Freedom House

Sudan

	2014	2015
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	18	18
Limits on Content (0-35)	19	19
Violations of User Rights (0-40)	28	28
TOTAL* (0-100)	**65**	**65**

* 0=most free, 100=least free

Population:	**38.8 million**
Internet Penetration 2014:	**25 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2015 Status:	**Not Free**

Key Developments: June 2014 – May 2015

- Access to the internet became more challenging for Sudanese citizens as internet prices surged while speeds declined dramatically (see **Availability and Ease of Access**).
- Extremely slow internet speeds were experienced in parts of the country during several politically contentious periods, leading to strong suspicions of government throttling (see **Restrictions on Connectivity**).
- A new Freedom of Access to Information Law passed in January 2015 classifies 12 types of information that are restricted from citizens. Observers believe the government passed the new law to legalize the withholding of information and its censorship powers (see **Legal Environment**).
- In the lead up to the April 2015 general elections, several online journalists and activists were arrested while numerous online news outlets were hacked (see **Prosecutions and Detentions** and **Technical Attacks**).

Introduction

Internet freedom in Sudan remained under threat in 2014 and 2015, as authoritarian President Omar al-Bashir's government intensified its crackdown on critical voices in the lead-up to general elections held in April 2015. In an attempt to expand control over the political space, the government enacted numerous laws designed to increase its powers while minimizing opportunities for opposition. In January 2015, for example, the Sudanese parliament approved constitutional amendments that gave the president powers to appoint and remove senior officials,[1] and established a new body of security forces under the control of the National Intelligence and Security Service (NISS), which was previously limited to intelligence gathering.[2]

A new Freedom of Access to Information Law passed in January 2015 with the purported aim of increasing transparency has instead led to greater limitations, with provisions that detail 12 types of information that are restricted from citizens, such as national security and foreign policy information. The limits effectively leave no room for journalists or the public to access any information of consequence. Observers believe the government passed the new law to legalize the withholding of information and its censorship powers.

Meanwhile, government authorities made other concerted efforts to restrict critical information and silence the opposition, including proactively manipulating the online information landscape and arresting several journalists and activists for their online activities. Several hacking attacks against critical news websites and activists' social media webpages were reported, escalating around the April 2015 general elections. While no critical news or opposition websites were blocked during the coverage period, Sudanese officials regularly demanded the blocking of online news outlets, particularly after the outlets criticized government officials or published articles about corruption.

Obstacles to Access

Access to the internet became more challenging for Sudanese citizens in 2014-2015 as a result of increasing costs and declining quality of services. Extremely slow internet speeds were experienced during several political contentious periods, leading to strong suspicions of government throttling.

Availability and Ease of Access

Access to information and communications technologies (ICTs) in Sudan slightly increased over the past year, with internet penetration reaching 25 percent in 2014, compared to 23 percent in 2013, according to the International Telecommunication Union (ITU).[3] The number of users may be higher as internet-enabled mobile phones have become widespread and cheaper in recent years.

Despite the spread of ICT services, access to the internet became more challenging for Sudanese citizens in 2014-2015 as the cost of access surged amid declining quality and speeds.[4] Telecom com-

1 "Sudan: Constitutional amendments give Bashir new powers," *Asharq Alawsat*, January 5, 2015, http://www.aawsat.net/2015/01/article55340104/sudan-constitutional-amendments-give-bashir-new-powers.

2 "Sudanese constitution to be amended to grant more powers to security services: official," *Sudan Tribune,* April 30, 2015, http://bit.ly/1GBIqVh.

3 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2000-2014, http://bit.ly/1cblxxY.

4 "Deterioration of telecommunication services in Sudan and companies complain of piracy,"[in Arabic] *Sudan Tribune*, April

panies introduced new bundles at higher rates that did not deliver speeds as advertised, while old bundles experienced worsening speeds. According to Akamai's 2014 "State of the Internet" fourth quarter report,[5] Sudan's average connection speed declined by 73 percent during the September-December 2014 quarter alone,[6] decreasing from 3.6 Mbps to 1.0 Mbps (significantly lower than the global average speed of 4.5 Mbps). Increasing tensions and violent clashes between government forces and rebel factions in Sudan's conflict regions have also led to frequent service disruptions.

As of mid-2015, monthly mobile internet subscriptions cost between SDG 2.62 to 68 (US$0.62 to $11), up from SDG 2 to 9 in 2014—an increase of 31 percent for 100MB of data and around 600 percent for 1GB packages. As a result, mobile phone penetration in Sudan decreased slightly from 73 percent in 2013 to 72 percent in 2014.[7] USB internet modems for personal desktops or laptops cost between SDG 124 and 261 (US$22 to $46) per month, and monthly fixed-line broadband subscriptions range from SDG 26 to 200 (US$5 to $35), depending on the package.

