Sudan

Not Free

25

100

A Obstacles to Access  5 25
B Limits on Content     12 35
C Violations of User Rights 8 40

Last Year's Score & Status

35 100 Not Free

Overview
Internet freedom in Sudan suffered as the country experienced mass protests, a harsh response from the government, and the ouster of long-time president Omar al-Bashir. In response to the uprising, the government instituted social media blocks and continued to regularly arrest and harass people in retaliation for their online activities. New legal restrictions passed in the summer of 2018 established additional penalties for online expression and the suspension of the constitution in April 2019 opened the door for more abuses of fundamental rights.

Until his removal in a 2019 coup, Sudan’s political system was dominated by an authoritarian president, Omar al-Bashir, and the National Congress Party (NCP), which has relied on repression and inducements to maintain power. Under military rule, security forces have cracked down on peaceful protests, while officers have maneuvered to maintain military control of key components of the government.

Key Developments

June 1, 2018 - May 31, 2019

- Numerous electrical outages hampered internet access during the coverage period (see A1 and A3). Although technical problems were blamed in some instances, a number of outages coincided with mass protests, raising questions about whether they were intentional.

- The economy continued to deteriorate, with inflation topping 70 percent in December 2018. The high relative cost of internet service made it less accessible to many Sudanese users (see A2).

- The government instituted multiple social media blocks, including around mass protests; one such block continued for two months (see A3 and B1).
Social media platforms were crucial in organizing mass protests that began in December 2018 and continued through the end of the coverage period. However, the government employed a number of tactics to prevent the use of social media for mass mobilization (see B8).

- Following al-Bashir’s ouster in April 2019, the constitution was suspended and a curfew and state of emergency were announced, threatening fundamental rights, including for online activists and journalists. This followed al-Bashir’s declaration of a state of emergency in February (see C1).

- In June 2018, the National Assembly passed the Law on Combating Cybercrimes of 2018, which introduced criminal penalties for spreading fake news online (see C2).

- Amendments to the Media Law (also known as the Press and Publications Act) imposed restrictions on online journalism and social media, including by requiring online journalists to register with the Journalism Council, which has the power to suspend publications and prevent online journalists from posting content it objects to (see C2).

A Obstacles to Access

Economic challenges intensified as inflation increased, resulting in higher prices for internet access and declining quality of service during the reporting period. There were multiple social media blocks during mass protests preceding al-Bashir’s ouster, one of which lasted for two months. Electricity outages also disrupted connectivity.

A1 0-6 pts
Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?

Internet penetration remains low, with 30.9 percent of individuals using the internet
as of 2017, according to the International Telecommunication Union (ITU). The ITU also reports that as of 2018, less than 1 percent of the population had a fixed-broadband subscription. Meanwhile, the 2018 GSMA Mobile Connectivity Index reports that 39 percent of the population has a mobile broadband connection. However, these figures are based on the total number of SIM cards, so the reported penetration rate may be inflated by individuals who have multiple SIM cards. Nevertheless, the available data suggests that most internet users have mobile subscriptions.

An unreliable electricity supply limits internet service in Sudan, including in major cities that have been subject to periodic power rationing due to electricity price increases. Most rural areas have unsteady access to electricity or none at all. Power cuts usually peak in the summer when demand for electricity is highest, especially in Khartoum, where a growing population and severe weather have intensified demand. Khartoum accounts for approximately 70 percent of the country’s electricity usage. Multiple blackouts occurred in January and February 2019, allegedly due to technical issues. However, many observers suspect that the blackouts were intentional and meant to disrupt the protests against the regime. Another outage occurred in April 2019 (see A3).

- 3. http://www.mobileconnectivityindex.com/#year=2018&zonelsocode=SDN&analy...
- 4. Sudan may have to stay in the dark a bit longer after Egypt postpones plans to supply electricity to the country
- 5. https://arabicpost.net/%D8%A7%D9%84%D8%A3%D8%AE%D8%A8%D8%A7%D8%B1/m...; https://arabic.sputniknews.com/arab_world/201902151039075189-%D8%A7%D9%...
Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?

