Freedom House

# Sudan

| | 2013 | 2014 |
|---|---|---|
| **Internet Freedom Status** | **Not Free** | **Not Free** |
| Obstacles to Access (0-25) | 17 | 18 |
| Limits on Content (0-35) | 19 | 19 |
| Violations of User Rights (0-40) | 27 | 28 |
| **TOTAL* (0-100)** | **63** | **65** |

* 0=most free, 100=least free

| | |
|---|---|
| Population: | 34.2 million |
| Internet Penetration 2013: | 23 percent |
| Social Media/ICT Apps Blocked: | No |
| Political/Social Content Blocked: | Yes |
| Bloggers/ICT Users Arrested: | Yes |
| Press Freedom 2014 Status: | Not Free |

## Key Developments: May 2013 – May 2014

- A localized internet service disruption in June and a nationwide blackout in September corresponded with large antigovernment protests; the blackouts were reportedly directed by the government (see **Obstacles to Access**).
- U.S. sanctions on Sudan had a negative impact on the ability of Sudan's civil society to leverage online technologies, inhibiting important civil society efforts (see **Limits on Content**).
- Monitoring and filtering devices from Blue Coat Systems were traced to three networks inside Sudan in June (see **Violations of User Rights**).
- Government surveillance of online activists and journalists was particularly pronounced during the June and September 2013 protests (see **Violations of User Rights**).
- A number of individuals were arrested for their ICT activities, while journalists and civil society groups were subject to an increasing degree of technical violence (see **Violations of User Rights**).

## Introduction

During the coverage period, journalists, civil society, and citizens at large in Sudan faced an ongoing government crackdown on free expression, triggered by mass protests that took place in June 2013 and smaller demonstrations that ensued through September 2013. The protests were sparked by the removal of government fuel subsidies, which escalated the cost of transportation and food items in a country already suffering from a severe economic crisis.

The period between the widespread "Sudan Revolts" protests in the summer of 2012 and the protests that took place throughout 2013 saw a tightening of press freedom, sporadic arrests of activists, and the shutdown of major civil society organizations. Government repression intensified toward the end of 2013, with the authorities using live bullets and an extensive arrest campaign to break up the September protests, in addition to shutting down all internet services for nearly 24 hours for the first time in Sudan. Access to Facebook and YouTube platforms was slow for days after the shutdown. A shorter internet blackout was reported on one service provider leading up to the June protests.

Meanwhile, the Sudanese government under President Omar al-Bashir increased its restrictions on internet freedom through various tactics during the coverage period. For example, the national regulator reportedly sought ways to control social media applications such as Facebook and WhatsApp, while government trolls within the National Intelligence and Security Service's Cyber Jihadist Unit increasingly manipulated the online information landscape. Government surveillance of online activists and journalists was particularly pronounced during the September 2013 protests, and sophisticated surveillance technology from U.S.-based Blue Coat Systems was traced to three devices inside Sudan, including on the networks of the Emirati-owned telecom provider, Canar.

A number of individuals were arrested for their online activities during the year, including the journalist Khalid Ahmed from *Al-Sudani* newspaper, who was arrested in June 2013 by the electronic crimes police for an article he was accused of publishing on an independent news website that criticized the army. Meanwhile, journalists and civil society groups were subject to an increasing degree of harassment, extralegal violence, and hacking attacks. In one incident, government authorities shut down the popular TEDxKhartoum event in May 2013. Numerous online news outlets and individual Facebook pages suffered hacking attacks throughout the year.

## Obstacles to Access

Access to information and communications technologies (ICTs) in Sudan continued to spread in the past year, with internet penetration growing from 21 percent in 2012 to 23 percent in 2013, according to the International Telecommunication Union (ITU).[1] The number of users, however, could be somewhat higher as internet-enabled mobile phones have become widespread and cheaper in

1 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2013," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

recent years. In 2013, 25 percent of the population had access to mobile-broadband services,[2] while mobile phone penetration stood at 73 percent, up from 60 percent in 2012.[3]

Sudan's telecommunications infrastructure and market are among the most developed and liberalized in the region,[4] which has enabled affordable services. As of mid-2014, a monthly mobile internet subscription cost between SDG 2 to 9 (US$0.35 to $1.50) for 100 MB to 1 GB.[5] In general, all companies offer daily internet for rates that do not exceed SDG 1 for basic access, and as a result of market competition, there are ongoing offers that make it possible to enjoy free or lower cost internet services during certain hours.

Aside from mobile internet, users also access the internet from personal desktops or laptop computers through routers or USB modems that cost between SDG 134 and 250 (US$24 to $44), and monthly fixed-line broadband subscriptions that cost from SDG 26 to 200 (US$5 to $35), depending on the package. Secondhand laptops and computers are widely available, and users can make payments toward a computer in monthly installments. Nevertheless, the number of fixed broadband subscriptions in the country is still very low, with a penetration rate of 0.17 percent in 2013 (up from 0.05 percent in 2012), according to the ITU.[6] Meanwhile, cybercafes, which are concentrated in market areas and popular around universities and dorms, charge between SDG 2 to 5 (US$0.35 to $0.87) per hour, though the number of cybercafes in Khartoum state has decreased noticeably since the early 2000s as mobile internet has become cheaper and more accessible to the public. In addition, the country's relatively low prices for mobile and internet access are still out of reach for the majority of the population in Sudan, where the median annual per-capita income was US$579 in 2013, according to Gallup research.[7]

Meanwhile, comprehensive economic sanctions imposed by the U.S. government against the al-Bashir regime since 1997 have been a significant hindrance to users' access to various ICTs and new media tools.[8] While the sanctions were amended in 2010 to authorize the export of certain ICTs and boost the free-flow of information,[9] and again in 2013 to allow educational institutions to exchange academic research,[10] the sanctions continued to block access to original software made by American companies, effectively limiting free access to knowledge on the internet. For example, important software such as anti-virus suites, e-document readers, and rich-content multimedia applications

2 International Telecommunication Union, "Sudan Profile (latest data available: 2013)," *ICT-Eye*, accessed August 1, 2014, http://www.itu.int/net4/itu-d/icteye/CountryProfileReport.aspx?countryID=8.

