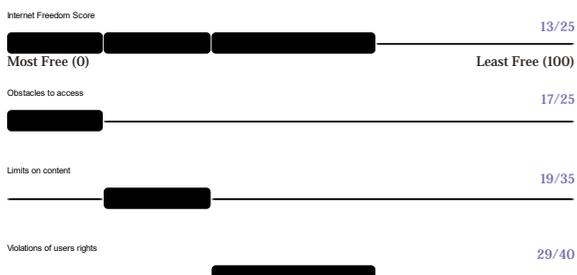


Sudan Country Report | Freedom on the Net 2018



Key Developments:

JUNE 1, 2017 - MAY 31, 2018

- Access to the internet became more challenging and expensive for Sudanese citizens amid a continually deteriorating economy (see Availability and Ease of Access).
- No online news outlet, social media, or communications platforms were restricted this year, though forced content removals became more prevalent (see Content Removals).
- While social media was critical for mobilizing protests against the economic crisis, the so-called Cyber Jihadists worked to thwart the movement by disseminating misinformation (see Media, Diversity, and Content Manipulation).
- A new cybercrime law and amendments to the media law introduced new restrictions on online activities (see Legal Environment).
- In July 2017, political activist Hatim Merghani was sentenced to two years in prison and a fine for publishing commentary on the corruption of a government official on WhatsApp and other social media channels. Numerous journalists and activists were also arrested or prosecuted for their online activities (see Prosecutions and Arrests for Online Activities).

Introduction:

Internet freedom in Sudan declined in the past year due to a crippling economic crisis that made access to ICTs prohibitively expensive for everyday users. The government also exerted increasing control over the online sphere by arresting online journalists and activists and introducing new restrictive laws.

In October 2017, the United States lifted economic, trade, and financial sanctions first imposed on Sudan in 1997, opening up opportunities for new companies to enter Sudan and fuel a long-awaited digital revolution.¹ However, the renewed hope was hampered by a massive economic downturn in late 2017 that saw the devaluation of the local currency and exponential spikes in inflation. Everyday citizens were hard-hit by the soaring prices of goods, including access to the internet.

So-called “bread protests” erupted in late 2017 through early 2018 against the government’s flagging response to the country’s deteriorating economy. Social media platforms were critical for mobilizing and documenting the protests, which were not covered in traditional media. Meanwhile, misinformation spread by the pro-government Cyber-Jihadist Unit tried to paint the protests as a deliberate ploy to destabilize Sudan and disseminated propaganda on how the government was effectively handling the economic situation.

The government sought to tighten restrictions on online activities in the past year, introducing a new cybercrime law and amendments to the media law (they were passed in June 2018, after this report’s coverage period). The cybercrime law announced criminal penalties for the spread of fake news online, while amendments to the media law require online journalists to register with the Journalism Council.

Meanwhile, the authorities continued to crackdown on online activities, sentencing at least one citizen to prison for critical commentary shared on social media and arresting numerous journalists and activists for alleged cybercrime.

Obstacles to Access:

Economic challenges intensified with high inflation rates in Sudan, resulting in higher costs and declining quality of services for Sudanese citizens in the past year.

Availability and Ease of Access

Access to the internet became more challenging for Sudanese citizens during the coverage period amid a continually deteriorating economy, which has raised the cost of living for many. In December 2017, the Central Bank of Sudan devalued the official rate of the SDG, while inflation rose to over 122 percent in January 2018,² compared to 30 percent inflation in December 2016.³ The operating environment for the ICT sector has also become more expensive, impacting both telecom companies and their subscribers.⁴ A month of fixed-line internet can cost nearly half of the average monthly income in Sudan.⁵

Consequently, internet penetration is still low at 29.6 percent, according to the latest available data from the International Telecommunications Union (ITU).⁶ Mobile phone penetration stood at 71 percent. The majority of internet users access the internet from their mobile devices, though only 22 percent of residents in the capital city, Khartoum, have a smartphone, compared to 9 percent of the total population.⁷

In addition to high prices, the quality of service for 3G users deteriorated as telecommunications companies tried to push people toward their 4G services, which is very expensive; as of mid-2018, 30 GB cost about 615 SDG (US \$34) and is not enough for an entire month of service.