Internet access is prohibitively expensive for many users, and the economic crisis increased relative prices further during the coverage period.

In a continuation of the economic deterioration that began in 2011, sustained petroleum scarcity led to inflation and higher prices in 2018. Sudan’s inflation rate remained high, at just over 40 percent in January 2019, which was a decrease from the 72.9 percent rate reported in December 2018. The central bank imposed limits on cash withdrawals during the reporting period, further limiting citizens’ ability to pay for goods, including internet service.

A month of fixed-line internet service can cost nearly half of the average monthly income in Sudan. In August 2019, after the coverage period ended, telecommunications companies reportedly raised internet subscription fees by 15 percent.

2. https://af.reuters.com/article/sudanNews/idAFC6N1T801O
3. https://www.reuters.com/article/sudan-energy/fuel-shortage-hits-sudan-a...
5. https://www.dabangasudan.org/en/all-news/article/sudan-internet-fees-ri...

A3 0-6 pts

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

The government frequently exercises control over the internet infrastructure, and did so on numerous occasions in the midst of antigovernment protests in late 2018 and early 2019.

Internet service providers (ISPs) blocked WhatsApp, Facebook, Twitter, Periscope, and Instagram from December 21, 2018 through February 26, 2019, according to the digital rights organization NetBlocks. The block was instituted less than a week
into nationwide protests that began in December. Users were able to access the blocked social media and messaging platforms through virtual private networks (VPNs), which users could generally only download with a strong wireless connection. NetBlocks stated in a study that Zain had the most “extensive blocking scheme” among providers. Users reportedly lost internet connectivity a day after the mass protests erupted in Khartoum in December. Multiple electricity outages in January and February coincided with the protests and social media block, raising concerns that the outages were intentional (see A1).

On April 7, 2019, a day after hundreds of thousands of protesters marched to the army headquarters in Khartoum, social media platforms were again blocked, including Telegram, which is used widely by activists and had remained accessible during the initial block from December to February. Several widely used VPN platforms such as Hotspot Shield, ExpressVPN, and others were reportedly blocked. Users struggled to find a VPN to download. The block was lifted on April 11, the day al-Bashir was ousted in a coup.

A power outage on April 7 coincided with mass protests and the social media block. NetBlocks reported that a few hours after the social media block was reported, 45 percent of telecommunications services were disabled by power outages that affected mobile service providers and fixed-line internet service. The Ministry of Water Resources, Irrigation and Electricity did not provide an explanation for the blackout.

After the coverage period, Sudan experienced a “near-total” network shutdown, which began on June 3, 2019 and lasted for over a month.

Sudan is connected to the global internet through international gateways controlled by the partly state-owned Sudan Telecom Company (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 largest cable.

1. https://netblocks.org/reports/study-shows-impact-of-sudan-internet-disr...
2. https://qz.com/africa/1510229/sudan-shuts-down-facebook-twitter-instagr...
3. https://netblocks.org/reports/study-shows-impact-of-sudan-internet-disr...
4. Social media disrupted in Sudan as protests converge in Khartoum-
Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?

There are no legal or regulatory obstacles that restrict the diversity of service providers, but there are economic constraints. Canar, one of the four licensed telecommunications providers in Sudan (offering fixed phone and home internet service) was partially owned by the Emirati mobile service provider Etisalat. However, in 2016 Etisalat sold its shares in the company to the Bank of Khartoum for $95 million.\(^1\) The bank used its 3.7 percent share in Canar to block Zain’s efforts to purchase it.\(^2\) Observers believe that the government’s move to increase its market share in the telecommunications industry will have a negative impact on internet freedom and reduce the dynamism in the market.

Three other licensed telecommunications providers operate in Sudan: Zain, MTN, and Sudatel. MTN and Zain are primarily foreign owned.\(^3\) The government owns more than a 20 percent share in Sudatel\(^4\) and reportedly has significant sway over the company’s board of directors.\(^5\)

Zain also has some apparent links to the government. According to a local source, in April 2019 Zain Sudan appointed Osama Kahin as its new general manager. Kahin is seen as an independent figure, unlike his predecessor, Al-Fatih Erwa, who is a former security officer. Erwa remained in the company, but due to his former positions in the security apparatus, his profile will be much lower.