3 International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2013."

4 Rupa Ranganathan and Cecilia Briceno-Garmendia, "Sudan's Infrastructure: A Continental Perspective," *Africa Infrastructure Country Diagnostic, Country Report*, World Bank, June 2011, http://www.ppiaf.org/sites/ppiaf.org/files/publication/AICD-Sudan-country-report.pdf.

5 On the Sudani network. Zain network offers more expensive, but still affordable packages with a 1 SDG internet package per day and a weekly subscription costing 5 SDG while MTN offers daily internet packages costing from 0.60 to 1 SDG.

6 International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions, 2000-2013."

7 Glenn Phelps and Steve Crabtree, "Worldwide, Median Household Income About $10,000," Gallup World, December 16, 2013, http://www.gallup.com/poll/166211/worldwide-median-household-income-000.aspx#1.

8 "What you Need to Know About U.S. Sanctions—Sudan," U.S. Department of the Treasury, June 25, 2008, http://www.treasury.gov/resource-center/sanctions/Programs/Documents/sudan.pdf.

9 "Treasury Department Issues New General License to Boost Internet-Based Communication, Free Flow of Information in Iran, Sudan and Cuba," U.S. Department of the Treasury, press release, March 8, 2010, http://www.treasury.gov/press-center/press-releases/Pages/tg577.aspx.

10 "US to ease sanctions on Sudan to allow educational exchange," *Sudan Tribune*, February 4, 2013, http://www.sudantribune.com/spip.php?article45407.

are blocked and inaccessible for users to download. Additionally, software security updates are unavailable, forcing users to rely on outdated versions that make their computers and devices vulnerable to malware and other technical attacks. Smartphones and tablets are also affected, as online stores where users can download and update applications are completely inaccessible in Sudan. Savvy users have been able to turn to circumvention tools such as proxies and virtual private networks (VPNs) to access these blocked services, but ordinary users likely miss out on these key ICT applications. The problem of sanctions-induced inaccessibility poses a serious security threat to activists and human rights defenders, making them unable to use these technologies in their work and potentially exposing them to state surveillance and censorship.

The U.S. sanctions regime has also stunted Sudan's educational potential, as free online educational websites such as Khan Academy, Google Scholar, and Audacity are blocked to users in the country. In January 2014, the free online education company Coursera announced that it had to restrict access to its courses to students from Cuba, Iran, and Sudan, citing U.S. sanctions that prohibit the export of services from for-profit companies to sanctioned countries.[11] Similarly, individuals enrolled in massive open online courses ("MOOCs") at American educational institutions, such as MITx, reported not receiving certificates of completion after passing online exams.[12] The EdX platform announced in February 2014, however, that it had found a solution to the sanctions regulations, enabling them to open its services to all students around the world.[13] Coursera also announced in September 2014 that it was granted an Office of Foreign Assets Control (OFAC) license to provide services in Sudan and Cuba.[14] Nevertheless, the ongoing restrictions were widely criticized as a violation of the universal right to education and likened to censorship.[15]

There are four licensed telecommunications operators in Sudan: Zain, MTN, Sudatel, and Canar. MTN and Sudatel both offer broadband internet, while Zain offers fast internet through its USB modem and mobile internet services. Canar offers fixed phone lines and home internet. All four providers are privately-owned by foreign companies, with the exception of Sudatel which has 22 percent of its shares owned by the government; the remaining shares are held by foreign entities.[16] Only Sudatel and Canar have a direct connection to the international gateway and lease access to the global internet to MTN and Zain.

Fairly strong market competition in Sudan's telecoms sector has enabled the growth of fast internet in the country. Under normal circumstances, the internet operates at advertised speeds of up to 21 Mbps on the Zain network in Khartoum and at 7.2 Mbps in other areas. According to May 2014

11 Coursera, "Update on Course Accessibility for Students in Cuba, Iran, Sudan, and Syria," (blog), January 28, 2014, http://blog.coursera.org/post/74891215298/update-on-course-accessibility-for-students-in-cuba.

12 Amanda Sperber, "In Sudan Civil Society Say It's Struggling to Work Around US Sanctions Block on Tech," *TechPresident*, January 14, 2014, http://techpresident.com/news/wegov/24667/sudan-civil-society-struggles-tech-us-sanctions.

13 Anant Agarwal, "We're not blocking anyone: EdX still educating students from Iran, Syria, Sudan, and Cuba," edX (blog), February 2, 2014, https://www.edx.org/blog/were-not-blocking-anyone-edx-still.

14 Jillian York, "Coursera Takes a Positive Step Forward in Cuba and Sudan," Electronic Frontier Foundation, September 8, 2014, https://www.eff.org/deeplinks/2014/09/coursera-takes-positive-step-forward-cuba-and-sudan.

15 *Al Jazeera*, "US sanctions lead Coursera to block online courses in select countries: Netizens question the impact of the US blocking online education in Iran, Cuba and Sudan," The Stream (blog), January 30, 2014, http://stream.aljazeera.com/story/201401292259-0023429; Milana Knezevic, "Why US sanctions are a blow to free expression," Index on Censorship (blog), January 31, 2014, http://www.indexoncensorship.org/2014/01/coursera/.

