



The Unfreedom Monitor

A Methodology for Tracking Digital Authoritarianism Around the World

SUDAN
COUNTRY REPORT

Khattab Hamad

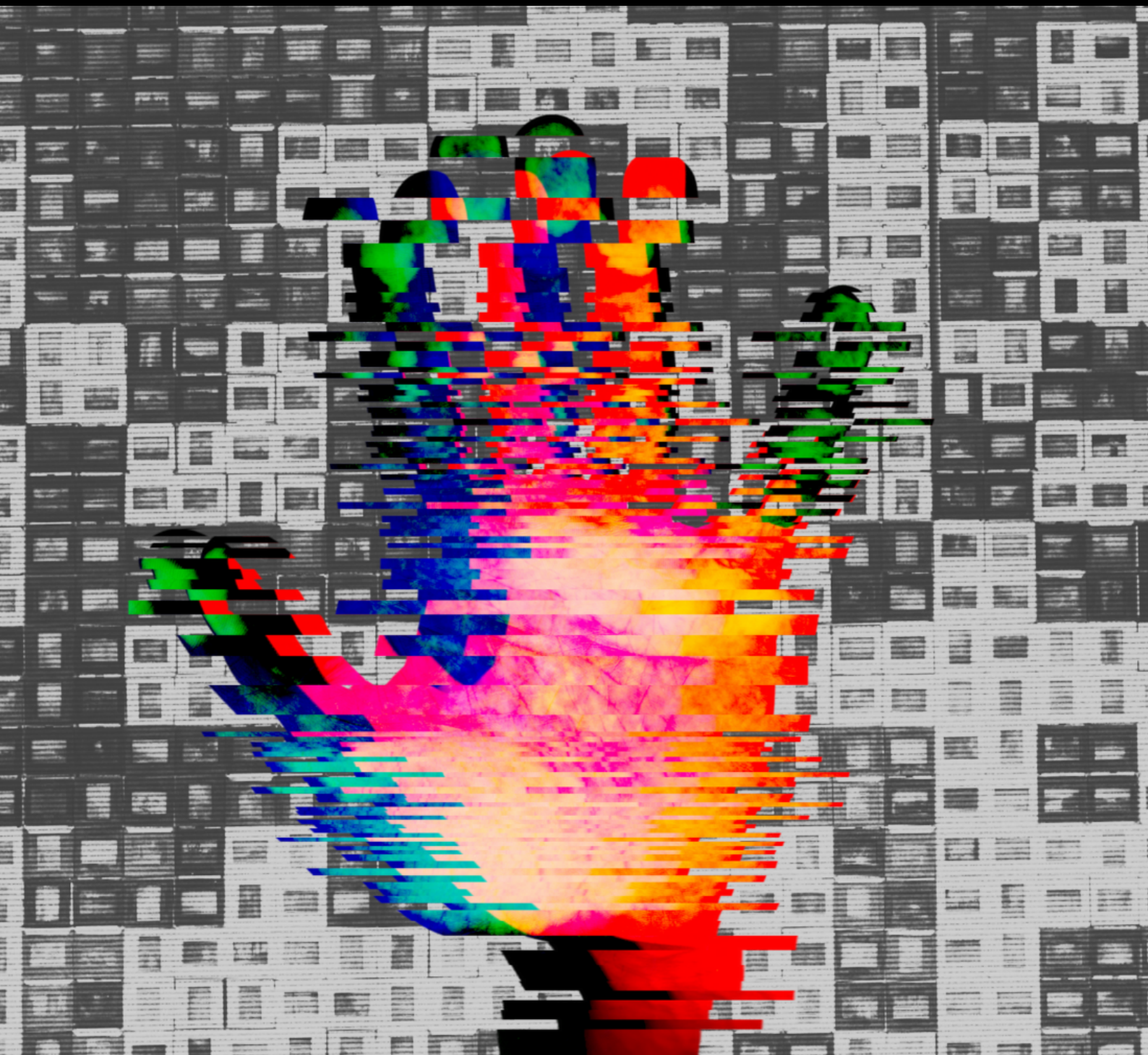


Table of Contents

Executive Summary	4
Background	5
Sudan's Political History	6
Sudan's Internet Pattern and Penetration	9
Methodology	10
The Main Contours of Digital Authoritarianism in Sudan	14
The Tools and Methods they Use	16
How do Citizens Respond to the State's Networked Authoritarianism	20
Analysis and Conclusion	21