\(^1\) Etisalat completes sale of Sudanese telco Canar-
\(^2\) Etisalat completes sale of Sudanese telco Canar-
\(^3\) https://www.zain.com/en/investor-relations/shareholders-dividends/ ;
http://documents.worldbank.org/curated/en/561781468202137788/Sudan-infr...
; https://uk.reuters.com/article/emirates-sudatel/sudatel-plans-to-invest...

5. According to a local source.

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?

The regulatory bodies that oversee service providers lack independence. Sudan’s National Telecommunication Corporation (NTC)\(^1\) is housed under the Ministry of Communications and Information Technology. The NTC is tasked with producing telecommunications statistics, regulating internet use, facilitating the introduction of new technologies, and developing the telecommunications and information technology (IT) industries. It is also responsible for determining what content is accessible on the internet (see B3), so is therefore implicated in the social media blocks that occurred during the coverage period.

According to a local source, Dr. Yahia Abdallah Hamad was abruptly removed from his position as director of the NTC in December 2018 by presidential decree, and Mustafa Abdel Hafeez replaced him.\(^2\) According to an apparent source within the NTC, Hamad was allegedly removed because he refused to obey the orders of the National Intelligence and Security Service (NISS) to shut down the internet and block access to social media platforms. However, Hamad quickly dismissed the story as fraudulent.\(^3\)

Although it is a state body, the NTC receives grants from international organizations such as the Intergovernmental Authority on Development and the World Bank, and its website describes the body as “self-financing.” The NTC received praise from the Council of Ministers for supervising the national SIM card registration campaign in late 2017 (see C4).

1. In March 2018, the NTC’s website was down.
2. According to a local source and
http://www.presidency.gov.sd/eng/news/A%20presidential%20decree%20appoi...
B Limits on Content

Social media platforms that were critical in mobilizing the protests that began in December 2018 were blocked during parts of the coverage period. The government’s so-called “cyber jihadists” worked to thwart the movement by disseminating misinformation.

B1 0-6 pts
Does the state block or filter, or compel service providers to block or filter, internet content?

The Sudanese government openly acknowledges blocking and filtering websites that it considers “immoral” and “blasphemous,” such as pornography sites. Political or social content was last blocked in 2012, when the online news outlet SudaneseOnline and Facebook were intermittently inaccessible, and the "Innocence of Muslims" YouTube video was blocked.

However, the government’s extensive social media blocks during the coverage period (see A3) curtailed the sharing of political and social content during the mass protests that began in December 2018. Social media was instrumental in organizing the demonstrations that continued through the end of the report’s coverage period. Blocking social media platforms was intended to disrupt the ability to access information related to the protests. However, many people were able to access social media through VPNs. Many users without VPNs on their phones paid specialists at technology shops around Sudan that were willing to install them. In April 2019, a number of free VPNs, such as Hotspot Shield, became inaccessible, which forced some users to again pay for the installation of VPNs that remained available.1

1. Author’s research.
Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?  

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 (see C7). This practice became more common after the protests began in December 2018. The NISS and individuals affiliated with the government harassed and intimidated users to delete content they objected to from Facebook groups.1

Prepublication censorship was prevalent during the reporting period, and several newspapers were reportedly banned for a number of days. Al-Jareeda, one of Sudan’s few independent newspapers, was repeatedly confiscated or banned from publishing. Although the newspaper continued to publish on its website and Facebook page, authorities also threatened to shut down its online presence. However, the paper continued to publish online through the coverage period.2

1. Interviews conducted by author.
2. Interview with Khalid Ahmed, member in the executive committee of the sudanese journalists network, 20 May 2019.