16 Rupa Ranganathan and Cecilia Briceno-Garmendia, "Sudan's Infrastructure: A Continental Perspective," *Africa Infrastructure Country Diagnostic, Country Report*, World Bank, June 2011, http://www.ppiaf.org/sites/ppiaf.org/files/publication/AICD-Sudan-country-report.pdf.

data from Akamai's "State of the Internet" report, Sudan's average connection speed is recorded at 3.2 Mbps (compared to a global average of 3.9 Mbps).[17] In addition, Sudan's broadband adoption (characterized by connection speeds greater than 4 Mbps) was over 20 percent, while the country's narrowband adoption (connection speeds below 256 kbps) was under 1 percent.[18]

Despite Sudan's open and liberalized ICT sector, the government has demonstrated an ability to restrict connectivity and access during particular events, such as the partial internet blackout on the Sudatel network on June 29, 2013 that lasted for nearly eight hours ahead of a planned antigovernment rally.[19] A complete internet blackout occurred three months later on September 25, 2013, when the internet intelligence company Renesys confirmed two separate internet blackouts that were reportedly directed by the government.[20] Beginning at 12:47 UTC on September 25, after three days of intense nationwide protests, Renesys reported that "all Sudanese routed networks were withdrawn from the global routing table," which was "not caused by a single catastrophic technical failure" and "strongly suggests a coordinated action to remove Sudan from the Internet."[21] Subscribers of the four service providers (Zain, MTN, Canar, and Sudani) were cut off for nearly 24 hours. Renesys also described the incident as "the largest government-directed Internet blackout since Egypt in January 2011."[22]

Denying responsibility for the blackouts, the government claimed that a major network problem had caused the internet outage, while the National Telecommunications Corporation (NTC), the national regulator, blamed a fire in the office of the Emirati-owned Canar telecom, which rents access to the global internet network to the other providers.[23] Though unconfirmed, analysts strongly believe the incident was most likely orchestrated by the NTC, the state agency that regulates the ICT sector in Sudan.

Founded in 1996 and housed under the Ministry of Telecommunications, 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."

17 Akamai, "Average Connection Speed: Sudan," map visualization, *The State of the Internet Q1* (2014), http://www.akamai.com/stateoftheinternet/soti-visualizations.html#stoi-map.

18 Akamai, "Broadband Adoption (connections to Akamai >4 Mbps): Sudan," map visualization, *The State of the Internet,* Q1 2014; Akamai, "Narrowband Adoption (connections to Akamai <256 kbps): Sudan," map visualization, *The State of the Internet,* Q1 2014, http://www.akamai.com/stateoftheinternet/soti-visualizations.html#stoi-map.

19 Renesys Corporation Twitter Feed (@renesys), 4:33PM, June 29, 2013, https://twitter.com/renesys/status/351060825722736640/photo/1.

20 Doug Madory, "Internet Blackout in Sudan," Renesys (blog), September 25, 2013, http://www.renesys.com/2013/09/internet-blackout-sudan/.

21 Doug Madory, "Internet Blackout in Sudan,"" Renesys (blog), September 25, 2013.

22 Doug Madory, "Internet Blackout in Sudan,"" Renesys (blog), September 25, 2013.

23 Peter Micek and Ben-Avie Jochai, "Update: Mass internet shutdown in Sudan follows days of protest," Access Now (blog), October 15, 2013, https://www.accessnow.org/blog/mass-internet-shutdown-in-sudan-follows-days-of-protest.

## Limits on Content

No new social, political, or religious websites were blocked during the coverage period, though access to Facebook and YouTube was reportedly very slow or virtually inaccessible to many users during and after the September 2013 wave of protests. Government efforts to manipulate the online information landscape became more concerted and systematic. U.S. sanctions on Sudan had a negative impact on the ability of Sudan's civil society to leverage online technologies, inhibiting important civil society efforts.

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.[24] The NTC's website also gives users the opportunity to submit requests to either block or unblock websites "that are deemed not containing pornography,"[25] though 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 NTC and includes a contact email address at filtering@ntc.gov.sd.[26]

Social media platforms are not blocked in Sudan, though access to Facebook and YouTube was reportedly very slow or virtually inaccessible to many users during and after the September 2013 wave of protests. At times, users were able to access the website through the secure "https" protocol instead of "http." Meanwhile, since 2008, YouTube and the popular Sudanese forum and news website *Sudanese Online* have been sporadically blocked for various periods for content perceived as too sensitive by the regime, such as articles on the war in Darfur.[27] The blocks typically range from a few days to a few weeks, and when a website becomes accessible again, it can take some time for content to be fully restored. YouTube was last blocked from September to November 2012 in response to the "Innocence of Muslims" video.

The most recent long-term blocking of websites coincided with the June to July 2012 "Sudan Revolts" protest movement, during which the NTC blocked the online newspapers *Sudanese Online*, *Al-Rakoba*, and *Hurriyat*,[28] the latter two of which are known to be antigovernment.[29] All three outlets were eventually unblocked but at times are still difficult to access.

In response to the growth of online publications that are critical of the ruling party, the Sudanese government has stated intentions to enact legal measures to restrict content regarded as "a threat to national and social security." According to the ruling party media secretary Yassar Youssef Ibrahim in a July 2013 interview, such "threats" encompass not only religiously immoral content, but also

24 "Blocking Or Unblock Websites," National Telecommunications Corporation, last modified October 22, 2014, http://www.ntc.gov.sd/index.php/en/blocking-websites.

25 "Blocking Or Unblock Websites."