Electricity shortages also limit internet services in Sudan, especially in major cities that have been subject to periodic power rationing due to electricity price increases. Most of the periphery areas have unsteady or no electricity 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. In January 2018, the country experienced a total electricity blackout, ironically during the president’s televised speech during which he was expected to address the economic situation.⁸ Another unexplained nationwide blackout occurred on February 27, 2018.⁹

Restrictions on Connectivity

There were no reported restrictions on connectivity during the coverage period.

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. Partial control over the international gateway has enabled the government to restrict internet connectivity during particular events in the past.

ICT Market

There are four licensed telecommunications operators in Sudan: Zain, MTN, Sudatel, and Canar. All are fully owned by foreign companies with the exception of Sudatel, in which the government owns a 22 percent share.¹⁰ However, the Sudanese government holds significant sway over Sudatel's board of directors, which includes high-ranking government officials.¹¹

Two providers, MTN and Sudatel, offer broadband internet, while Canar offers fixed phone lines and home internet. The Bank of Khartoum subsequently purchased Canar from UAE's Etisalat in June 2016, after the bank used its 3.7 percent share in Canar to block Zain's efforts to purchase it. Observers believe the government's move to increase its market share of the telecom industry will have a negative impact on internet freedom for Sudanese users due to the government's growing ownership of the market.

Regulatory Bodies

Sudan's telecommunications sector is regulated by the National Telecommunications Corporation (NTC),¹² which is housed under the Ministry of Telecommunications and Information Technology. The NTC is tasked with producing telecommunications statistics, monitoring the use of the internet, introducing new technology into the country, and developing the country's telecommunications and IT industry. It is also responsible for deciding what content should be accessible on the internet.

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 body received praise from the Council of Ministers for supervising the national SIM card registration campaign in late 2017 (see Surveillance, Privacy, and Anonymity).

Limits on Content:

No online news outlet, social media, or communications platforms were restricted this year, though forced content removals became more prevalent. Social media was critical for mobilizing protests against the economic crisis. The so-called Cyber Jihadists worked to thwart the movement by disseminating misinformation.

Blocking and Filtering

The Sudanese government openly acknowledges blocking and filtering websites that it considers "immoral" and "blasphemous." The NTC manages online filtering in the country 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,¹³ though the regulator has acknowledged that it had not been successful in blocking all "negative" sites in Sudan.¹⁴ The NTC also obligates cybercafé owners to download blocking and filtering software as a requirement to sustain their licenses.¹⁵

The NTC's website gives users the opportunity to submit requests to unblock websites "that are deemed to not contain pornography,"¹⁶ but it does not specify whether the appeals extend to political websites. Users attempting to access a blocked site are met with a black page that explicitly states, "This site has been blocked by the National Telecommunications Corporation," and includes links to further information and a contact email address.¹⁷ In addition to the NTC, the General Prosecutor also has the right to block any site that threatens national security or violates social mores.¹⁸

Political or social content was last blocked in 2012, when Sudanese Online and Facebook were intermittently inaccessible and the "Innocence of Muslims" YouTube video was blocked.

Content Removal

Forced content removal was more prevalent in the past year, though the extent of the practice remains unknown.

In May 2018, Al-Taghyeer, an independent online newspaper, published an article about a song critical of the government called "Barkawi," written by a famous Sudan-based poet and sung by Egypt-based musician Ahmed Abdullah. After the article and the song went viral, the musician received threats from the Sudanese embassy in Cairo and was compelled to immediately remove the song from YouTube to avoid reprisals.

