 2022 TPRA report, 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. ⁵⁸ Zain also holds 40 percent of the mobile internet subscriptions market, while MTN and Sudatel hold 32 and 28 percent, respectively. ⁵⁹

MTN and Zain are primarily foreign owned. ⁶⁰ The government owns 30 percent of Sudatel. ⁶¹ Following the ousting of the al-Bashir regime, the transitional government changed Sudatel's board of directors; for instance, Transitional Sovereign Council (TSC) member Ibrahim Jaber Ibrahim now chairs the board. ⁶² The al-Bashir regime reportedly had significant sway over the company's board of directors. ⁶³

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. ⁶⁴

Zain has reportedly maintained links to the government. Hisham Allam was appointed chief executive in 2020. ⁶⁵

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, ⁶⁶ is tasked with regulating internet use and telecommunications licensing, facilitating competition, producing statistics, and developing the information and communications technology (ICT) sector. ⁶⁷ It is also responsible for determining what content is accessible on the internet (see B3). ⁶⁸

In September 2019, the TSC separated the TPRA from the Ministry of Defense and brought it under its direct administration; previously, the TPRA fell under the Ministry of Information. The decisions to place the TPRA under the purview of the Ministry of Defense, and then the TSC itself, were met with criticism, as the body has the power to engage in surveillance and restrict internet connectivity. ⁶⁹ In February 2021, the transitional government created the MTDT ⁷⁰ and brought the TPRA under its purview. In October 2021, the coup authorities arrested the MTDT minister. ⁷¹ Lieutenant General Abdel Fattah al-Burhan, the military government's leader, named Adel Hassan Mohamed Hussein to the MTDT in January 2022. ⁷² In July 2019, Major General Sadiq Jamal al-Deen al-Sadig was appointed as the head of the TPRA. ⁷³ Al-Sadig 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). **74**

TPRA decisions, such as the decision to restrict internet access in October 2022 are seen as political in nature (see A3).

In October 2022, the government cancelled the registration of the Sudanese Consumers Protection Society (SCPS), an organization with a history of advocating against internet shutdowns. **75**

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
---	------------

Score Change: The score improved from 3 to 5 because the government did not block social media platforms during the coverage period.

Sudanese authorities are known to block and filter websites and targeted one news site during the coverage period. However, authorities refrained from blocking access to social media during the period.

In September 2022, the cybercrime unit of the public prosecution ordered a block on the website of the *Al-Sudani* newspaper. The newspaper, which said it did not receive a complaint before the order was issued, vowed to appeal it in court. **76** Despite the decision, the website remained accessible. **77**

The ousted al-Bashir regime openly acknowledged blocking and filtering websites that it considered “negative.” **78** Websites hosting pornography reportedly became accessible in Sudan in 2019; the authorities had previously blocked most pornographic content. In July 2021, however, the TPRA announced that it would continue to block pornographic websites, citing the Telecommunications Law of 2018. **79**

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), ⁸⁰ VPNs remained accessible through the coverage period. ⁸¹

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, the authorities use intimidation to coerce internet users to delete content. The General Intelligence Service (GIS) and individuals affiliated with the government harass and intimidate users to delete content they object to in Facebook groups (see C7). ⁸²

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. ⁸³ 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 was used to justify internet restrictions following the October 2021 coup, as well as previous internet restrictions.

In December 2020, the TPRA approved the 2020 regulations on content filtering and website blockage. ⁸⁴ 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.” ⁸⁵ 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 (\$524). ⁸⁶

The TPRA's website gives users the opportunity to submit requests to unblock websites "that are deemed to not contain pornography," ⁸⁷ 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. ⁸⁸

In the past, the ISPs were transparent in communicating when websites were blocked due to the filtering directives of the former NTC. ⁸⁹ However, ISPs reportedly no longer show this explanation when sites are blocked. ⁹⁰

Little is known about the procedural aspects of the Sudanese government's restrictions of online content. The TPRA still has not disclosed details about the 2018 social media blocks and network shutdowns. 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. ⁹¹

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, ⁹² though it also acknowledged that it had not succeeded in blocking all "negative" sites in Sudan. ⁹³ The TPRA additionally requires cybercafé owners to download blocking and filtering software. ⁹⁴

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. While journalists enjoyed an unprecedented level of freedom in the immediate aftermath of al-Bashir's ouster, the army has since done much to restrict it.