26 Image of a blocked site: https://docs.google.com/file/d/0B6mgwvplJ6IadERXT3RTZW1jSkk/edit.

27 OpenNet Initiative, "Internet Filtering in Sudan."

28 Eva Galperin, "Sudan Revolts, Government Cracks Down on Dissent," Electronic Frontier Foundation, July 10, 2012, https://www.eff.org/deeplinks/2012/07/sudan-revolts-government-cracks-down-dissent.

29 *Hurriyat* is based in Kampala, Uganda and its editorial staff is comprised of prominent journalists who left Sudan after enduring numerous court trials for their writings. *Al-Rakoba*, on the other hand, has a number of anonymous journalists inside Sudan but is managed by a group based in the Gulf region.

opposition publications and political criticism.[30] To combat the perceived threats, the secretary advocated for a law to govern electronic media "that grants authorities the right to block websites when they violate agreed upon limitations."[31]

In May 2014, the national regulator, the NTC, reportedly began a technical study on social networking applications such as Facebook and WhatsApp in an effort to find ways to control their use in the country, citing concerns that the applications encourage indecent activities that go against Sudan's customs and traditions.[32] Other reports have alleged that the Ministry of Culture and Information in Khartoum state is looking to use sophisticated technical tools to block social media platforms, though the ministry denied any intent to block websites.[33]

As a result of growing online censorship, some opposition news outlets have moved their servers abroad to avoid blocking. For example, *Sudanese Online* currently operates from the United States, while *Sudan Tribune* is based out of France and *Al Taghyeer* ("Change") is based in the United Kingdom.[34] This trend may continue if a draft media law with implications for digital news is passed (see "Violations of User Rights").

Despite increasing instances of internet censorship in recent years, online newspapers in Sudan continue to have more freedom than traditional media outlets, which are frequently subject to pre-publication censorship, confiscations of entire press runs of newspapers, and warnings from National Intelligence and Security Service (NISS) agents against reporting on certain taboo topics.[35] Restrictions on traditional news outlets increased following the National Security Act of 2010, which gave the NISS permission to arrest journalists and censor newspapers under the pretext of national security.[36] As such, many print newspapers have begun to circulate censored or banned material on their websites and social media pages, and online news outlets are gaining traction. Most recently, independent journalists successfully launched the electronic newspaper *Al-Tareeg* ("the road") in January 2014,[37] and the newspaper *Sudan Voices* launched its online version in May.[38]

Compared to the highly restrictive space for press freedom in the traditional media sphere, the internet remains a relatively open space for freedom of expression, with bold voices expressing discontent with the government on various online platforms. Nonetheless, self-censorship is prevalent and may be increasing as the government extends its media crackdown to the internet. During the September 2013 protests, some opposition journalists began publishing anonymously to

30 Adam Mohamed Ahmad, "'We need a law that governs the electronic media,'" *The Niles*, July 10, 2013, http://www.theniles.org/articles/?id=1938.

31 Adam Mohamed Ahmad, "Too many red lines: Pressure on Sudan media freedom increases," *The Niles*, July 7, 2013, http://www.theniles.org/articles/?id=1288.

32 "Sudan looking into ways to control Facebook and Whatsapp," *Sudan Tribune,* May 28, 2014, http://www.sudantribune.com/spip.php?article51144.

33 "Sudan looking into ways to control Facebook and Whatsapp," *Sudan Tribune,* May 28, 2014.

34 Reem Abbas, "Sudan's Shift from Print to Online Newspapers," Doha Centre for Media Freedom, May 16, 2013, http://www.dc4mf.org/en/node/3740.

35 Interview with an editor-in-chief in Khartoum, Sudan, August 2012.

36 The NISS carries out arbitrary arrests, may detain an individual for up to 45 days without charges and can renew the detention period after the end of the 45-day period. NISS officers have total immunity from the law. "Sudanese Security Service Carries out Brutal Campaign Against Opponents," Amnesty International, July 19, 2010, http://www.amnesty.org/en/news-and-updates/report/sudanese-security-service-carries-out-brutal-campaign-against-opponents-2010.

37 *Al-Tareeg*: http://www.altareeq.info/ar/.

38 *Sudan Voices*: http://sudanvoices.com/.

avoid being identified for writing about taboo topics, such as human rights violations linked to the country's conflict regions, state corruption, the economic recession, and criticism of national security agents.

Government efforts to manipulate the online information landscape have become more concerted and systematic. In response to the Arab Spring events and the proliferation of antigovernment protest movements organized on social media sites in 2011, the Sudanese government began deploying a force known as the Cyber Jihadist Unit tasked to conduct "online defense operations" and "crush online dissent."[39] A leaked 2011 document revealed that the Unit employs over 200 individuals divided across different locations who work three shifts to ensure around the clock coverage, particularly during timeframes when internet traffic is highest, such as late at night and during the weekend.[40] More recent research from 2013 found that the number of recruits has increased, with the NISS recruiting heavily at government universities, especially at the police-owned Al-Ribat University.[41] The Unit seems to have adequate funding for training, and stipends are given to the young recruits who are mostly students or unemployed youth. According to private interviews, the Cyber Jihadists have also received training courses in hacking and online monitoring from India and Malaysia, among other countries.

Based at the NISS, the Cyber Jihadist Unit proactively monitors content posted on blogs, social media websites, and online newspaper forums. The Unit also infiltrates online discussions in an effort to ascertain information about cyber-dissidents and spread misinformation. This strategy has been employed most prominently on the news forum, *Sudanese Online*, which is known for its popularity among antigovernment intellectuals, journalists, politicians, and activists. When the government took notice of the website's influence in the mid-2000s, it planted contributors to spread false information, instigate problems between users, and discredit posts written by members of the forum.[42] The Unit also frequently hacks websites and personal email and social media accounts of activists (see "Violations of User Rights").[43]

On May 10, 2014, NISS allegedly launched a rumor that it had arrested the administrators of an opposition group's Facebook page, publishing the story in a print progovernment newspaper (*Al Saiha)* with the headline, "National Security Arrests the Creators of al Bashir's Diaries." Created over two years ago, the popular Facebook page is known for its use of humor and satire to criticize the government. Within a day, the administrators announced on their Facebook page that the news

39 Email interview with editors from *Hurriyat* and *Al-Rakoba*, January 2013; "Sudan to Unleash Cyber Jihadists," *BBC News*, March 23, 2011, http://www.bbc.co.uk/news/technology-12829808.