Media, Diversity, and Content Manipulation

Compared to the highly restrictive space in the traditional media sphere—which is characterized by pre-publication censorship, confiscations of entire press runs of newspapers, and warnings from NISS agents against reporting on certain taboo topics¹⁹—the internet remains a relatively open space for freedom of expression, with bold voices expressing discontent with the government on various online platforms. Online news outlets such as Altareeq,²⁰ Altaghyeer,²¹ Radio Dabnga,²² 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, Sudanese citizens increasingly rely on online outlets and social media for uncensored information.²³ Blogging is also popular, allowing journalists and writers to publish commentary free from the restrictions leveled on print newspapers and provides ethnic, gender, and religious minorities a platform to express themselves. The more active Sudanese bloggers write in the English language.

The economic crisis and associated rise in the costs to access the internet has negatively impacted the quality of content available to users, mainly because the high cost of data has disincentivized accessing higher quality content or content in its entirety. Many people share information on WhatsApp, which uses less data, but at the expense of visiting other online news sources for more information.

WhatsApp is also particularly popular among Sudanese for the platform's relative privacy and anonymity features.²⁴ Some government officials have found the app threatening, blaming WhatsApp for the spread of rumors and leaked information, among other issues. During the height of Sudan's fuel shortages in April 2017, for example, the finance minister told the press that he held WhatsApp responsible for spreading false information and panic about fuel prices and thus creating the fuel crisis.²⁵

Government threats against the internet has led to growing self-censorship in recent years. Many journalists writing for online platforms publish anonymously to avoid prosecution, while ordinary internet users in Sudan have become more inclined to self-censor to avoid government surveillance and arbitrary legal consequences.

In response to Sudan's more vibrant online information landscape, the government employs a concerted and systematic strategy to manipulate online conversations through its so-called Cyber Jihadist Unit. Established in 2011 in the wake of the Arab Spring, the unit falls under the National Intelligence and Security Service (NISS) and works to proactively monitor content posted on blogs, social media websites, and online news forums.²⁶ The unit also infiltrates online discussions in an effort to ascertain information about cyber-dissidents and is believed to orchestrate technical attacks against independent websites, especially during political events.²⁷

In the past year, Cyber Jihadists worked to thwart the so-called "bread protests" that took place in early 2018.²⁸ Their strategies included posting pictures from war-torn areas of Syria to demonstrate a higher quality of life in Sudan and commentary that negates citizens' 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 propaganda illustrating how the government was effectively handling the economic situation.

Digital Activism

Social media and communications platforms were critical to the organization of protests in early 2018. Between December 2017 and February 2018, mass protests broke out against the country's economic deterioration, particularly in response to the 2018 state budget, which was seen as more focused on security and the military and heavily based on taxing ordinary citizens who had already seen large increases in taxes in recent years.²⁹ The "bread protests" were heavily organized through Facebook, Twitter and WhatsApp and saw larger numbers of ordinary citizens engage compared to previous protests given the widespread impact of the economic crisis.

While the Cyber Jihadists tried to shutdown popular Facebook pages disseminating information about the protests by reporting the pages en masse, social media was the main source of news about the protest movement. Citizen journalists posted videos of the protests, and reporting on police violence against protestors was only covered online.

Violations of User Rights:

A new cybercrime law and amendments to the media law introduced new restrictions on online activities (they were passed in June 2018, after this report's coverage period). At least one citizen was sentenced to prison, while numerous arrests and interrogations for online activities were reported. Violence against users decreased.

Legal Environment

Sudan has restrictive laws that limit press and internet freedom. Most notably, the Informatic Offences (Combating) Act 2007 (also known as the IT Crime Act, cybercrimes or electronic crimes law)³⁰ criminalizes the establishment of websites that criticize the government or publish defamatory material and content that disturbs public morality or public order.³¹ Violations involve fines and prison sentences between two to five years.

New laws enacted in 2018 (after this report's coverage period) seek to tighten restrictions on online activities. In June 2018, the National Assembly passed the Law on Combatting Cybercrimes of 2018 that introduced criminal penalties for the spread of fake news online.³² The law also penalizes criticizing foreigners with up to two years in prison.