Internet access at cybercafes, which are concentrated in market areas and popular around universities and dorms, has also become more expensive, with minimum charges ranging between SDG 3-15 (US $0.50-2.51) per hour, up from SDG 2-5 (US $0.35-0.87) in 2014—a 50 and 200 percent increase, respectively—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. As a result of increasing prices, mobile phone and internet access is still out of reach for the majority of the population in Sudan.

Furthermore, approximately 1.2 million citizens living in rebel-controlled areas in South Kordofan have extremely limited access to the internet.[8] Nearly two million internally displaced persons (IDPs) living in camps have no access whatsoever.

In a positive step, previous obstacles to access imposed by U.S. economic sanctions in place against the al-Bashir regime since 1997 were mitigated in February 2015, when the U.S. Treasury Department announced it was easing the long-standing sanctions.[9] The sanctions banned the import of ICT hardware and original software made by American companies, such as anti-virus, anti-malware, anti-tracking, and anti-censorship software and more secure ICT applications. The ban had been particularly punitive on Sudanese activists and ordinary citizens, whose use of outdated technologies and software made them vulnerable to malware and other technical attacks. Under the February amendments to the sanctions, these vital technologies can now be imported into the country.[10]

Restrictions on Connectivity

Sudan connects to the global internet through three international gateways—the partly state-owned

2014, http://bit.ly/1KkHeXp.

5 Akamai, "Average Connection Speed," map visualization, *State of the Internet, Q4 2014,* accessed May 29, 2015, http://akamai.me/1LiS6KD.

6 Akamai, *State of the Internet, Q4 2014 Report,* 2015, http://bit.ly/1Lgq4AI.

7 International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions," 2000-2014, http://bit.ly/1cblxxY.

8 See "Mayors in Sudan's South Kordofan demand no-fly zone," Radio Dabanga, February 24, 2014, http://bit.ly/1RkJ8gf, and UNHCR, "Sudan," 2015, http://www.unhcr.org/pages/49e483b76.html.

9 "US Eases Sudan Sanctions to Allow Communications Gear," *Voice of America News*, February 17, 2015, http://bit.ly/1RSINSX.

10 U.S. Department of Treasury, "Publication of Sudan General License- Related to Personal communications," February 17, 2015, http://1.usa.gov/1GeXnmr.

Sudan Telecom Company (Sudatel), Zain, and Canar Telecom[11]—which are connected via four submarine cables: Saudi Arabia-Sudan-2 (SAS-2), Saudi Arabia-Sudan-1 (SAS-1), Eastern Africa Submarine System (EASSy), and FALCON.[12] Partial control over the international gateway has enabled the government to restrict internet connectivity during particular events in the past, such as during the September 2013 nationwide protests when the government shut down service of all telecom providers for nearly 24 hours.[13]

In August 2014, a five-day internet blackout was reported in the West Darfur region of Sudan, negatively impacting hundreds of students who were unable to apply for university, though the cause of the disruption remains unclear.[14] In many other parts of the country, extremely slow internet speeds were experienced during several political contentious periods in 2014-2015, leading to strong suspicions of government throttling. For example, in the lead-up to the one-year anniversary of the September 2013 protests, broadband connection speeds in Khartoum declined significantly from an average speed of 3.2 Mbps to 2.22 Mbps in September 2014,[15] which observers believed was an intentional effort by the Sudanese government to impede anniversary protests.[16] In October 2014, during a largescale campaign initiated online to raise awareness about the mass rape of 200 women in the Darfuri town of Tabit (see "Media, Diversity, and Content Manipulation"), internet connections were reportedly as low as 1.48 Mbps. During the April 2015 elections, speeds were also slower than average at 2.34 Mbps.[17]

ICT Market

There is fairly strong market competition in Sudan's telecoms sector among four licensed telecommunications operators: Zain, MTN, Sudatel, and Canar. 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 a foreign entity.[18] The Sudanese government manipulates the telecommunications sector indirectly through Sudatel's board of directors, which includes the current Minister of Finance and National Economy as the board's chairman[19] and the current Governor of the Central Bank of Sudan as a board member.[20]

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. Major internet providers provide 3G services.[21] In December 2014, the Minister of Communications and Information

11 Doug Madory, "Internet Blackout in Sudan," Dyn Research, September 25, 2013, http://bit.ly/1QN46V3.

12 Check interactive ,Huawei Marine Networks, "Submarine Cable Map for Sudan," http://bit.ly/1ZRMhKz.

13 See Freedom House, "Sudan," *Freedom on the Net 2014,* http://bit.ly/1M2wVig.

14 "Online registration to Sadness Universities and Institutes," *3ayin*, August 20, 2014, http://bit.ly/1M1optw.