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

The NISS and the NTC were nontransparent surrounding the social media blocks and network shutdowns during the coverage period. In December 2018, NISS head Sala Abdallah admitted that the government was responsible for blocking social media platforms, but the NTC did not provide further information about the decision.1

The NTC manages online censorship through its internet service control unit and is somewhat transparent about the content it blocks, reporting that 95 percent of blocked material is related to pornography,2 though the regulator has acknowledged that it has not succeeded in blocking all “negative” sites in Sudan.3 The NTC also requires cybercafé owners to download blocking and filtering software.4

The NTC’s website gives users the opportunity to submit requests to unblock
websites “that are deemed to not contain pornography,” but it does not specify whether the blocking of political websites can be appealed. Users attempting to access a blocked site are met with a page stating, “This site has been blocked by the National Telecommunications Corporation,” which includes links to further information and a contact email address. In addition to the NTC, the general prosecutor has the power to block any site that threatens national security or violates social mores.

1. https://www.reuters.com/article/us-sudan-protests-internet/sudan-restri...
4. “Sudanese intelligence prosecutes Internet content that ‘threatens the morals of the nation’,” Alhayat, February 29, 2016, http://www.alhayat.com/article/734492/ةيدوعسلا-تايلحم-/جيلخلا-/ارابختسالا...
5. NTC, “Blocking Or Unblock Websites.”
6. Image of a blocked site: https://docs.google.com/file/d/0B6mgwvplJ6IadERXTZW1jSkk/edit?pli=1

Do online journalists, commentators, and ordinary users practice self-censorship?

Government threats against online journalists and internet users has led to growing self-censorship in recent years. 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. WhatsApp, for example, is particularly popular in Sudan due to the platform’s privacy and anonymity features. Telegram was also widely used during the antigovernment protests.

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


• 2. As described by analyst.

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?

Although Sudan has a vibrant online information landscape, the government frequently manipulates internet content to advance its agenda. The government employs a concerted and systematic strategy to spread disinformation and manipulate online discussions on social media through its so-called cyber jihadist unit. Established in 2011 in the wake of the Arab Spring, the unit is part of the NISS and works to proactively monitor content posted on blogs, social media platforms, and online news forums.\(^1\) The unit also infiltrates online discussions in an effort to collect information about dissidents and is believed to orchestrate technical attacks against independent websites, especially during political events (see C8).\(^2\)

Recently, the unit has increasingly spread fake news in order to muddle public debate and discredit independent media outlets and activists who unknowingly circulate the fraudulent stories. Many pictures, videos, and stories circulated on social media during the coverage period were confirmed to be fake news.

For example, in January 2019, reports surfaced that at least three people were killed when police used live ammunition against demonstrators in Khartoum, including a teenager named Mohamed al-Obeid. Local journalists quickly shared his image on social media, and the story soon spread to international news outlets. As activists attempted to ascertain more details about the boy’s identity, suspicion grew, until it became clear that the image depicted the aftermath of police violence in Brazil. Sudanese activists asserted that the fraudulent story originated with a team of NISS internet trolls known for disseminating smears and falsehoods.\(^3\) According to activists, the incident provided an opportunity for the government to discredit the media and influential civil society organizations that shared the tweet, such as the Central Committee of Sudan Doctors and Sudan Change Now.\(^4\)
Cyber jihadists worked to thwart the so-called “bread protests” that took place in early 2018. Their strategies included posting pictures from war-torn areas of Syria to demonstrate a higher quality of life in Sudan and spreading commentary that rejected social media posts about the high prices of medicine and basic goods. The cyber jihadists also spread misinformation about the protests being a deliberate ploy to destabilize Sudan and disseminated propaganda that claimed the government was effectively handling the economic situation.

The unit also apparently abuses mechanisms to report social media accounts for violating platforms’ community standards, which sometimes leads to accounts being shut down or blocked. Additionally, the unit floods platforms with coordinated posts, hashtags, and messages in an effort to sway public opinion.

- **3.** Research conducted by analyst and [https://twitter.com/YousraElbagir/status/108667123284805890](https://twitter.com/YousraElbagir/status/108667123284805890)
- **4.** [https://twitter.com/Sd_Doctors/status/1086767221815287809?](https://twitter.com/Sd_Doctors/status/1086767221815287809?); [https://twitter.com/Sudanchangenow/status/1086772829478182913](https://twitter.com/Sudanchangenow/status/1086772829478182913)
- **5.** It should be noted that activists rarely use the term “Cyber Jihad Unit”, in fact they refer to thee affiliated with this unit as "electronic chickens" as of 2012.