40 "With the NCP's Documents: Operation Electronic Defense to Bring Down the Sudanese Revolution" [in Arabic], *Sudan Motion,* April 14, 2012, http://sudanmotion.com/index.php/news/3-sudan-news/4143-2012-04-14-10-30-28.

41 Interview with telecommunications expert in Khartoum, Sudan, January 15, 2013.

42 Interview with a press freedom advocate and journalist in Khartoum, Sudan, January 16, 2012.

43 In August 2012, a thread on *Sudanese Online* titled, "Accounts Targeted and Monitored by the Cyber-Jihad Unit," started by an exiled activist revealed a list of 274 names, Facebook pages and groups and described the expanded technical capacities of the unit. Leaked to the exiled activist by "a trusted source," the list made evident that the unit's primary targets were online activists, particularly young people, whose social media accounts publish timely information about the protests and news about human rights violations. For example, the first name mentioned in the list was Amani Al-Agab, a well-known online activist who is very active on Sudanese forums as well as Facebook. There is little information available on Amani Al-Agab; however, it is known that she is outside Sudan. http://www.change.org/users/7806131; See also, Bukhari Osman, "Accounts Targeted by Cyber Jihad Unit" [in Arabic], August 23, 2012, *Sudanese Online*, http://www.sudaneseonline.com/cgi-bin/sdb/2bb.cgi?seq=print&board=400&msg=1345716699&rn=1.

article was a rumor, though the false story indicates how the authorities may be trying to crack down on social media by instilling a fear of reprisal among users.

Meanwhile, blogging is an increasingly important platform for journalists and writers who use it to publish commentary free from the restrictions leveled on print newspapers. Blogs also give ethnic, gender, and religious minorities a venue to express themselves. As of mid-2014, there are about 300 Sudanese blogs registered in the newly established Sudanese Bloggers Network.[44] The more active Sudanese bloggers write in the English language.

The internet has also become a powerful tool for activists to fight for social, political, and economic change, enabling protests such as the ones in June and September 2013 to organize across the country.[45] During the damaging floods that befell Khartoum state in July and August 2013, youth activists turned to Facebook to launch the grassroots campaign known as Nafeer to help flood victims.[46] Working with a local NGO, the Nafeer Facebook campaign attracted over 5,000 volunteers within two weeks, in addition to collecting generous cash donations from Sudanese based both locally and abroad,[47] which allowed emergency relief to be delivered to victims more quickly than aid from the government.

Nevertheless, U.S. sanctions have had a negative impact on the ability of Sudan's civil society to leverage online technologies such as crowd-funding or online payment platforms, which has inhibited important civil society efforts. For example, when Nafeer turned to the internet to seek both volunteers and donations during the August 2013 floods, its Paypal account was shut down for receiving donations from the diaspora in the United States.[48] Similarly, many organizations have been unable to receive financial support from Sudanese diaspora communities that can strengthen their independence from foreign aid as well as their sustainability.

Crisis mappers have also noted that the sanctions are limiting their ability to access the tools they need. According to Abeer Awad Khairy, a crisis mapper who created an online map for the August 2013 floods used by Nafeer and the United Nations to identify regions in need of relief, all Google products are sanctioned in Sudan, including Google Crisis Map and People Finder. Crisis mapping tools produced by other American companies such as Esri, which makes GIS technology for mapping, are also blocked, making it difficult for a proper network of crisis mappers to operate within the country.[49]

Sanctions have further inhibited diaspora communities seeking to send assistance home via crowd-funding tools. In December 2013, for example, a group of Sudanese diaspora activists living

44 Interview with the Sudanese Bloggers Network, January 23, 2013, http://sdunlimitedbloggers.blogspot.com/.

45 Ismai'il Kushkush, "Protesters and the Police Clash in Sudan," *The New York Times*, July 6, 2012, https://www.nytimes.com/2012/07/07/world/africa/in-sudan-protesters-clash-with-the-riot-police.html?_r=0.

46 Isma'il Kushkush, "As Floods Ravage Sudan, Young Volunteers Revive a Tradition of Aid," *The New York Times,* August, 29, 2013, http://www.nytimes.com/2013/08/30/world/africa/as-floods-ravage-sudan-young-volunteers-revive-a-tradition-of-aid.html?pagewanted=all.

47 Author's Research.

48 Tweet by @Amjedfarid (in Arabic): "The Americans closed #Nafeer's paypal account because of sanctions. What are we supposed to deal with, the government's harassment or the Americans?" August 21, 2013, https://twitter.com/amjedfarid/status/370239060427550720.

49 YouTube video: "US technology sanctions on Sudan," posted by LiftUS sanctions, January 18, 2014, http://www.youtube.com/watch?v=lMaHzjTzQro.

in the United States, Europe, and the Middle East launched a crowd-funding campaign via the online platform Indiegogo to help renovate a school in the peripheries of Khartoum that gives free education to 330 internally displaced students from the Nuba Mountains and Darfur.[50] Within five days of launching the campaign, the group received a message from Indiegogo saying that the campaign had been "frozen" because it may have been in violation of U.S. sanctions policies. In response, the fundraising team attached the most recent OFAC update on Sudan sanctions from November 2013, which provides an exemption for conflict areas and communities impacted by conflict, as well as on the peripheries around Khartoum.[51] Fortunately, Indiegogo accepted the explanation and put the campaign back online after freezing it for 24 hours.