15 Net Index "The Global Standard in Internet Metrics," Sudan's map visualization, http://bit.ly/1GPBfK4.

16 Author's interview.

17 Net Index "The Global Standard in Internet Metrics."

18 Rupa Ranganathan and Cecilia Briceno-Garmendia, *Sudan's Infrastructure: A Continental Perspective*, Africa Infrastructure Country Diagnostic, (Washington, D.C.): World Bank, June 2011) http://bit.ly/1OOZoXz.

19 "Dirar named Chairman of Sudatel's Board of Directors, Tarig as a CEO,"[in Arabic] *Alintibaha,* May 18, 2014, http://bit.ly/1jQCymW.

20 Sudan Central Bank, "The Present Board of Directors," http://bit.ly/1jxA7pG.

21 3G short form of third generation, is the third generation of mobile telecommunications technology. International Telecommunication union, "IMT-2000 Project," http://www.itu.int/osg/imt-project/.

Technology stated that 4G would be introduced in Sudan mid-2015,[22] though as of June 2015, 4G had not been installed.[23]

Increasing prices on telecom services in 2014-2015 were partially due to tax incentives given to telecom providers alongside higher value added taxes (VAT) imposed on consumers. In 2013, the government of Sudan exempted the telecommunications sector from a 30 percent tax on all profits until the end of 2015.[24] Despite the exemption, the government's revenue from the telecommunications sector grew in 2014-2015 due to VAT revenues totaling US $600 million per year from consumers,[25] while revenue taxes on telecoms did not exceed US $40 million per year.[26]

Regulatory Bodies

Founded in 1996 and housed under the Ministry of Telecommunications and Information Technology, the National Telecommunications Corporation (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."

Limits on Content

Online self-censorship increased notably in 2014-2015 in response to the government's heavy-handed crackdown against both print and online media in advance of the April 2015 elections. Government efforts to manipulate the online information landscape also became more concerted and systematic.

Blocking and Filtering

News websites and social media platforms were not blocked in Sudan during the coverage period, though access to Facebook and the online news outlet *Al Rakoba* was reportedly very slow or at times virtually inaccessible to many users.[27] Meanwhile, Sudanese officials regularly demanded the blocking of online news outlets, particularly after the outlets criticized government officials or published articles about corruption.[28]

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

22 "Future plans to reduce telecommunication' tariff,"[in Arabic] *Alkhartoum*, December 23, 2014, http://bit.ly/1MzSAbR.

23 See World Time Zone: http://www.worldtimezone.com/4g.html

24 Matt Smith, "Sudan shelves telecom profit tax for three years," *Reuters*, June 16, 2013, http://reut.rs/1MQ13w3.

25 "An interview with Alfatih Erwah," [in Arabic] *Alssayha*, March 11, 2015, http://bit.ly/1OERWzU.

26 "National Council stresses the need to revise the law on privatization," [in Arabic] *Almighar*, December 22, 2014, http://bit.ly/1ZRNMIz.

27 Author's interviews.

28 "Tabita Boutros calls for closing some online news outlets, specifically Sudan Motion," [in Arabic] *Sudan Motion*, March 14, 2014, http://bit.ly/1W2w8ma.

percent of blocked material is related to pornography.[29] The NTC's website also gives users the opportunity to submit requests to either block or unblock websites "that are deemed to not contain pornography,"[30] 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 National Telecommunications Corporation," and includes links to further information and a contact email address.[31]

In addition to the NTC, NISS agents reportedly have the technical capability to block websites deemed harmful and threatening to Sudan's national security,[32] while the General Prosecutor also has the right to block any site that threatens national security or violates social mores.[33]

During a June 2014 workshop on online media, the Sudanese Information Minister described Facebook and independent online news outlets *Al Rakoba*, *Hurriyat*, and *Sudanese Online* as "anomalous" and "mercenary" and stated his intention to censor the sites for tarnishing Sudan's image and blocking potential foreign investment opportunities.[34] The minister reiterated the same official position against online media in a televised interview,[35] affirming that the government blocks content that it perceives as immoral or a threat to national security.

Content Removal

The extent to which the government forces websites to delete certain content is unknown, though anecdotal incidents in 2014-2015 suggested that some degree of forced content removal by the state exists, and that such ad hoc requirements lack transparency. For example, in March 2014, the government forced three news outlets to delete articles from their websites that had cited a government press release, which quoted an official from the ruling National Congress Party (NCP) using an offensive slur to characterize the opposition.[36] Criticism of the quote went viral on social media, prompting the NCP—beleaguered by strong pushback from the opposition in the lead up to the April 2015 presidential elections—to delete the original press release from its own website, in addition to forcing other outlets to both delete the stories and post a retraction.[37] Furthermore, the NCP dismissed its Khartoum-chapter webmaster from his job for publishing the statement that had caused the social media uproar.[38]

Media, Diversity, and Content Manipulation

Despite increasing instances of internet censorship in recent years, online newspapers in Sudan con-

29 National Telecommunications Corporation, "Blocking Or Unblock Websites," last modified October 22, 2014, http://bit.ly/1GnidzI.