Acknowledgements

The Unfreedom Monitor is the collective work of dozens of researchers and writers spread across multiple countries and working in time zones. Desk research was supported by colloquia and research assistance from the Global Voices community. In the interests of security, the names of all the team members have been withheld in this report. For citation purposes, the report can be attributed to "Global Voices Advox." Any errors or omissions should also be addressed to Advox at advox@globalvoices.org. Funding for this project was provided by the Deutsche Welle Academy (DW) which in turn received funding from the Federal Republic of Germany through the BMZ, as well as by other Global Voices supporters, a list of which can be found on our [sponsors page](#).

© Advox 2022



Stichting Global Voices

Kingsfordweg 151
1043GR Amsterdam
The Netherlands
<https://globalvoices.org>



(c) Advox, April 2022.

This work is licensed under a Creative Commons Attribution 4.0 International License

EXECUTIVE SUMMARY

Digital authoritarianism is a growing global trend, yet there is little comparative data on how the phenomenon is playing out in different countries around the world. The Unfreedom Monitor is an initiative by Global Voices Advox to understand, map, and make comparisons on the phenomenon in different contexts, including Sudan. This paper explores the challenges that Sudanese people face in the digital space by studying the motives, methods, and tools of authoritarians and the responses of the people as they attempt to bypass digital authoritarianism.

The study combined the Global Voices' Civic Media Observatory method with qualitative analysis of the contextual issues around digital authoritarianism to define the main contours of digital authoritarianism in Sudan. The paper finds that fear of accountability, fear of losing power, protection of private and family interests, protection of existing alliances, and other ideological reasons drive Sudanese autocrats to copy the techniques of authoritarians in other contexts.

Many of the tools and methods deployed in Sudan are deployed to extinguish online activities. The methods are not limited to censorship, and disinformation, but also include coordinated inauthentic behaviour (CIB), revoking access, and enacting loose laws. The government also uses laws to enable digital authoritarianism and give its tactics the cover of legality. The government has access to all telecommunication infrastructure (data centers and offices), which threatens cyberspace safety and users' privacy. Yet there is resistance. This research found that the citizens inside and outside Sudan used various methods to circumvent digital repression and defend themselves from the violence of the state, physically and in cyberspace.

BACKGROUND

Sudanese people use technology in many parts of their social and political lives. A lot of people use technology in business, agriculture, education, entertainment, and other fields that return them benefits. Other parties use technology illegally for their personal benefit by committing cyber crimes.

Since the internet revolution began and smartphones became an important extension of the body, the internet has been a source of information and space that lets people express their opinions and share knowledge freely without restrictions. Inevitably, some actors — often politicians and political organisations — started to publish fake information in the digital space to support their agendas and defend their interests.

The misuse of technology impacted public life in Sudan — including the efforts to build a democratic state. In 2019, in the eastern city of Kassala, the authorities ordered the shutdown of the internet because of a tribal conflict between two ethnic groups. A few members of the parties in the conflict used the internet and social media platforms to spread hate speech against each other to mobilise people. This behaviour created ethnic polarisation which unfortunately claimed eight lives (“Precautionary internet slowdown”) In another instance, some extremists used social media platforms to create a campaign to flog the girls who are “not wearing the Islamic dress” (“Boo”).