In October 2022, the police announced that it would take legal action against those who “defame its work and spread rumors.” ⁹⁵ In November 2022, the cabinet announced that it has passed an amendment to the LCC, mandating fines and imprisonment for those who defame public officials or agencies or otherwise disseminate purportedly false news (see C2). ⁹⁶ The risk of criminal prosecution for online speech has led people to self-censor.

In October 2021, *al-Democracy*, a newspaper that transitioned into a digital outlet after the coup, reported that their offices were under surveillance by security forces. ⁹⁷

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. ⁹⁸ Many journalists writing for online platforms publish anonymously to avoid prosecution. Since 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

Political actors frequently manipulate internet content to advance their agendas. Networks of accounts identified during the coverage period sought to generate support for the 2021 military coup. The RSF used networks of inauthentic accounts to promote its activities and its commander, Mohamad Hamdan Dagalo, as tensions between the RSF and SAF in early 2023.

Government officials pressure news outlets operating online and offline to avoid using negative language to describe the government. In February 2022, during the previous coverage period, the National Council of Press and Publication issued a letter to the *Al-Jareda* newspaper, warning it to change its description of the TSC, which it called “putschist” in its reporting. ¹⁰⁰ *Al-Jareda* preserved their original language on Facebook. ¹⁰¹

The government imposed editorial directives on media outlets following the October 2021 coup. The directives, which indicated media outlets should refer to the coup as an “action” or “decision,” were provided orally through the Press and Publications Council and the Private Media Department of the Ministry of Culture and Information (MCI) to Sudan TV, Sudanese Radio, and other outlets. **102**

Officials have used inauthentic accounts on social media to amplify their content. In October 2022, the Sudan2day news outlet reported that Mubarak Ardol, head of the Sudanese Mineral Resources Company and secretary-general of the pro-coup National Consensus Force (NCF) party, used inauthentic accounts to engage with his posts on Facebook. **103**

In October 2022, Beam Reports reported that RSF used inauthentic accounts to promote its activities via X, the platform then known as Twitter. **104** In April 2023, as tensions between the SAF and RSF rose, 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, **105** while the other was comprised of accounts that may have been hijacked. **106**

Campaigns targeting Sudanese social media users are identified regularly. In January 2022, Marc Owen Jones, a disinformation researcher, identified a network likely including inauthentic and hacked accounts to share content about the United Arab Emirates’ support for and relationship with Sudan. **107** In August 2021, Jones noted a Twitter network that likely included inauthentic and hacked accounts amplified a narrative that Sudanese internet users opposed the government’s decision to transfer al-Bashir to the International Criminal Court. **108**

In November 2022, a network containing more than 15 accounts was identified in promoting the 2021 coup. **109** 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. **110**

In February 2022, Alhadi Mohammed Alameen, an online journalist for the Sudan Tribune, received a request to refrain from reporting on terrorism and religious

extremism. It was unclear who sent the message. ¹¹¹ Rather than adhering to the request, Alameen stopped writing altogether. ¹¹²

Numerous entities spread disinformation in Sudan. Key foreign players in manipulating the information space in Sudan are based in Russia, Egypt, Ethiopia, and the UAE. Domestic actors who spread disinformation include the SAF, the RSF, the GIS, Islamist parties, and parties opposed to military rule. Some common disinformation narratives have sought to generate support for the 2021 coup, launder the reputations of individuals and institutions with poor human rights records, discourage and distract people from participating in protests, and discredit secular or feminist groups. ¹¹³