30 "Blocking Or Unblock Websites."

31 Image of a blocked site: http://bit.ly/1GeYxyn.

32 "Expert: NISS is capable of blocking websites that are posing a threat to Sudan's national security," *Aljareeda*, November 7, 2014.

33 "Cybercrime is an act of terrorism that threatens the sovereignty of the state," [in Arabic] *Alintibaha*, August 13, 2014, http://bit.ly/1NRfFg5.

34 "Ahmed Bilal: These websites are anomalous" and "mercenary," [in Arabic] *Alrakoba*, June 30, 2014, http://bit.ly/1RSLYKi.

35 See YouTube video in Arabic, *Sudan national TV*, 29:50 to 34:00, June 20, 2013, http://bit.ly/1RSM7gJ.

36 "NCP: those who call for abstention are riff raff,"[in Arabic] *Alyoum Altali*, March 7, 2015 , http://bit.ly/1LGV2Ro.

37 "Clarification form NCP about the statement attributed to Yasser Youssef,"*Alyoum Altali,* March 8, 2015, http://bit.ly/1jxBdBR.

38 "Webmaster expelled from his position," *Al-Tayar*, March 8, 2015.

tinue 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 NISS agents against reporting on certain taboo topics, which include human rights violations linked to the country's conflict regions, state corruption, the economic recession, and criticism of national security agents.[39] Restrictions on print and broadcast 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.

Compared to the highly restrictive space 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. Many print newspapers circulate censored or banned material on their websites and social media pages, leading Sudanese citizens to increasingly turn to online outlets and social media for uncensored information. Continuous pressure on traditional media has led a number of independent journalists to establish online news outlets in the past few years, though several outlets were subject to frequent technical attacks by government forces throughout 2014-2015 as part of an apparent attempt to limit access to independent news and voices in the lead-up to the April 2015 elections (see "Technical Attacks").

Blogging is an important platform for journalists and writers 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-2015, there were about 300 Sudanese blogs registered with the Sudanese Bloggers Network. The more active Sudanese bloggers write in the English language.

Nonetheless, online self-censorship increased notably in 2014-2015 in response to the government's heavy-handed crackdown against both print and online media in advance of the April 2015 elections.[40] The majority of journalists writing for online newspapers, such as the newly established *Altareeq* and *Altaghyeer*, write anonymously.[41]

Government efforts to manipulate the online information landscape have become more concerted and systematic. During the coverage period, the government's Cyber Jihadist Unit continued to spread misinformation on news related to human rights violations and corruption allegations. The unit, which falls under the NISS, proactively monitors content posted on blogs, social media websites, and online newspaper forums and infiltrates online discussions in an effort to ascertain information about cyber-dissidents.

A largescale cyber jihadist campaign was launched in November 2014 in response to global online and offline activism surrounding the mass rape of over 200 women and girls in Tabit town in North Darfur by Sudanese soldiers,[42] which was first reported by Radio Dabanga.[43] Led by Khalid Ewais, a

39 "Chairman of the Sudanese National Press Council: security services intervene when "redlines are crossed" and threaten national security,"[in Arabic] *Asharq Alawsat*, February, 15, 2015, http://bit.ly/19IMgmC; "President: We will not allow the press to go beyond the red lines,"*Ashorooq*, February 25, 2015, http://bit.ly/1XfYExM.

40 Author's interview.

41 *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 in 2012. For more, see Reem Abbas, "Sudan's Shift from Print to Online Newspapers," Doha Centre for Media Freedom, May 16, 2013, http://bit.ly/1GniAKB. *Altareeg* was established in January 2014, and its "Who we are" section does not include names of staff but rather the institution's reporting code of conduct.

42 "Mass rape of "200" in North Darfur," *Radio Dabanga*, November 2 , 2014, http://bit.ly/1W2wEk9; Human Rights Watch, "Sudan: Mass Rape by Army in Darfur," February 11, 2015, http://bit.ly/1E9pI7e.

43 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

Sudanese journalist based in the United Arab Emirates, the social media campaign to raise awareness about the mass rape led to several demonstrations around the world and in Sudan.[44] Various counter-campaigns from the Cyber Jihadist Unit were subsequently launched on both government and ostensibly apolitical social media pages that aimed to delegitimize the rape atrocity by smearing Radio Dabanga and Khalid Ewais.[45] For example, cyber jihadists circulated a message on WhatsApp claiming that Ewais had received a US $1 million bribe from the African Union/United Nations Hybrid operation in Darfur (UNAMID),[46] which Ewais denied in an interview with a Khartoum-based newspaper.[47]