Also in June, amendments to the Media Law (also known as the Press and Publications Act) were approved, which were reportedly aimed at imposing restrictions on online journalism and social media.³³ Notably, the amendments require online journalists to register with the Journalism Council.³⁴ Digital newspapers were not previously required to register, which allowed them to operate without an official physical office due to security concerns.³⁵ The amendments also reportedly include a separate article on offenses in electronic publishing, which carry tough sentences.³⁶

The highly restrictive Media Law was last updated in November 2016 to include specific clauses pertaining to online journalism, extending onerous limitations long placed on the traditional press to the online sphere,³⁷ such as provisions that hold editors-in-chief liable for all content published by their press outlets.³⁸

National security imperatives also restrict journalism, particularly under the 2010 National Security Act, which gives the National Intelligence and Security Service (NISS) immunity from prosecution and the permission to arrest, detain, and censor journalists under the pretext of national security.³⁹

Prosecutions and Detentions for Online Activities

Arrests, prosecutions, and interrogations for online activities continued in the past year, particularly as heavy-handed censorship on the print and broadcast sectors led journalists to migrate online to disseminate news. The arrests reflected an ongoing tactic to limit internet freedom by silencing critical voices and encouraging self-censorship.

At least one citizen was sentenced to prison for online activities during the reporting period. In July 2017, political activist Hatim Merghani was sentenced to two years in prison and a fine for publishing commentary on the

corruption of a government official on WhatsApp and other social media channels.⁴⁰

Numerous journalists faced prosecutions for alleged cybercrime:

- In July 2017, a journalist with the *Al-Jareeda* newspaper was charged for defamation under the cybercrimes law for an article on the corruption of the South Darfur finance minister.⁴¹
- In October 2017, journalist Alaa-Deen Mahmoud discovered he had cybercrimes charges pending against him for being the owner of the online newspaper, the Khartoum Post, which had published an article critical of a government official. He was also accused of being the author of the anonymous article. The only evidence against him was documentation that he had added a friend to the Khartoum Post's Facebook page. He was released on bail, though his case remains open as of mid-2018.⁴²
- In a similar case, journalist Ali Atif Abdelwahab was accused in March 2018 of being the owner of the independent online newspaper Al-Taghyeer and arrested for allegedly publishing false news about the assassination of an ordinary citizen at the hands of the Rapid Support Forces (RSF), a paramilitary force active in Darfur and now in Eastern Sudan on the platform. However, Abdelwahab worked for *Al-Taghyeer*, a print newspaper, which has no relation to the online version. Although he insisted on the misunderstanding, he still faces charges under the cybercrimes law on public order, which carries a maximum sentence of seven years.⁴³

Several activists and everyday citizens were arrested for their social media activities:

- In October 2017, a video circulated of a young man wearing makeup and dancing in a wedding hall. He was reportedly arrested after the party and sentenced to a fine and 40 lashes.
- In February 2018, an online activist was arrested from his house in Suakin, Red Sea (state) for publishing a video on Facebook and WhatsApp that ridiculed the president during his last visit to the state.⁴⁴
- In April 2018, philosophy professor Dr. Esmat Mahmoud was arrested from a class he was teaching and interrogated about a Facebook post he published the previous day criticizing the director of the university.⁴⁵
- Also in April, activist Muhsin Musa from South Kordofan was arrested for posts on his Twitter and Facebook accounts voicing concerns about government corruption and the lack of services in the state. A young woman was arrested alongside Musa after she shared his post and commented on it on her Facebook page.⁴⁶
- Suad Fadul was charged with cybercrimes in April 2018 after she shared a video on WhatsApp in which she detailed how she had recently been removed from her position at the Sudan Communication Company and replaced with the president's niece.⁴⁷

In a dangerous new pattern, the public order police (also known as the morality police) have arrested individuals featured in viral videos for violating laws on personal behavior and dress codes. Sentences vary between 40 lashes for indecent clothing to jail-time and a hefty fine for indecent acts. In February 2018, a video circulated on Facebook and WhatsApp in which a group of young men and women were dancing at a party. Days later, the morality police announced that the people shown in the video were arrested and they would be persecuted. In March, a young woman also filmed dancing in a viral video was arrested by the same police force.