The al-Bashir regime spread disinformation and manipulated social media discussion through the so-called cyberjihad unit, ¹¹⁴ which was established under the NISS's purview in 2011. In 2019, the unit was especially active on Facebook and Twitter, using human-run accounts to harass opposition figures and protesters, flooding platforms with coordinated posts to sway public opinion, and spreading false information to muddle debate. ¹¹⁵ It also sought to report target accounts for violating social platforms' community standards, sometimes leading to their closure or suspension. ¹¹⁶ The unit also reportedly orchestrated technical attacks against independent websites (see C8).

Despite the al-Bashir regime's ouster, the cyberjihad unit reportedly remains active on social media. ¹¹⁷ In 2020, the unit shared disinformation related to the transitional government's COVID-19 response, with the apparent goal of mobilizing antilockdown protests. ¹¹⁸

Dozens of online newspapers and other outlets have appeared since 2019, some of which appear to be affiliated with the security services or the cyberjihad unit. The outlets use sensational headlines and social media posts to malign activists and civil society organizations. ¹¹⁹ In November 2019, the al-Ain news site cited anonymous sources when it reported on other outlets that were connected to the NCP, the ruling party of al-Bashir, or the former regime's security services. ¹²⁰

The government of Khartoum State established a "Rumor Combating Center" in December 2022, purportedly to combat hate speech, bullying, and false online content. ¹²¹

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

0/3

Several economic and regulatory constraints negatively affect users' ability to publish content online. 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. **122**

In a January 2023 comment, Sudanese journalist Shamael Elnoor, a Sudanese journalist, said 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. **123**

In February 2022, the social network then known as Twitter allowed Sudanese users to register accounts with a local phone number. **124** Twitter previously restricted Sudanese users from registering with local numbers because of US sanctions. ChatGPT is inaccessible in Sudan because it cannot authenticate accounts that use Sudanese phone numbers. **125**

The cost of issuing a license to establish any media services center, including a news site, is 400,000 pounds (\$662). **126** In a country where the average annual salary stood at 480,000 pounds (\$794) in 2022, **127** these fees, which are imposed under the Press and Publication Act of 2009, severely restrict the media environment.

In January 2022, the MCI revoked the accreditation of Al Jazeera Mubasher journalist Mohammed Omar and photographer Badawi Bashir for their "unprofessional coverage of the Sudanese affairs." The outlet's broadcast license was also revoked. **128**

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. The US sanctions regime prevented Sudanese news sites from

generating revenue through advertisement monetization with US companies. In 2021, Sudan Digital, a private Sudanese company and research entity, reported that Facebook, Google, and other platforms are working to enable ad sales in Sudan following the end of the sanctions. ¹²⁹ Numerous news sites are funded by affiliates of the former al-Bashir government (see B5). In March 2020, Hussein Khogali, the owner of Omdurman TV and an NCP loyalist, announced that he would close the outlet because of its inability to pay broadcasting fees. ¹³⁰ Khogali wrote an article saying that the government refused to place official and semiofficial advertisements on the channel, effectively boycotting the outlet. ¹³¹

In February 2020, the government appointed Lukman Ahmed, a former British Broadcasting Corporation journalist, as director of the Sudanese General Corporation for Radio and Television Transmission. ¹³² The corporation primarily regulates broadcast media, which are also an important source of news in the online media space. Ahmed and other officials indicated that they would seek to liberalize the media environment and reduce state control of broadcasters. ¹³³ Ahmed was removed in April 2021, reappointed by then prime minister Abdulla Hamdok in December 2021, and was removed by al-Burhan again in April 2022. ¹³⁴

B7 0-4 pts

Does the online information landscape lack diversity and reliability?

2/4

Sudan's online information space is increasingly diverse, though its reliability is hampered by a lack of editorial standards from online outlets, online misinformation, and manipulation by political actors (see B5).