In its attempt to distort the facts, cyber jihadists then posted a video on YouTube in which Tabit residents were interviewed denying the Radio Dabanga report.[48] Simultaneously, the government's "Official Page of the Rapid Response Operations Room" Facebook page published photos showing a women's rally in Tabit denying the report and claiming that Radio Dabanga had dishonored them.[49] All the while, members of the Sudanese parliament openly demanded the blocking of Radio Dabanga in Sudan.[50] The government eventually yielded to international pressure garnered by the campaign and allowed officials from the United Nations Mission in Darfur (UNAMID) to conduct an investigation,[51] albeit under the government's supervision.[52] Unfortunately, the government subsequently blocked the investigation[53] and later closed down the UN Human Rights office in Khartoum.[54]

Digital Activism

Despite numerous obstacles and restrictions on ICTs in Sudan, the country's growing population of technologically savvy citizens regularly engages in digital activism to demand government accountability and social change. Digital activism was particularly vibrant in the lead-up to the April 2015 general elections, as exemplified by the "Leave!" campaign launched in February 2015 in response to President Omar Al-Bashir's statement that he would not leave the presidency unless he was voted out, which citizens rejected given the Al-Bashir's record of rigging elections in the past.[55] The campaign encouraged a wholesale boycott of the election as a form of protest against Al-Bashir's au-

project of the Radio Darfur Network. Dabnga, "About Us," http://bit.ly/1LkMr5H.

44 "Sudan: Worldwide Protests and Social Media for Darfur Mass Rape Grow," *All Africa*, November 23, 2014, http://bit.ly/1Pv2SjN; Mark Kerrison, "Sudanese protest against mass rapes in Darfur outside Downing Street," *DEMOTIX*, November 14, 2014, http://bit.ly/1LGWLGr.

45 Collection of the cartons included in this PDF http://bit.ly/1M2BF7p; See Facebook post [in Arabic], November 20, 2014, http://on.fb.me/1Gf02N8; Khalid Ibrahim Ewais, Facebook Post, November 23, 2014, http://on.fb.me/1QN8y6i.

46 Khalid Ibrahim Ewais, Facebook Post, November 23, 2014, http://on.fb.me/1QN8y6i.

47 "khalid Ewais denies receiving money for the United Nations," [in Arabic] *Almijhar*, November 25, 2014.

48 "Facts about Tabet," [in Arabic] YouTube video, 9:54, posted by Sudan's Hoopoe, November 23, 2014, http://bit.ly/1RSOmk3.

49 Photos form Official Page of the Rapid Response Operations Room: Facebook Photo, November 20, 2014, http://on.fb.me/1jxCusL; Facebook Photo, November 22, 2014, http://on.fb.me/1Xg0RJr; Facebook Photo, November 22, 2014, http://on.fb.me/1M1uHcE; Facebook Photo, November 22, 2014, http://on.fb.me/1RSOH6q.

50 "Confrontation with Radio Dabanga, and the search for means to hush it,"[in Arabic] *Alsaiha,* November 29, 2014, http://bit.ly/1RkOKqI.

51 Jenn Psaki, "Government of Sudan Delays Access to Investigate Reports of Mass Rape in North Darfur," press statement, U.S. Department of State, November 12, 2014, http://1.usa.gov/1EEFdp5.

52 "Sudan: Army Filmed UNAMID Mass Rape Investigations in Tabit," *All Africa*, November 12, 2014, http://bit.ly/1KkNnTx.

53 "Sudan again blocks UNAMID investigation into Darfur mass rape claims," *Sudan Tribune*, November 16, 2014, http://bit.ly/1RkOSqn.

54 AFP, "Sudan asks UN to shut human rights office in Khartoum over abuse claims," *The Guardian,* November 27, 2014, http://bit.ly/1LkOIO9.

55 "Sudanese president: I will not leave unless people decide that through the ballot box," [in Arabic] *Al-Youm Al-Sabie***,** February 26, 2015.

thoritarianism.[56] Though several organizers of the "Leave!" campaign were arrested around the country[57] and Al-Bashir was ultimately re-elected in April, voter turnout stood at between 30-35 percent compared to 72 percent in the previous elections in 2010, reflecting the boycott's relative success.[58]

Violations of User Rights

A new Freedom of Access to Information Law passed in January 2015 classifies 12 types of information that are restricted from citizens, which observers believe was part of an effort to legalize the government's censorship powers. In the lead-up to the April 2015 general elections, the government took preemptive measures to restrict critical information and silence the opposition by arresting numerous online journalists and activists. Hacking attacks against critical news websites and activists' social media accounts also escalated around the general elections.

Legal Environment

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. In January 2015, the parliament approved new amendments to the constitution regarding the elections;[59] however, a permanent constitution is still being developed as of mid-2015, leaving the INC as the country's highest binding document. Sudan's judiciary is not independent, though it 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.[60]

Sudan has several restrictive laws that seek to limit press and internet freedom. For example, the Informatic Offences (Combating) Act (known as the IT Crime Act, or electronic crimes law),[61] criminalizes the establishment of websites that criticize the government or publish defamatory material and content that disturbs public morality or public order.[62] Violations involve fines and prison sentences between two to five years. The 2009 revisions to the highly restrictive 2004 Press and Printed Press Materials Law allows for restrictions on the press in the interests of national security and public order

56 Fatima Naib, "Boycott call dampens Sudan's election spirit," *Al Jazeera*, April 10, 2015, http://www.aljazeera.com/news/2015/04/sudan-gripped-election-fever-opposition-boycott-150410154035525.html.