B6 0-3 pts
Are there economic or regulatory constraints that negatively affect users’ ability to publish content online?

There are a number of economic and regulatory constraints that negatively affect users’ ability to publish content online. Tight government control of the media environment has prevented independent online news outlets and journalists from becoming economically viable. Polarization further constrains the development of sustainable independent journalism. **1**

Furthermore, the amendments to the Media Law that were passed in 2018 (see C2) require online news outlets to register with the Journalism Council, which has the
power to suspend publications and prevent online journalists from posting content it objects to. As registered outlets, online publications are required to have a physical office, which many news sites previously avoided due to security and financial concerns.

According to a local source, there are numerous news sites that are financed by the government, such as Al-Nileen. In 2017, a news site called Bajnews became the first online publication founded and funded by a businessperson in Sudan; all other news sites are funded by either the government or donors.

- 1. FH interview with author.
- 3. As in the case of Hurriyat, Al-Rakoba, Al-Taghyeer, Al-Tareeg.

B7 0-4 pts

Does the online information landscape lack diversity? 24

Compared to the highly restrictive space in the traditional media sphere, which is characterized by prepublication censorship, confiscations of entire press runs of newspapers, and warnings from NISS agents against reporting on certain taboo topics, 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-tareeq, Altaghyeer, Radio Dabanga, Hurriyat, and Alrakoba cover controversial topics such as corruption and human rights violations.
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.6

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.

However, the economic crisis and associated rise in the cost of internet access has negatively impacted the quality of content available, mainly because users are less likely to access higher-quality content, or do not access online content at all, due to the high cost of data (see A2). Many people share information on WhatsApp, which uses less data than other platforms.

- 1. NISS confiscates newspapers covering Sudan crises
- 3. Al Tareeq was established in January 2014.
- 4. Altaghyeer [Arabic for change with political connotation] was established in 2013 following the government’s crackdown on independent journalists, who were eventually banned from practicing traditional journalism in Sudan.
- 5. Launched from the Netherlands in November 2008, Radio Dabanga focuses on reporting on Darfur and has a strong online presence and wide audience in conflicts areas. It website is bilingual and runs in depth reports and features. It is a project of the Radio Darfur Network. Dabnga, “About Us,” https://www.dabangasudan.org/en/about-us.
The blocking of social media platforms during the coverage period curtailed the ability of activists to mobilize the antigovernment protests. The internet is an increasingly important tool for mobilization, since many activists fear arrest if they hold public meetings.1

Social media and communications platforms were critical in organizing protests in early 2018, as well as the protests that began in December 2018 and ultimately led to al-Bashir’s ouster.2 However, the government’s blocks of social media platforms and disruptions to network coverage limited the ability of activists to organize the protests (see A3). Ordinary users worked around the blocks by utilizing VPNs that are free of charge and circulating instructions on downloading VPNs, which allowed many users continued access to social media platforms (see A3).

The government’s blocking and network disruption scheme was clearly intended to disrupt mobilization efforts, as evidenced by the armed NISS and Rapid Support Forces (RSF) agents who stopped protesters and searched their phones for videos, posts, or pictures about the ongoing demonstrations.3 One eyewitness and his friend were stopped on Nile Street in Khartoum by an agent who requested their phones. Both individuals anticipated such an encounter and hid their phones in their car. “Everyone who had pictures and videos on the protests was arrested in front of us,” said the eyewitness in an interview.4

Another source said that her colleague was stopped and searched, and that security agents did not believe that she only had a basic mobile phone, which led them to search for a smartphone in her car.5

After accounts of such practices by security agents spread online, protesters sought to protect themselves by deleting social media apps and information received on Whatsapp and other platforms. Some demonstrators bought a separate phone to use at protests or when they perceived a threat from security forces.6 Protesters also used functions available on some phones that allow users to switch to a guest account that would have less apps available, and therefore less incriminating information.7

Between December 2017 and February 2018, mass protests broke out against the government’s handling of the poor economy and proposed tax increases.8 The “bread protests” were largely organized through Facebook, Twitter, and WhatsApp and led to the participation of an unprecedented number of ordinary citizens. Some
government officials threatened WhatsApp, blaming it for the spread of rumors and leaked information, among other issues. For example, local sources report that during the height of fuel shortages in April 2017, the finance minister told the press that he held WhatsApp responsible for the fuel crisis by spreading false information and panic about fuel prices.