Compared to the highly restrictive space in the traditional media sphere, which is characterized by prepublication censorship, confiscations of entire press runs of newspapers, ¹³⁵ and warnings from GIS agents against reporting on certain taboo topics, ¹³⁶ the internet remains a relatively open space for freedom of expression. Many voices express discontent with the government on various online platforms. Online news outlets such as Al-Taghyeer, ¹³⁷ Radio Dabanga, ¹³⁸ 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. ¹³⁹

Facing heavy censorship, many print newspapers have shifted to digital formats, circulating censored or banned material on their websites and social media pages; as a result, residents increasingly rely on online outlets and social media for uncensored information. **140**

The online landscape's diversity is impacted by how difficult it is to submit online payments for domain and hosting service providers abroad. There are some service providers in Sudan, but security concerns also stand as a barrier to establishing new online media outlets. **141** The January 2023 closure of BBC Arabic's radio service triggered a discussion about how this development impacts the diversity of sources of information, especially because the internet penetration rate is low. **142**

Citizen journalism has grown after al-Bashir's ouster, which has contributed to increasing diversity of the media space by offering multiple sources of information. **143** 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 media landscape lacks reliability, in part because the dozens of new media outlets that emerged after al-Bashir's ouster have 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. **144** Government officials reportedly attributed the June 2021 blocking of news sites to the spread of online rumors from "unregistered sites and pages." **145**

The online space is muddled with misleading content that undermines access to accurate information, and in some cases leads to offline harms. In April 2023, following the removal of legacy verification checks on what was then known as Twitter, a Twitter Blue account claiming to represent the RSF tweeted false information that Dagalo of the RSF had died from combat injuries. **146**

In June 2022, the Association of Lawyers of Eastern Sudan raised 26 lawsuits against websites that allegedly spread tribal hate speech, content which has incited communal violence in the past (see A3). **147**

B8 0-6 pts

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

3/6

The internet is an increasingly important tool for mobilization, though internet shutdowns designed to impede online organizing have harmed the environment. Sudanese security forces continue to respond to protests with indiscriminate force.

Activists relied on Facebook and Twitter to mobilize protests before the October 2021 internet shutdown. Organizers then mobilized protests through short-message service (SMS) messages, until mobile services were also restricted. ¹⁴⁸ 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. ¹⁴⁹

Security forces allegedly surveilled and physically inspected protesters' mobile phones to delete evidence of human rights abuses (see C5). After accounts of security officers' practices spread online, protesters sought to protect themselves by deleting social media apps and information received on WhatsApp and other platforms. Some demonstrators acquired separate phones to use at protests or when they perceived a threat from security forces. ¹⁵⁰ Protesters also used functions available on some phones that allowed them to use guest accounts that would have fewer installed apps available (and, therefore, less incriminating information). ¹⁵¹ In November 2021, an anonymous team of digital security experts created a guide to securing phones to help protesters protect themselves if they faced inspection. ¹⁵²

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. ¹⁵³ In addition to suspending parts of the constitution, al-Burhan declared a state of emergency that was lifted in May 2022. ¹⁵⁴

Before the SAF-RSF conflict, 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 disclosed that the constitution guaranteed the right to access the information using any means, including the internet. ¹⁵⁵ However, this draft was not finalized prior to the outbreak of conflict in April 2023.

In August 2022, journalists established their first union to improve wages and their work environment. ¹⁵⁶ The last independent journalists' union was dissolved in 1989. Sudan's registrar of labor organizations refused to recognize the union. ¹⁵⁷

In August 2019, the military junta that overthrew the al-Bashir regime and the Forces of Freedom and Change, a coalition of civilian organizations and rebel forces, 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. ¹⁵⁸ 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. ¹⁵⁹ In addition, the interim constitution restructures Sudan's national judiciary and mandates that the transitional government ensures the judiciary's independence. ¹⁶⁰