57 "Preemptive arrests before the second public event for the Sudanese opposition for "Leave!" campaign," [in Arabic] *Sudan Tribune*, February 5, 2015, http://bit.ly/1M2Ejdt.

58 "Sudan elections: Polls close after low turnout," *BBC*, April 17, 2015 http://bbc.in/1HAm4aT; International Institute for Democracy and Electoral Assistance, "Voter turnout data for Sudan," http://bit.ly/1Gf2eUI.

59 AFP,"Sudan amends constitution to let Bashir name governors," *Daily Mail*, January 4, 2015, http://dailym.ai/1M1w8b2.

60 "Sudan's top court reverses newspaper closure amid continued crackdown on press," *All Africa,* March 5, 2014, http://bit.ly/1NkNtz4.

61 The Informatic Offences (Combating) Act, 2007, http://bit.ly/1NkNx1R.

62 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 deformation 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.

and holds editors-in-chief liable for all content published in their newspapers.[63] The 2010 National Security Act gives the NISS immunity from prosecution and the permission to arrest, detain, and censor newspapers under the pretext of national security.[64] Though there are no specific references to online media, the press and national security laws' broad wording allows them to be applied to online content.

In January 2015, the government passed a new Freedom of Access to Information Law[65] with the supposed aim of improving Sudan's last place ranking on Transparency International's Corruption Perception's Index.[66] While the government claimed that the law would increase transparency and the public's access to information,[67] the law itself has not been made publicly available as of mid-2015. According to local reports and observers, the law is in practice highly limiting, with provisions that reportedly classify 12 types of information that are restricted from citizens, such as national security and foreign policy information, among others.[68] The classification system effectively leaves no room for journalists or the public to access any information of consequence. Moreover, freedom of information requests will be overseen by a minister appointed by the president, giving the executive branch exclusive control over access to information, while arbitrarily determined fees imposed for each inquiry will make the process of requesting information burdensome. Furthermore, according to local sources, individuals will be perversely subject to penalties under other laws if they request certain types of classified information, such as information that the government could decide is a threat to national security.[69] Many observers believe the government passed the new law to legalize the withholding of information and its censorship powers.[70] Others contend the law provides the legal grounds to argue for more access to information.[71]

Meanwhile, a new draft press law introduced in December 2012 is still in the works as of mid-2015. According to a statement by the head of the Press and Publications Council in November 2014, the new press law will include sections governing online journalism.[72] Also in November 2014, the Sudanese police department stated that it had over 200 cybercrime cases open against 250 defendants during 2014, which the authorities used as an argument for including online journalism in the new press law.[73] Activists believe that the government exaggerated the number of cybercrime cases to justify passing more restrictive laws to regulate the internet.

Online journalists have no legal status in Sudan.[74] While this legal limbo can be beneficial for online

63 Committee to Protect Journalists, "Repressive press law passed in Sudan," June 11, 2009, https://cpj.org/x/2c67.

64 Amnesty International, "Sudanese security service carries out brutal campaign against opponents," July 19, 2010, http://bit.ly/1OP3OOi.

65 National Council, "Sudanese Parliament passes new laws," January 28, 2015, http://bit.ly/1M1wRJh.

66 International Transparency, "Sudan visualization," http://www.transparency.org/country#SDN.

67 Lori Baitarian, "Sudan passes freedom of information law but journalists remain wary," Committee to Protect Journalists, February 5, 2015, https://cpj.org/x/5ee7.

68 Other classified information restricted from access: confidential documents; national defense secrets; information about laws in process; personal information such as education, profession, and finance; personal correspondence; information that could affect ongoing negotiations; information related to police investigations or judicial committees; confidential political information; and information that is scheduled to be public. See: "Government classifies 12 types of information and charges fees obtain the information,"[in Arabic] *Alyoum Altali,* January 19, 2015, http://bit.ly/1RSQB75.

69 According to Freedom House interviews with an anonymous Sudanese journalist, March 2015.

70 Author's interview, March 2015.

71 Author's interview, March 2015.

72 "Expert: NISS is capable of blocking websites that are posing a threat to Sudan's national security."

73 "Police: Increase in cybercrimes in the country," *Alyoum Altali*, November 7, 2014.