## Violations of User Rights

Monitoring and filtering devices from Blue Coat Systems were traced to three networks inside Sudan in June 2013. Government surveillance of online activists and journalists was particularly pronounced during the June and September 2013 protests. A number of individuals were arrested for their ICT activities during the coverage period, while journalists and civil society groups were subject to an increasing degree of technical violence.

Freedom of speech, expression, and association are nominally protected under the 2005 Interim National Constitution (INC) that was adopted as part of the 2005 Comprehensive Peace Agreement (CPA) between the government of Sudan and the southern rebel group, though the constitution officially expired following the independence of South Sudan in July 2011. A permanent constitution is still being drafted as of mid-2014, leaving the INC as the country's highest binding document.

Sudan has a host of restrictive laws that seeks to limit internet freedom. For example, the Informatic Offences (Combating) Act (known as the IT Crime Act, or electronic crimes law),[52] criminalizes the establishment of websites that criticize the government or publish defamatory material and content that disturbs public morality or public order.[53] Violations involve fines and prison sentences between two to five years. While only one case of defamation has been filed under the IT Crime Act since its enactment in 2007,[54] the act inherently contradicts Sudan's constitutional protection of freedom of expression and fundamentally undermines internet freedom in the country.

For bloggers and online activists, the press laws and the criminal law are more dangerous. In 2009, the government revised the highly restrictive 2004 Press and Printed Press Materials Law, which continued to allow for restrictions on the press in the interests of national security and public order,

50 "Support Nuba Mountain IDP Students," Indiegogo campaign, December 13, 2013, http://www.indiegogo.com/projects/support-nuba-mountain-idp-students/x/5649009.

51 E.O. 13412 exempts Southern Kordofan/Nuba Mountains State, Blue Nile State, Abyei, Darfur, and marginalized areas in and around Khartoum – referred to as "the Specified Areas of Sudan" – from certain of the prohibitions imposed by E.O. 13067. See, Department of the Treasury, "Sudan Sanctions Program," Office of Foreign Assets Control (OFAC), November 5, 2013, p. 3, http://www.treasury.gov/resource-center/sanctions/Programs/Documents/sudan.pdf.

52 "The Informatic Offences (Combating) Act, 2007," National Telecommunications Corporation, http://www.ntc.gov.sd/images/stories/docs/English/Informatics_offences_Act_2007.pdf.

53 Abdelgadir Mohammed Abdelgadir, "Fences of Silence: Systematic Repression of Freedom of the Press, Opinion and Expression in Sudan," International Press Institute, 2012, http://www.freemedia.at/fileadmin/media/Fences_of_Silence-AbdelgadirMAbdelgadir-3.pdf.

54 Details of case unknown. Interview with a press freedom advocate in Khartoum, Sudan, January 16, 2012.

and holds editors-in-chief liable for all content published in their newspapers.[55] While there is no specific reference to online media, the press law's broad wording allows for its application to online content.

In December 2012, a new draft press law was presented to the national assembly that aims to further restrict media freedom in Sudan. While the draft law has yet to be publicly released as of mid-2014, a member of the Sudanese National Council asserted in an interview with the Doha Centre for Media Freedom in April 2013 that the new law would include regulations on online media.[56] Meanwhile, the authorities also restrict media freedom through the 2010 National Security Act, which gives the NISS immunity from prosecution and the permission to arrest, detain, and censor newspapers under the pretext of national security.[57] Furthermore, Sudan's judiciary is not independent, though it has recently ruled against the government in support of press freedom, reversing a government order to shut down the *Al-Tayar* independent daily in March 2014.[58]

Bloggers and citizen journalists in Sudan are increasingly detained and harassed for their work, particularly during times of protest. In June 2013, national security agents arrested the journalist Khalid Ahmed from *Al-Sudani* newspaper for allegedly publishing an article in an independent news website that criticized the army in Abu-Karshola town in Southern Kordofan, where the government has been at war with the Sudan People's Liberation Movement (SPLM) rebels since June 2011. Despite his claim that he had not written the article, Ahmed was taken to the intellectual property rights court where he was charged with "harming the morale of the Sudanese armed forces," "sharing military information," and "tarnishing the reputation of the army's chief of staff" under the penal code and IT Crime Act.[59] The court cleared Ahmed of all charges in March 2014 due to lack of evidence,[60] but journalists worry that the incident will set a precedent for the authorities to continue prosecuting online journalists.

In July 2013, three youths were arrested in Northern Kordofan for posting and commenting on a link to an online article on Facebook about corruption charges of the Zakat ("philanthropy") Unit in the government of Northern Kordofan.[61] They were arrested for a day, released after interrogations,[62] then rearrested again shortly after and charged with defamation.[63] Details of their conviction are unknown as of mid-2014.

55 Committee to Protect Journalists, "Repressive press law passed in Sudan," press release, June 11, 2009, http://www.cpj.org/2009/06/repressive-press-law-passed-in-sudan.php.

56 Reem Abbas, "Proposed Sudan Media Law Targets Press Freedom," *Al-Monitor*, January 17, 2013, http://www.al-monitor.com/pulse/originals/2013/01/sudan-press-freedom.html#ixzz2OY2WyeL3; Ahmed Vall, "'New Law Will Grant Greater Media Freedom in Sudan,'" Doha Centre for Media Freedom, April 7, 2013, http://www.dc4mf.org/en/content/new-law-will-grant-greater-media-freedom-sudan.