Meanwhile, the authorities continued to pursue online activists based outside Sudan, particularly those who live in Saudi Arabia. In July 2017, Saudi officials handed journalist and online activist Ad-Divina to the NISS. Later in November, Saudi authorities arrested Hisham Ali Mohamed Ali, an online activist residing in Saudi Arabia, and handed him over to the NISS in May 2018. In July 2018, Mohamed's family reported that he had been hospitalized as a result of severe torture.⁴⁸

Surveillance, Privacy, and Anonymity

Unchecked surveillance of ICTs is a grave concern among citizens in Sudan, where the government is known to actively monitor internet communications on social media platforms and target online activists and journalists during politically sensitive periods. The NISS regularly intercepts private email messages, enabled by sophisticated surveillance technologies.

According to Citizen Lab research from June 2013, Sudan possesses high-tech surveillance equipment from the U.S.-based Blue Coat Systems, a technology company that manufactures monitoring and filtering devices. The surveillance system was initially traced to three networks inside Sudan, including the networks of the private telecom provider Canar.⁴⁹ In July 2017, NISS agents reportedly planted Blue Coat surveillance software into the phones and laptops of at least eleven activists during an out-of-country meeting and training. According to a local expert, the software was installed through the WiFi modem shared by the group and enabled the monitoring of all online activities.⁵⁰

Article 9 of the NTC's General Regulations 2012, based on the 2001 Communications Act, obligates mobile companies to keep a complete record of their customers' data, and mandatory SIM card registration was enforced in late 2017. Subscribers were given the deadline of December 31, 2017 to register their phone numbers using their National ID, which includes detailed personal information such as home address, birthplace, and mother's name.

Intimidation and Violence

Online journalists and activists often face extralegal intimidation, harassment, and violence for their online activities, though there were fewer reported incidents of violence during the coverage period compared to previous years.

Most online violence targets social media influencers and minority groups such as LGBTI. In October 2017, a video circulated of a young man wearing makeup and dancing in a wedding hall. He was reportedly arrested after the party and sentenced to a fine and 40 lashes. The young man also received serious threats online and off, which eventually led him to flee the country.⁵¹

Female activists in particular are subject to multilayered attacks such as threats and smear campaigns on social media. In one prominent example from the past few 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 being against the veil and religion. Some of the victims became fearful for their life in the face of violent threats from religious fundamentalists. Two victims reported this page at the cybercrimes prosecution office to no avail; instead, one of the victims was shamed and scolded for posting her picture online. The page was only shut down after serious advocacy with international human rights groups. One group in particular sent a representative to meet with Facebook executives and campaign on this issue. The page was finally removed in April 2017.

Technical Attacks

Independent news sites are frequently subject to technical attacks, which many believe are perpetrated by the government's Cyber Jihadist Unit. Attacks usually intensify during political events and unrest, while some prominent news sites ward off daily DDoS attempts. Several online outlets reported technical attacks against their websites in the past year, but they were able to respond by increasing their cyber security 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 "Inboxat" (Arabic for "Inbox messages") where they share sexual harassment messages they receive on social media with one another.

Notes:

¹ Under the sanctions, Sudanese users could not download applications or software online without a VPN or access services such as Google and even online courses.

² <https://www.albawaba.com/business/sudans-inflation-jumps-543-percent-february-1104238>

³ "Sudan inflation rises to 30.47 pct in December," *Reuters Africa*, January 18, 2017, <http://bit.ly/2ncTg35>; Globally, the average inflation rate is approximately 3 percent, <https://www.statista.com/statistics/256598/global-inflation-rate-compared-to-previous-year/>