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. ¹⁶¹ After ISPs failed to execute the court's decision, arrest warrants were issued for their managers; ¹⁶²

an inside source later claimed that telecommunications providers restored internet access due to political and economic pressure, not because of the court decision. ¹⁶³ 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 July 2020, then premier Hamdok signed amendments to 2018 LCC, which introduced criminal penalties for the spread of false news online. ¹⁶⁴ 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. ¹⁶⁵ Those found in violation of the 2007 law face fines and two-to-five-year prison sentences. ¹⁶⁶

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.” ¹⁶⁷ The July 2020 amendments were reportedly supported by almost the entirety of the TSC. ¹⁶⁸ The Ministry of Justice reportedly began exploring further reforms to the LCC in November 2020. ¹⁶⁹

In November 2022, the cabinet passed an amendment to the LCC that criminalizes insulting state leaders and agencies, ¹⁷⁰ though its full text was not released. Under the amendment, authorities were obliged to impose imprisonment and a fine against offenders. ¹⁷¹

Article 23 of the 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.” ¹⁷²

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. ¹⁷³ 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” ¹⁷⁴ used to display the materials, may be used for abusive searches and seizures of electronic devices (see C5). ¹⁷⁵

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; ¹⁷⁶ amendments to the law in 2020 grant the GIS this immunity (see C5).

C3 0-6 pts

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

3/6

Arrests, prosecutions, and interrogations for online activities continued during the coverage period. Internet users have continued to fear arrest for online dissent since the October 2021 coup. After the conflict between the SAF and the RSF began in April 2023, the Journalists’ Syndicate has reported that many of its members have faced violations from both sides. ¹⁷⁷ These violations included arrests, as well as threats, injuries, and disappearances (see C7). Journalists regularly receive legal complaints and lawsuits in retaliation for their reporting.

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 had been transferred to an RSF detention camp as of June 1, 2023. ¹⁷⁸

Salem Mahmoud, a correspondent for Al-Arabiya, was live-streaming via Facebook when RSF personnel interrupted his reporting to question him about his work. **179**

On April 11, 2023, Sudanese police arrested and detained Yasir Mirghany, the head of the SCPS, on allegations of corruption related to European Union funds received by SCPS in 2012. Mirghany was released on April 18. **180** SCPS has a strong history in fighting against internet shutdowns using legal means, and had its registration cancelled during the coverage period (see A5), inhibiting the group's ability to operate.

In March 2023, after taking out her phone to record the demolition of homes in Khartoum, journalist Ikhlas Nimir, who sometimes shares reporting from her public Facebook page and has worked for online media outlets in the past, was arrested and detained for 10 hours after being beaten and forced into a police car at gunpoint (see C7). **181**

In October 2022, police arrested Hafeiza Mousa, a journalist who was live-streaming via Facebook to share a protest of women traders in the Darfur town of Zalinje. The police detained her at the police station and took her phone without any legal process. **182**

In September 2022, Amira Salih of Ultra Sudan, an online news outlet, was arrested by police as she covered a protest in Khartoum. **183** She was beaten (see C7) and released later that day without charge.

In August 2022, Saif Eldien Adam Ahmed, an online activist from Darfur, was detained by police, beaten (see C7), and charged with defamation after posting online about the arrest of four Christians who were charged with apostasy. **184**

The government still places legal pressures on journalists using the vague terms in the LCC. Following the July 2020 amendments to the LCC (see C2), military officials announced that a new cybercrime commissioner would monitor and prosecute "insults" lodged against the army. **185**

In September 2022, the Journalists' Syndicate condemned the arrest of Abdalrahman al-Ajib, who was arrested by police due to publishing an article about a corruption case related to the Ministry of Minerals in a newspaper and on his Facebook account. He was charged under Articles 24 and 25 of the LCC. **186**

In October 2022, police filed a complaint against Osman Shabona, who reports for several online media outlets, after he wrote an article that criticized the police. ¹⁸⁷