During the protests in late 2017 and early 2018, cyber jihadists attempted to shut down popular Facebook pages disseminating information about the demonstrations by reporting the pages en masse. Social media was the main source of news about the protest movement.

- 1. Several meetings and workshops have been raided by the NISS and professionals were arrested. On January 31st, at least 30 lawyers were arrested as they held a meeting on providing legal aid to detainees. Additionally, several CSOs have partially shut-down operations out of fear of reprisals or shutdown.
- 3. Ongoing at end of coverage period.
- 4. Interview with Z.A, an activist, 10 February 2019
- 5. Interview conducted with R.A.
- 6. This became very common and it started to get the nickname “the protest phone” and it is often a second-hand or older phone and sometimes it is a normal and not a smart phone.
- 7. This was shared on Twitter and other social media outlets.
- 8. Export taxes on non-essential food items increased to almost 40% while tariffs on cars increased by 300%. The increase in car tariffs forced the tariffs authority to have to accept instalments as thousands were unable to pay the fees to bring their cars into the country.

C Violations of User Rights

A new cybercrime law and amendments to the Media Law introduced new restrictions on online activities. Numerous arrests and interrogations of online journalists and activists were reported and users commonly face harassment.
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?

Although the constitution guarantees freedom of expression and other fundamental rights, they are frequently curtailed in practice, including for those who publish content online. Constitutional rights were systematically undermined by states of emergency declared during the coverage period.

When the army ousted al-Bashir in April 2019 following four months of popular protests, the new transitional military council announced the suspension of the constitution, a state of emergency, and a curfew, which threatened the rights of online journalists and activists. Earlier in the year, in February, al-Bashir declared a state of emergency, which also undermined basic constitutional rights.

In the past, the Constitutional Court has ruled in favor of prepublication censorship if it is deemed in the interest of national security.

1. https://www.washingtonpost.com/world/africa/sudans-military-expected-to...

Are there laws that assign criminal penalties or civil liability for online activities?

There are a number of laws that can be used to penalize online activists, journalists, and ordinary users in retaliation for legitimate content.
In June 2018, the National Assembly passed the Law on Combating Cybercrimes of 2018, which introduced criminal penalties for the spread of fake news online. According to the Social Media Exchange (SMEX), a digital rights organization, Article 23 of the law 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.”

Amendments to the highly restrictive Media Law passed in 2016 include specific clauses that address online journalism. The amendments extend onerous restrictions long placed on the traditional press to the online sphere, such as provisions that assign fines to journalists and publications found to undermine public order or national security and hold editors-in-chief criminally responsible for all content published by their outlets.

The Informatic Offenses (Combating) Act of 2007, which provides the basis for the new cybercrimes law, criminalizes the establishment of websites that publish defamatory material and content that disturbs public morality or public order. Those found in violation of the law face fines and prison sentences of between two and five years.

National security imperatives also open journalists up to arrest. The 2010 National Security Act gives the NISS immunity from prosecution and the ability to arrest, detain, and censor journalists under the pretext of national security.

1. https://smex.org/do-new-sudanese-laws-regulate-digital-space-or-limit-f...
2. https://smex.org/do-new-sudanese-laws-regulate-digital-space-or-limit-f...