57 "Sudanese Security Service Carries Out Brutal Campaign Against Opponents," Amnesty International, July 19, 2010, http://www.amnesty.org/en/news-and-updates/report/sudanese-security-service-carries-out-brutal-campaign-against-opponents-2010.

58 "Sudan's top court reverses newspaper closure amid continued crackdown on press," *Sudan Tribune,* March 5, 2014, http://allafrica.com/stories/201403060770.html.

59 Based on author interview. June/July 2013.

60 Mekki Elmograbi, "Good Day: Faisal and Khalid Cases, and the Fair Sudanese Courts!" *Sudan Vision Daily*, March 5, 2014, http://news.sudanvisiondaily.com/article.html?rsnpaid=1386.

61 Based on FOTN Sudan analyst's research on the ground.

62 "Sudan security questions group of youths over Facebook posts," *Sudan Tribune*, July 9, 2013, http://www.sudantribune.com/spip.php?article47241.

63 Author's Research.

During the September 2013 protests, the pro-democracy group Sudan Change Now (SCN) came under heavy attack by the NISS, with more than ten of its members arrested and kept in detention for weeks, including Dahlia Al-Roubi, a social media activist and SCN member, who was arrested and held for a week; she was released without charges. At least four journalists were detained during the protests, including two women. In another case, Samar Mirghani, a pharmacist and Khartoum University graduate, was arrested while filming the police shoot a young male protester with her phone during the September protests.[64] She was later tortured in detention and had her phone confiscated for the alleged possession of "indecent" materials. Her trial received a significant amount of national attention, and on October 28, 2013, she was found innocent of the charges lodged against her under article 153 of the penal code (obtaining and having indecent content on her mobile phone) and article 69 (disturbing the public peace), though she received a fine of SDG 5,000 (US$1,120) for participating in the protests[65]

The government actively monitors internet communications, and the NISS regularly intercepts private email messages.[66] The Sudan Police Department also monitors internet cafes to make sure users do not access websites deemed immoral by the authorities.[67] Government surveillance of online activists and journalists was particularly pronounced during the June and September 2013 protests. Meanwhile, mobile phones have become an especially dangerous tool for activists given the widespread suspicion that the authorities possess phone-tapping and location tracking tools.[68]

In November 2013, the Al-Arabiya TV channel hosted a show interviewing Mubarak Mohamed, a former officer who worked for the NISS, during which he stated that 80 percent of NISS's intelligence gathering is collected through phone tapping, although he was not specific on what the phone surveillance entails.[69] In one notable incident during the September 2013 protests, three members of Sudan Change Now were arrested shortly after they turned on their mobile phones while in public, raising concerns that activists were being tracked.[70]

Mobile phone tapping and tracking was made more feasible in 2008 when a law was enacted requiring subscribers to register their SIM cards with providers. Nevertheless, it was still relatively easy to purchase a SIM card without providing personal information for activation until the June 2012 protests when the policy became more strictly enforced, particularly by the partially government-owned telecom, Sudani.[71] Activists believe the effort to be a strategic move by the authorities to track user phone numbers and personal information.

After the September 2013 protests, the campaign to register SIM cards became more aggressive, involving television, newspaper, and billboard advertisements; public mobile registration services; and lotteries to win prizes such as money, gold, or cars. The provider MTN even advertised that users could register their friends' SIM cards for them. Registration requires a copy of a national ID

64 Author's Research.

65 "A Sudanese Woman Testifies about Her Torture at Hands of Security Agents" (in Arabic), *AlArabiya*, October 3, 2013, http://bit.ly/1uUzgmd.

66 U.S. Department of State, "Sudan 2013 Human Rights Report," http://www.state.gov/documents/organization/220376.pdf.

67 OpenNet Initiative, "Internet Filtering in Sudan."

68 Interview in Khartoum, Sudan, August 1, 2012.

69 Author's Research

70 Author's Interview with SCN representative, Khartoum, January 2014

71 Based on author's research.

and home address details. In April 2013, a representative from the NISS told the press that there were 700 police cases a day against unregistered numbers or numbers registered under false names.[72]

Government requests for user data on international communications platforms such as Facebook have been on the rise in recent years. Between July 2013 and June 2014, a total of five requests were made by the government for information on five separate user accounts on Facebook, compared to zero requests the previous year; none of these requests were granted.[73]

According to recent research, Sudan has acquired high-tech surveillance equipment. In June 2013, Citizen Lab traced the U.S.-based Blue Coat Systems—which manufactures devices that can be used to monitor network traffic and filter content—to three networks inside Sudan, including on the networks of the private telecom provider, Canar.[74] These revelations made evident that the U.S. sanctions regime against Sudan have not impeded the Sudanese government from gaining access to or purchasing U.S.-made surveillance software, as intended. Rather, the sanctions more often impinge upon regular users' access to ICTs, albeit unintentionally, as discussed above. Meanwhile, Blue Coat Systems claimed that the devices reached embargoed countries without their knowledge.[75]

Facebook is widely monitored and used to track and incriminate activists for arrest.[76] During recent protests, for example, the social media platform was the first website detainees were asked to open while in detention, and private messages as well as the pages that activists "like" were checked to see if they were affiliated with a certain political party or social movement. Consequently, many young people have stopped posting personal pictures on their profiles and changed their Facebook names to pseudonyms to avoid being identified. Testimonies of detained activists have also revealed that the authorities possess pretty sophisticated technical abilities, with one detained SCN member recounting how his Macbook had been confiscated and broken into, despite his refusal to provide his password details.[77]

Sudanese dissidents living abroad have also been targeted by the NISS, indicating a level of surveillance that may be able to cross international borders or entail cooperation with other governments. The prominent Sudanese blogger, Amir Ahmed Nasr, was one such expatriate who was confronted by an apparent Sudanese security agent while living in Kuala Lumpur, Malaysia. Also known for his autobiography about his blogging experience on difficult questions about Islam, identity, and Middle Eastern politics—which is banned in Malaysia—Nsar was told by the security agent that he was "being watched back in Khartoum by the NISS, and that [he] should

72 Abdul-Gasim Sawsan, "NISS: 700 false complaints daily and fake sim-cards carrying names of Omar Al-Bashir and Leila Alwi" [in Arabic], *Al-Rakoba,* April 2, 2013, http://www.alrakoba.net/news-action-show-id-92958.htm.