In December 2022, a court heard the RSF's complaint against Rashan Oshi, editor-in-chief of the Morning News website, ¹⁸⁸ over her description of the organization as a "militia." ¹⁸⁹

In April 2022, during the previous coverage period, Sulaima Ishaq, the director of the Combating Violence against Women Unit, was sued by the GIS because she allegedly "leaked" information to online outlet Alintibaha about two rape cases associated with Sudanese security forces. ¹⁹⁰

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 the tension between the RSF and GIS. ¹⁹¹ Hisham Ali, ¹⁹² a Saudi Arabia-based online activist and blogger, was arrested by Saudi authorities in late 2017 and transferred to Sudan in May 2018. ¹⁹³ He was detained until his release in April 2019. ¹⁹⁴

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.

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 ID number. ¹⁹⁵ 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 the camera, microphone, files, and other features of a target's smartphone after a URL click. ¹⁹⁶ In April 2023, the Greek government admitted to allowing Predator's export to Sudan. ¹⁹⁷

SMEX reported that the RSF has been inspecting the contents of citizens' phones since the outbreak of armed conflict in Khartoum in April 2023. ¹⁹⁸ While torturing and interrogating freelance photojournalist Faiz Abubaker (see C7), RSF members also went through his Facebook account before releasing him.

Sudanese authorities used their access to mobile networks to trace the locations of and arrest some activists after the October 2021 coup. ¹⁹⁹ The Emergency Lawyers Committee disclosed that security forces subpoenaed phone histories and tracked personal cell phones for a number of arrested anti-coup protestors during interrogations. ²⁰⁰ Additionally, during the October 2021 protests, security forces allegedly inspected participants' mobile phones to delete evidence of rights abuses committed by security officers. ²⁰¹ For instance, a political activist and a lawyer wrote a Facebook post in which she claimed that an army officer asked to examine photographs; when she refused, she was taken to a police station. ²⁰²

After word spread that security officers were searching devices, protesters developed a number of tactics to protect themselves digitally (see B8).

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.” ²⁰³ 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.” ²⁰⁴

The NISS regularly intercepted private email messages with the aid of sophisticated surveillance technologies. An industry source argued that he has strong reason to believe 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. ²⁰⁵ Another pressing issue is the lawful interception clause in the contracts users sign with telecommunication companies, which is intentionally broad and gives the authorities the right to tape one’s phone without clear evidence of criminal conduct or an ongoing investigation. ²⁰⁶

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. ²⁰⁷ 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. ²⁰⁸

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 December 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. **209**

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. **210**

An activist who was summoned for questioning in early 2018 **211** 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. **212**

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. **213**

Between January and July 2022, Meta did not receive any requests for data from the Sudanese government. **214** This was the first period since 2013 for which Meta did not receive such requests.

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?

1/5

Score Change: The score declined from 2 to 1 because officials used verbal threats and physical violence in retaliation for users' online activities.

Online journalists and activists often face extralegal intimidation, harassment, and violence in retaliation for their online activities. Violence against both online and traditional journalists 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.

On May 18, 2023, RSF soldiers stopped freelance journalist Eissa Dafaallah, who also reports using his Facebook account, while he was filming after fighting in Nyala, in Darfur. He was beaten even after identifying himself as a member of the press, and had his mobile phone and money stolen. **215**

On May 11, 2023, RSF forces stormed the offices of independent newspaper *Al-Hirak al-Siyasi*, which also publishes online, reportedly threatening staff members and looting equipment. **216**

On May 1, 2023, 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 for three hours, threatened at knifepoint, and beaten. **217** The RSF also went through the contents of his Facebook account and released him after he was able to prove that he was not affiliated with the SAF. **218** Abubaker fled to Egypt after recovering from his wounds.