According to Section 4, crimes against public
order and morality Sudan cyber law, of Sudan’s Cybercrime Law (2007), intentional or unintentional producing, preparing, sending, storing, or promoting any content that violates public order or morality, makes the offender liable to imprisonment of 4 to 5 years or a fine or both. The maximum penalty for committing both crimes is 7 years or fine or both. Also, under the same section, creating, promoting, using, website that calls for, or promote, ideas against public law or morality is punished by 3 years in prison or fine or both. Cyber defamation crimes necessitate 2 years in prison or fine or both. Public order is not defined clearly in the law. Subsequently, most of the opposition content online falls under this section making online activists liable under this law.


Are individuals penalized for online activities? 26

Arrests, prosecutions, and interrogations for online activities continued during the coverage period, particularly as heavy-handed censorship of the print and broadcast sectors led journalists to migrate online to disseminate news. The arrests reflected government efforts to limit internet freedom by silencing critical voices and intimidating online journalists and users into self-censorship. In a positive development, an estimated 800 protesters and activists, many of whom were held for months, were released after al-Bashir’s ouster in April 2019. However, the subsequent violent crackdown on protesters and activists by security forces in June, after the coverage period ended, raised concerns about continued violations of user rights.

At least 79 journalists were arrested as the protests escalated between December 2018 and February 2019, and several were held in detention for weeks. A number of journalists and bloggers were penalized for content published online. For example, in January 2018, Faisal Mohamed Saleh, an online journalist for Al-Araby and Altaghyeer, was arrested and interrogated for his coverage of the protests. Online journalist Ghurashi Awad was arrested on the same day and also interrogated for his coverage of the protests. Awad was reportedly detained for over a month.
In January 2019, the Sudania 24 television network reported that the State Security Prosecution had produced arrest warrants for 38 journalists and activists, including those who publish online, for incitement and publishing fake news. According to reports, 28 of the 38 people targeted by the warrants were living outside Sudan. Their names were not revealed, which created more fear among journalists and activists. The government has reportedly explored using Interpol to pursue those living abroad. Authorities have pursued online activists based outside Sudan before, particularly those who live in Saudi Arabia. For example, Hisham Ali, an online activist and blogger based in Saudi Arabia, was arrested by Saudi authorities in late 2017 and transferred to Sudan in May 2018. He was detained until his release in April 2019.

A number of people near protest sites were reportedly stopped by security forces, who searched their phones for digital content related to the demonstrations. If protest-related content was found on their phones, including pictures, videos, and online posts, they were arrested (see B8).

1. http://www.acjps.org/sudan-hundreds-of-peaceful-protesters-and-activist...
2. https://www.nytimes.com/2019/06/04/world/africa/sudan-war-facts-history...
3. “At least 79 journalists arrested in two months of protests in Sudan”
5. http://www.civicmonitor.org/radio-dabanga-releases-list-of-detained-jou...
6. “Sudan issues arrest warrant for 38 journalists, activists”
8. “Sudanese activist deported from Saudi Arabia detained in Khartoum “

C4 0-4 pts
Does the government place restrictions on anonymous communication or encryption?

The government does not directly restrict encryption, but SIM card registration requirements limit anonymous communication.

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 given a deadline of December 31, 2017 to register their phone numbers using their national identity cards, which include detailed personal information such as home address and birthplace. These requirements enable the government to access mobile user information, limiting anonymity.

C5 0-6 pts
Does state surveillance of internet activities infringe on users’ right to privacy?

Unchecked surveillance of ICTs 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 NISS regularly intercepts private email messages with the aid of sophisticated surveillance technologies.

According to 2013 research published by Citizen Lab, a Canadian digital rights organization, Sudan possesses high-tech surveillance equipment produced by the American technology company Blue Coat Systems, which manufactures monitoring and filtering devices. The surveillance system was initially traced to three networks inside Sudan, including the networks of the private telecommunications provider Canar. 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. According to a local expert, the software was installed through the Wi-Fi modem shared by the group and enabled the comprehensive monitoring of their online activities.

• 2. Based FH consultant interviews, March 2018.

C6 0-6 pts
Are service providers and other technology companies required to aid the government in monitoring the communications of their users?

Service providers are required to aid the government in the surveillance of their
users. 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.

An activist who was summoned for questioning in early 2018 noted that an NISS officer told him that because authorities have access to the national ID system and the user information stored by telecommunications companies, they could collect extensive information about mobile users with just their phone numbers.