73 "Sudan," Facebook government requests report, accessed November 5, 2014, https://govtrequests.facebook.com/country/Sudan/2014-H1/.

74 Ellen Nakashima, "Report: Web monitoring devices made by US firm Blue Coat detected in Iran, Sudan," *The Washington Post*, July 8, 2013, http://www.washingtonpost.com/world/national-security/report-web-monitoring-devices-made-by-us-firm-blue-coat-detected-in-iran-sudan/2013/07/08/09877ad6-e7cf-11e2-a301-ea5a8116d211_story.html.

75 Ellen Nakashima, "Report: Web monitoring devices made by US firm Blue Coat detected in Iran, Sudan," *The Washington Post*, July 8, 2013.

76 Bukhari Osman, "Accounts Targeted by Cyber Jihad Unit" [in Arabic], August 23, 2012, *Sudanese Online*, http://www.sudaneseonline.com/cgi-bin/sdb/2bb.cgi?seq=print&board=400&msg=1345716699&rn=1.

77 Author's Interview with SCN representative, Khartoum, January 2014.

stop [his] articles and speeches against the NCP, or else there will be consequences."[78] The blogger subsequently left Malaysia to seek political asylum in Canada.

Extralegal intimidation is also a tactic regularly employed by security agents within Sudan, as visibly demonstrated when the government shut down a popular TEDxKhartoum event in May 2013.[79] Despite months of preparation that included support from a number of government institutions, security agents obstructed the event minutes after it began, threatening to revoke the organizers' permit and later cut off the facility's electricity. Because the event had no political agenda, the main organizer of TedxSudan, Anwar Dafa-Alla, believed that the government was nervous about the event being live-streamed. Dafa-Alla later participated in the September 2013 protests and subsequently left Sudan to seek political asylum in the United States, after being told by a government insider that his name was on a "shoot-to-kill" list.

Journalists and civil society groups have been subject to an increasing degree of technical violence. Online news outlets such as *Al-Rakoba*, *Sudanese-Online*, and *Hurriyat* frequently experience hacking attacks by what activists believe is the work of the Cyber Jihadist Unit.[80] The webmaster account of the *Sudan Tribune* website was most recently hacked in April 2014, which resulted in the disabling of all staff passwords and the posting of a fake news article on the site about the assassination of the South Sudanese leader, Riek Machar.[81] Later in April, the opposition website "3ayin"[82] was hacked by a group calling itself Haras al Hudoud (or "soldiers of the frontier"), whose name appeared on the screen when users tried to access the hacked site while it was down. Haras al Hudoud refers to a group of the government's armed forces in Darfur, though there is no direct evidence that the government was behind the hacking attack. In October 2013, GIRIFNA (a non-violent youth-based resistance movement) suffered a hacking attempt on its website. According to the group's IT team, the attempt was a phishing attack that tried to trick users into giving up their passwords by directing them to a fake mirror website.[83]

Individual Facebook pages are also frequently targeted for attacks. In October 2013, for example, Khalid Ewais, a Sudanese journalist working for the UAE-based *Al-Arabiya* channel, reported on his Facebook page that his account had experienced a failed hacking attempt.[84] An inside source who formerly worked at the Cyber Jihadist Unit revealed that the Unit's practice of Facebook hacking typically begins with the creation of a fake account using a "girl's name and picture to discredit information on pages or to add activists to gain access to their pages."[85] Sometimes the fake profile

78 Author's interview with Amir A. Nasr. Via email. January 16, 2014.

79 "Sudanese Security Shuts Down TEDx Event in Khartoum," *Sudan Tribune*, May 11, 2013, http://www.sudantribune.com/spip.php?article46532.

80 Interview with Newspaper Owners/ Editors, January 2013- January 2014.

81 "Sudan Tribune website hacked; Machar not target of assassination attempt," *Sudan Tribune*, April 2, 2014, http://www.sudantribune.com/spip.php?article50505.

82 http://www.3ayin.com/ is the Arabic off-shoot of "Nuba Reports" that specializes in collecting video footage and reports from a team of citizen journalists in the Nuba Mountains to disclose information linked to the civil war there and especially its impact on civilians.

83 Reem Abbas, "The Online War in Sudan," Doha Center for Media Freedom, October 30, 2013.

84 Reem Abbas, "The Online War in Sudan," Doha Center for Media Freedom, October 30, 2013, http://www.dc4mf.org/en/content/online-war-sudan.

85 Anonymous interview.

has the same name and picture as one of a user's friends and usually does not have many of its own friends.[86]

In response to increasing technical attacks against activists in recent years, a hacktivist group known as AnonSudan emerged in September 2013 when it hacked several government websites, including the government's main site,[87] the presidency's site, and a number of ministerial sites. The group proudly announced on Twitter that it had taken down 149 websites affiliated with the government.[88]

86 Reem Abbas, "The Online War in Sudan," Doha Center for Media Freedom, October 30, 2013.

87 Government of Sudan website: http://sudan.gov.sd

88 Reem Abbas, "The Online War in Sudan," Doha Center for Media Freedom, October 30, 2013.