On social media, including WhatsApp and Facebook, lists of names of journalists alleged to be working for either side in the conflict have been circulated by anonymous accounts, potentially putting their lives in danger. **219** One journalist whose name was among those circulated reported receiving multiple death threats over WhatsApp. **220** A female journalist received threatening WhatsApp messages after she criticized the RSF in a private WhatsApp group for Sudanese media workers. **221** 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. **222**

In March 2023, journalist Ikhlas Nimir, who sometimes shares reporting from her public Facebook page and has worked for online media outlets in the past, was

beaten by ten police officers and forced into a police car at gunpoint, where she was forcibly detained for ten hours after she took out her phone to record the demolition of homes in Khartoum (see C3). **223**

In January 2023, Azza Aira, an activist from Eastern Sudan, posted on Twitter that she received a threat from the governor of the Red Sea State, Mohamed Adroub Kalmoub. **224**

In September 2022, Amira Salih of Ultra Sudan, an online news outlet, was beaten with sticks while in detention by police after her coverage of a protest in Khartoum (see C3). **225**

The RSF information department manager sent a direct threat to the editor of the Monte Carro investigative website in September 2022. **226**

In August 2022, Saif Eldlien Adam Ahmed, an online activist from Darfur, was beaten while in detention after posting online about the arrest of four Christians who were charged with apostasy (see C3). **227**

In July 2022, Omer Arbab, a former military officer who became an online advocate, received a call from Ibrahim Jabir, a member of the TSC, saying that he was being watched and that they were able to “destroy him.” **228**

Security forces harassed protesters for their online activity during the coverage period, and authorities made attempts to restrict their online activities (see B8). Activists and protesters detained in recent years were subjected to torture by the authorities. Activists reported numerous cases of violent arrest by security forces and torture while in custody. **229**

Several activists, particularly women, have been targeted by harassment campaigns in the past. The campaigns appeared to be led by trolls mobilizing internet users opposed to women’s rights, especially in relation to Islam. In January and February 2021, Hanan Hassan, a lawyer and politician, was targeted with continuous reporting of her Facebook page, as well as online threats and harassment after making a controversial statement about the prophet Muhammad and one of his wives. **230** She now uses another Facebook account and has changed her name on the platform. Tahani Abbas, an activist with No to Women’s Oppression, was the subject of a troll campaign; personal pictures of her were

circulated with derogatory comments, along with comments labeling women's rights activists in general as apostates, communists, and prostitutes. ²³¹

Minority groups such as LGBT+ people are also frequent targets of online harassment. ²³²

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

Cyberattacks were reported less frequently during the coverage period than in previous years.

In January 2023, the official Facebook page of the Almareikh football club was hacked by the "Sudan Cyber Security" hacking group, ²³³ after an individual tied to RSF commander Dagalo became the club's president. ²³⁴

In November 2022, the government released a statement that an inauthentic website was impersonating the official Sudan News Agency site. ²³⁵

In previous years, independent news sites have been subjected to technical attacks, which many believe are perpetrated by the cyberjihad unit (see B5). Attacks usually intensify around significant political events and unrest, while some prominent news sites ward off daily distributed denial-of-service 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 2023: Sudan," DataReportal, February 14, 2023, <https://datareportal.com/reports/digital-2023-sudan>.
- 2 International Telecommunications Union, "Digital Development Dashboard: Sudan," accessed August 18, 2023, <https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Develo...>
- 3 Speedtest, "Sudan Median Country Speeds," accessed August 18, 2023, <https://www.speedtest.net/global-index/sudan#mobile>.

- 4 International Telecommunication Union, “Fixed Broadband Subscriptions, 2000-2020,” accessed August 18, 2023, <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>.
- 5 Sudatel Sudan, “Good News from Sudatel!,” April 21, 2022, <https://www.sudatel.sd/blog/2022/04/21/good-news-sudatel/>.

More footnotes



On Sudan

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

See More [➤](#)

Country Facts

Global Freedom Score

10 / 100 Not Free

Internet Freedom Score

30 / 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 2023

Other Years

2022

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

@2024 FreedomHouse