Telecommunications providers can be compelled to aid the government in monitoring the communications of their users, but authorities reportedly have a tighter grip on Zain and Sudatel than MTN. The NISS allegedly has significant involvement in telecommunications providers’ hiring processes, and NISS agents are apparently sometimes embedded within the companies.

- 1. Interview over the phone. 23 February 2019

C7 0-5 pts
Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?

Online journalists and activists often face extralegal intimidation, harassment, and violence in retaliation for their online activities. During the coverage period, the frequency of such incidents increased significantly, particularly surrounding the antigovernment protests. A number of protesters who posted on social media were harassed by security agents around the mass demonstrations.

In March 2019, journalist Ezzeldeen Dahab was summoned by the NISS and interrogated for several hours about his social media posts. He was forced to sign a statement committing to not incite the regime.

During the coverage period, an editor working at Altaghyeer removed his name from the site to avoid legal action and harassment after he was threatened in retaliation for a series of articles about the RSF, a paramilitary group that was created by al-Bashir. The RSF’s head, Lieutenant General Mohamed Hamdan Dagalo (commonly known as “Hemetti”), was the deputy head of the Transitional Military Council (TMC).
In several instances during the coverage period, Sudanese nationals living outside of the country were subject to harassment. In February 2019, a Sudanese professional (who wished to remain anonymous) living abroad posted on Monbrshat, a women’s Facebook group, about information she received regarding a Sudanese man in Turkey who facilitates the purchase of tear gas for the Sudanese government. Her post was subsequently reported and she experienced extensive harassment on social media, as well as threatening phone calls. A picture of the woman and her husband were also posted on social media with their full names. Her sister received a threatening call as well.4 The Facebook group continued to endure online attacks as it posted pictures and information about NISS and other government officials.

Social media influencers and minority groups such as the LGBT+ community are frequent targets of online harassment. Women activists are often victimized by threats and smear campaigns on social media. In one prominent example from recent years, over 15 female activists were doxed on the fake “Sudanese Women against the Hijab” Facebook group, where their private pictures were posted without their consent alongside fabricated quotes about their supposed opposition to the veil and Islam. Some of the victims feared for their lives in the face of threats of violence from religious fundamentalists. Two victims reported this page to the cybercrimes prosecution office, which took no action. Instead, one of the victims was shamed and scolded for posting her picture online. The page was only shut down in 2017 after international human rights groups brought attention to the issue.

- 1. “Darfur journalists condemn the summoning of Ezzeldeen Dahab”(AR)- https://newspaper.sudafax.com/19676/%D8%A5%D8%B9%D9%84%D8%A7%D9%85%D8%A7%D8%AF% D8%AD%D8%A8%D9%84-%D8%A5%D9%88%D9%84-%D8%A7%D9%85%D8%A7%D8%AF% D8%AF%D9%88%D8%A7%D8%A8/
- 3. https://www.theguardian.com/world/2019/may/29/hemedti-the-feared-comman...
- 4. Author interview with S.A. in February 2019.

C8 0-3 pts

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

Government and news websites often face hacking and other forms of cyberattack.
In late 2018, Anonymous responded to the social media blocks by hacking government websites. In total, 260 websites were hacked and became inaccessible, including the sites of two progovernment television networks.1

Independent news sites are frequently subjected to technical attacks, which many believe are perpetrated by the cyber jihadist 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 during the reporting period, but they were able to respond by increasing their cybersecurity capabilities.

Throughout 2017, a Facebook page created by Sudanese women to post screenshots of sexual harassment incidents faced several hacking attempts following strong condemnation from numerous male users. The women also have a private group with over 7,300 members on social media called “Inbox messages,” where they share sexually inappropriate and aggressive messages from men on social media with one another.


Country Facts

- Freedom in the World Status
  - Not Free
Networks Restricted
Yes

Social Media Blocked
Yes

Websites Blocked
No

Pro-government Commentators
Yes

Users Arrested
Yes

Previous Reports

- 2018 Report