74 Press and Printed Press Materials 2009: https://www.article19.org/data/files/pdfs/laws/sudan-draft-of-the-press-and-printed-press-material-act-2008.pdf.

journalists, freeing them from the limitations of the restrictive press law, they forfeit many privileges available to print journalists, such as media access at official events.[75]

Prosecutions and Detentions for Online Activities

In the lead-up to the April 2015 general elections, the government took preemptive measures to restrict critical information and silence the opposition by arresting online journalists and activists:

- In December 2014, police detained *Altayyar* journalist Tagelsir Wadelhkhair for publishing on the newspaper's website a story about real estate corruption that involved the senior legal advisor to the Ministry of Justice and the former director of the Land Registry Office.[76] He was held for one day and charged with defamation.

- In May 2015, online female activist Solafa Saad was arrested by plainclothes security services following a Facebook post describing her personal experience with racism, which was widely disseminated.[77] She was interrogated for seven hours, during which her interrogators blamed her for the wide circulation of her Facebook post. The interrogators were particularly furious that her post was picked up by the satirical Facebook page "Al-Bashir Diary."[78] Saad was beaten by her interrogators, who used racial slurs and shaved her head for talking back at them.[79]

- In July 2015, Waleed Al Hussein, the creator of the critical online news outlet, *Al Rakoba*, was arrested by the authorities in Saudi Arabia, where he had been residing with his family.[80] As of September, he was being held in solitary confinement without charges and subjected to interrogations about his work with *Al Rakoba*. Family members believe he was arrested at the request of the Sudanese government, which had targeted Hussein for his work in the past and was seeking to have him extradited back to Sudan.[81]

Surveillance, Privacy, and Anonymity

Unchecked surveillance of ICTs is a grave concern in Sudan. The Sudanese government actively monitors internet communications on social media platforms, particularly targeting online activists and journalists during political protests, and 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, in-

75 Author's interview, March 2015.

76 "Police detains journalist Tagelsir Wadelhkhair and keeps him in Cybercrime Procuratorate Office," [in Arabic] *Almshaheer,* December 26, 2014, http://bit.ly/1M2GTjH.

77 Solafa Saad, Facebook Post, April 30, 2015, http://on.fb.me/1NRkypr.

78 Retrieved from: Al Bashir Diary, Facebook Photo, May 4, 2015, http://on.fb.me/1W1sdk5.

79 Retrieved from the activist Facebook account - her status was set to public. Solafa Saad, Facebook Post, April 30, 2015, http://on.fb.me/1NRkypr.

80 Journalists for Human Rights, "Saudi Authorities Detains Sudanese citizen in Al-khobar as being demanded and sleeked by Sudanese Intelligence organs," September 1, 2015, http://bit.ly/1LzJuw0.

81 Amnesty International, "Sudanese Activist Arrested, Risks Deportation," urgent action, September 9, 2015, http://bit.ly/1LH10lk.

cluding on the networks of the private telecom provider Canar.[82] In addition, Citizen Lab also located sophisticated computer spyware technology known as Remote Control System (RCS) by the Italian company Hacking Team in Sudan in early 2014.[83] Advertised by Hacking Team as "offensive technology" sold exclusively to law enforcement and intelligence agencies around the world, RCS spyware has the ability to steal files and passwords and intercept Skype calls and chats.[84] Internal emails leaked by hackers in July 2015 confirmed that Sudan's NISS had purchased Hacking Team's RCS spyware in 2012,[85] though another leaked email from January 2014 revealed that training of intelligence agents was stymied by an overwhelming lack of computer literacy and English-language skills.[86] Other leaked emails revealed that the company had discontinued business with Sudan in November 2014.[87]

Use of mobile phones has become increasingly dangerous for activists, given widespread suspicion that the authorities possess phone-tapping and location tracking tools.[88] A number of Sudanese journalists and activists have reported fears that their phones are tapped,[89] and there is a strong belief among Sudanese activists and journalists that the government has advanced capabilities to remotely activate a mobile phone's microphone to eavesdrop on conversations even if the cell phone is switched off. According to anonymous sources, the Iranian Ambassador once requested journalists to place their inactive cell phones far away from their conversation with the Ambassador, who had admitted that they [the Iranians] themselves had introduced this capability to the Sudanese government.[90]

SIM card registration requirements were enacted in 2008, compromising mobile phone users' privacy and anonymity, particularly given the strong sense among observers that the government is able to access user communications through providers without due process.[91] In a renewed effort to enforce SIM card registration—which requires an official identification card and home address information[92]—the government disconnected all unregistered SIM cards in June 2014 and reportedly plans to link SIM cards to users' national identification numbers in the future.[93]

Intimidation and Violence

Security agents in Sudan regularly employ extralegal intimidation, harassment, and violence against online journalists and activists. The authorities also routinely abuse political detainees to obtain access to private communications that could be used as evidence in court.[94] In one case from Sep-

82 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.

83 Bill Marczak, et al., *Mapping Hacking Team's "Untraceable" Spyware,* Citizen Lab, February 17, 2014, http://bit.ly/1kPDo0Y.