⁴ Zain, the country's largest telecom operator, reported a decrease in its third quarter net profits due to Sudan and Iraq. In fact, the company reported that "\$20 million of its net profit losses in the third quarter stemmed from its unit in Sudan." According to a source at Zain, the company is making profit, however, due to tough regulations and the unavailability of hard currency, they are unable to exchange their profits into hard currency. The source also added that in recent times "the company has resorted to using the profits to purchase property, agricultural lands and other investments and market them to Gulf-based investors who then make purchases and make payments to the mother company in hard currency." One of the recent investments recently made by the company is the purchase of a large plot of land on Sudan's most expensive avenue and the construction of a massive modern office complex. <http://gulfnnews.com/business/sectors/kuwait-telecoms-giant-zain-s-profits-fall-over-sudan-iraq-1.2115038>

⁵ According to Numbeo as of September 2018. Average monthly salary is 3,333 SDG, compared to 1,250 SDG for monthly internet. https://www.numbeo.com/cost-of-living/country_result.jsp?country=Sudan

⁶ International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2016," and "Mobile-Cellular Telephone Subscriptions, 2000-2016," <http://bit.ly/1cbxY>

⁷ The State of Sudan Digital- https://sudandigital.com/en_US/2018/03/04/state-sudan-digital-2018/

⁸ <https://www.thenational.ae/world/africa/sudan-hit-by-nationwide-electricity-blackout-during-televised-presidential-speech-1.694404>

⁹ http://www.china.org.cn/world/Off_the_Wire/2018-02/28/content_50619317.htm

¹⁰ Rupa Ranganathan and Cecilia Briceno-Garmendia, *Sudan's Infrastructure: A Continental Perspective*, Africa Infrastructure Country Diagnostic, (Washington, D.C.): World Bank, June 2011), <http://documents.worldbank.org/curated/en/561781468202137788/Sudan-infrastructure-a-continental-perspective>

¹¹ Sudan Central Bank, "The Present Board of Directors," <https://cbos.gov.sd/en/members>

¹² In March 2018, the NTC's website was down.

¹³ National Telecommunications Corporation, "Blocking Or Unblock Websites," last modified September 21, 2016, <http://tpra.gov.sd/regulation-issues/consumers-issues/blocking-websites/>

¹⁴ "Sudan steps up measures to block 'negative' websites," *Sudan Tribune*, March 25, 2014, <http://www.sudantribune.com/spip.php?article50432>

¹⁵ "Sudanese intelligence prosecutes Internet content that 'threatens the morals of the nation,'" *Alhayat*, February 29, 2016, <http://bit.ly/2JlfrT>; "Violations of Internet cafes in Khartoum state," *Ashoroq*, September 24, 2016, <http://bit.ly/2pg7K23>

¹⁶ NTC, "Blocking Or Unblock Websites."

¹⁷ Image of a blocked site: <https://docs.google.com/file/d/0B6mgwvPJ6IadERXT3RTZWIjSkk/edit?pli=1>

¹⁸ "Cybercrime: Cyber terrorism threatens the sovereignty of the state," [in Arabic] *Alintibaha*, August 13, 2014, <http://bit.ly/1NRfEg5>.

¹⁹ "Sudanese Security continues crackdown on press, journalists strike," *Sudan Tribune*, December 01, 2016, <http://bit.ly/2okLkM0>

[20](#) *Altareeq* was established in January 2014.

[21](#) *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.

[22](#) 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. Its website is bilingual and runs in depth reports and features. It is a project of the Radio Darfur Network. Dabnga, "About Us," <http://bit.ly/1LkMr5H>.

[23](#) "Blocking information in Sudan revives websites," *Aljazeera*, January 9, 2017, <http://bit.ly/2nloyos>

[24](#) Khalid Albaih, "How WhatsApp is fueling a 'sharing revolution' in Sudan," *The Guardian*, October 15, 2015, <https://www.theguardian.com/world/2015/oct/15/sudan-whatsapp-sharing-revolution>

[25](#) Finance Minister Holds Whatsapp responsible for the fuel crisis in Sudan (Arabic)- <https://www.sudanakhbar.com/267744>

[26](#) "Sudan to unleash cyber jihadists," *BBC*, March 23, 2011, bbc.in/1V3FWdi.

[27](#) See Freedom on the Net, Sudan 2015, bit.ly/1QOpZp5.

[28](#) 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.

[29](#) 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.

[30](#) The Informatic Offences (Combating) Act, 2007, <https://cbos.gov.sd/en/content/informatic-offences-combating-act-2007>

[31](#) Abdelgadir Mohammed Abdelgadir, *Fences of Silence: Systematic Repression of Freedom of the Press, Opinion and Expression in Sudan*, (International Press Institute, 2012) <http://bit.ly/1Pv7nee>. 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.

[32](#) <https://smex.org/do-new-sudanese-laws-regulate-digital-space-or-limit-freedom-of-expression/>

[33](#) <https://smex.org/do-new-sudanese-laws-regulate-digital-space-or-limit-freedom-of-expression/>

[34](#) Sudanese Cabinet Press Release, October 26, 2017. <https://goo.gl/anHZQX>; "Amendments to the Press Law to restrict social media and increase newspapers' suspension days," *Altaghyeer*, (Arabic), November 11, 2017. <https://goo.gl/ZUmTwi>; "Sudan: A new law includes digital press to the Press Council's jurisdiction," *Altareeq* (Arabic), Nov 6, 2017. <https://goo.gl/NnCxgZ>; Sudanese journalists protest against draft press law, <http://www.sudantribune.com/spip.php?article64012>

[35](#) As in the case of Hurriyat, Al-Rakoba, Al-Taghyeer, Al-Tareeg.

[36](#) The Council of Ministers Passes a law with harsher penalties on electronic publishing- <https://www.altaghyeer.info/2018/03/23/مجلس-الوزراء-يجيز-قانون-يشدد-العقوبات>

[37](#) "Ministry of Justice receives amendments to the Sudanese Press Law of 2016." [in Arabic] *Altareeq*, November 8, 2016, <http://bit.ly/2nvP1Tr>; "The Sudanese Press Freedom Forum: online journalism to be included in the Press Law," [in Arabic] *Al-Sahafa*, August 30, 2016, <http://bit.ly/2nSJYwB>

[38](#) Committee to Protect Journalists, "Repressive press law passed in Sudan," June 11, 2009, <https://cpj.org/x/2c67>.

[39](#) Amnesty International, "Sudanese security service carries out brutal campaign against opponents," July 19, 2010, <https://www.amnesty.org/en/press-releases/2010/07/17643/>

[40](#) Leader in the Sudanese Congress Party jailed due to a whatsapp message (Arabic)- <https://www.altaghyeer.info/2017/07/22/سجن-قاضي-المؤتمر-السوداني-بسبب-رسالة-واتس>

[41](#) Four Sudanese citizens charged with defamation and cybercrimes for social media activity- <http://www.acjps.org/four-sudanese-citizens-charged-with-defamation-and-cybercrimes-for-social-media-activity/>

[42](#) Interview with Alaa-aldeen Mahmoud on 8th of March 2018

[43](#) Interview with Al-Taghyeer editor on Tuesday 6th of March 2018 over whatsapp.

[44](#) Interview with Al-Taghyeer journalist, February 2018.

[45](#) <http://www.acjps.org/four-sudanese-citizens-charged-with-defamation-and-cybercrimes-for-social-media-activity/>

[46](#) <http://www.acjps.org/four-sudanese-citizens-charged-with-defamation-and-cybercrimes-for-social-media-activity/>

[47](#) Four Sudanese citizens charged with defamation and cybercrimes for social media activity- <http://www.acjps.org/four-sudanese-citizens-charged-with-defamation-and-cybercrimes-for-social-media-activity/>

[48](#) Sudanese activist deported from Saudi Arabia detained in Khartoum- <https://www.dabangasudan.org/en/all-news/article/sudanese-activist-deported-from-saudi-arabia-detained-in-khartoum>

[49](#) Ellen Nakashima, "Report: Web monitoring devices made by US firm Blue Coat detected in Iran, Sudan," *Washington Post*, July 8, 2013, <http://wapo.st/1Pv95fA>.

[50](#) Based FH consultant interviews, March 2018.

[51](#) He was a Sudanese-Canadian