84 Hacking Team, "Customer Policy," accessed February 13, 2014, http://bit.ly/1GnkbjG.

85 PDF of a receipt that shows the National Intelligence and Security Services of Sudan purchased Hacking Team's services: http://bit.ly/1Pv9A9p.

86 Email from Alessandro Scarafile, "Sudan Follow-Up," Hacking Team, http://bit.ly/1jxGpWe.

87 Cora Currier and Morgan Maqruis-Boire, "A Detailed look At Hacking Team's Emails About Its Repressive Clients," *The Intercept*, July 7, 2015, http://bit.ly/1jxGv0h.

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

89 Lori Baitarian, "Sudan passes freedom of information law but journalists remain wary," Committee to Protect Journalists, February 5, 2015, https://cpj.org/x/5ee7; Author's interview, March 2015.

90 Author's interview, March 2015.

91 Freedom House interview, March 2015.

92 "NTC announces the end of grace period to register sim cards," [in Arabic] *Sudani Net*, June 1, 2014, http://bit.ly/1W2A0n3.

93 "Sudan: Telecoms companies block non-registered SIM cards," *African Manager,* June 1, 2014, http://bit.ly/1NRlJ8x.

94 "Sudan: Telecoms companies block non-registered SIM cards."

tember 2014 reported by the Sudanese Human Rights Network, NISS officials used torture to force a political detainee to reveal his email passwords.[95]

Sudanese women are regularly targeted for harassment and cyberbullying by both state and non-state actors for their online activities. Throughout 2014-2015, numerous female bloggers received online threats for activities that ranged from sharing their views on wearing the hijab to writing feminist poetry.[96] There were also reports of security agents arbitrarily detaining female online activists for periods between seven hours and three days on spurious charges of defamation and spreading rumors.

Technical Attacks

Independent online news outlets are frequently subject to hacking attacks by what activists believe is the work of the Cyber Jihadist Unit. A group calling itself Haras al Hudoud ("soldiers of the frontier") also claimed responsibility for several technical attacks throughout the year,[97] advertising itself on screen when users tried to access hacked sites while they were down.[98] Some online newspapers reported hacking attempts traced to hackers in India and Sudan.[99]

Several cyberattacks against critical news websites and activists' social media accounts occurred during the coverage period, escalating around the April 2015 general elections:

- The website of *Nuba Reports*, which provides in-depth coverage of ongoing conflicts in Sudan's war-torn regions, was hit in September 2014 with a massive DDoS attack. The attack came three days after a *Nuba Reports* summary of human rights violations in the conflict regions since 2012 was circulated at the 27th session of the UN Human Rights Council in Geneva.[100] Since then, the site has been under constant attack.[101]

- In October 2014, during the campaign to raise awareness about the mass rape of 200 women in South Darfur, campaign leader Khalid Ewais's Facebook account was hacked a number of times, leaving it disabled for five days in a row during one of the attacks.[102]

- In November 2014, independent outlet *Alrakoba* was hacked by Haras al Hudoud and was offline for a day.

- On April 12, 2015, the eve of national elections in Sudan, online news outlets *SudaNile* and *Hurriyat* experienced simultaneous Denial of Service (DoS) attacks. The outlet *3ayin* was attacked two days later. Consequently, two of the websites were disabled for over ten hours, while *SudaNile* was down for five consecutive days.

95 See the full report on the Sudanese Human Rights Network, التعذيب داخل معتقالت جهاز االمن, 2015, http://bit.ly/1NkPgEo.

96 Author interviews. "Hijab is a head covering worn in public by some Muslim women" *Oxford Dictionary*. Sudanese Public Order Law orders that women wear head cover when they are in public space.

97 "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." See Freedom House, "Sudan," *Freedom on the Net 2014*.

98 Alnilin [in Arabic], http://www.alnilin.com/1183731.htm.

99 Author's interview.

100 Reporters Without Borders, "HACKERS ATTACK WEBSITE THAT COVERS SUDAN'S WAR-TORN REGIONS," September 19, 2014, http://bit.ly/1BTrNnN.

101 "NUBA REPORTS WEBSITE UNDER ATTACK,"*Nuba Report*, September 18, 2014, http://bit.ly/1LkSdUS.

102 Author's interview.

Facebook user Wad Galuba,[103] who posts news about corruption and insiders insights of NISS operations, reported frequent hacking attempts and death threats every time the user published a hot topic.[104]

International experts and commentators on Sudan also reported massive, and repeated, attacks on their online accounts.[105]

103 Facebook Page, https://www.facebook.com/Wdglibaa.

104 Author's interview.

105 Eric Reeves, Twitter Post, February 22, 2015, http://bit.ly/1KkRf6X; Eric Reeves, "I Have Been Silenced," New York Times, February 25, 2015, http://nyti.ms/1Gf5oYJ.