The misuse of information also affected the efforts to combat the pandemic. During the COVID-19 pandemic, the advocates of the ousted regime started a campaign saying there is no COVID-19, calling on their supporters to protest against total lockdown, saying the pandemic was a ruse the government was using to restrict freedom of expression and assembly (“Revolution of Awareness”). The lack of awareness of public health had an impact on vaccination campaigns, which led the government to create a media plan to confront the misinformation around vaccination (“Rumours and Misinformation”). Economically, Sudan has a parallel market of currency exchange, whose rates rise and fall depending on rumours (“Because of a rumour”).

SUDAN'S POLITICAL HISTORY

Historically, the Sudanese Armed Forces (SAF) have stood in the way of democracy taking root in Sudan. Since its independence from the British in 1956, Sudan has not been ruled by a civilian-led or democratic elected government for longer than three years (Infoplease).

Elections were held in Sudan many times; the first elections were held in 1958 after the independence from Britain (Gosnell 409–417). The second elections took place in 1965 and the third followed after three years when the government was dissolved ("Sudan"). After 16 years of military rule (1969–1985), elections were held in 1986 (James L. Chiriyankandath 96–102). But the government hadn't been in power for three years, when Omer Al-Bashir took power in a coup. He continued to hold that power for thirty years, while going through the motions of democratic process to legalise his rule ("Sudan").

After the overthrow of Al-Bashir, there was hope for a truly democratic system, but Sudan has again been under military rule since October 25, 2021, when Lt. Gen Burhan led a military coup against his partners in the transitional government which came after the Sudan uprising (Hamad). For now, there is no separation between the various arms of government (judiciary, executive, legislature) as Burhan appoints all their authorities ("Sovereign Council").

Sudan is experiencing a special period in its modern history, isolated from the international community because of sanctions and its presence on the list of state sponsors of terrorism. This is why it is trying to build sustainable ties with the international community, which has opened a space for foreign entities to express opinions about how the domestic issues in Sudan should be. The UN, the Troika (the US, the UK and Norway), the EU, the African Union, the Kingdom of Saudi Arabia, the UAE, and Egypt are the main players that have key roles in Sudan. The UN, represented by its Integrated Transition Assistance Mission in Sudan (UNITAMS), condemned the coup and played a key role after it by starting a dialogue with various parts of Sudanese society to solve the political crisis. The US is the key player in impacting Sudan's domestic affairs after removing Sudan from the list of state sponsors of terrorism and lifting economic sanctions. The other countries and unions mentioned established a group called "Friends of Sudan" which was working to promote the democratic transition, civic empowerment and economic aid. This led Sudan to be careful about the future of its relationship with other countries.

“ Sudan is experiencing a special period in its modern history, isolated from the international community because of sanctions and its presence on the list of state sponsors of terrorism. ”

Not only do foreign countries have an impact on how the country runs, international financial organisations have a say in the country's economic policies. The International Monetary Fund (IMF) and World Bank pressured Sudan to reform its economic structure to join the Heavily Indebted Poor Countries (HIPC initiative). The World Bank estimated Sudan's debts at USD 56.6 billion. This led the Sudanese government to remove subsidies from oil and wheat and then decide to float its currency. These decisions were hard for the citizens to accept, so the World Bank provided cash aid to the Sudanese citizens to help them to adjust to the new economic situation.

The Sudanese revolution started on December 19, 2018, when the pupils of a school in Atbara City, Northern Sudan, took to the streets to express their discontent with the increasing price of bread. This protest inspired the rest of the citizens to work to oust the Al-Bashir-led Islamist regime of Inqaz. The people succeeded in removing Al-Bashir, and then began a new era in Sudan history, when the Forces of Freedom and Change (FFC) signed a political agreement with the Transitional Military Council (TMC). This agreement started a power-shared transitional period in Sudan between TMC and FFC.

The transitional government convinced the US to remove Sudan from the list of state sponsors of terrorism and lift economic sanctions. Also, it succeeded in stopping the war in the Darfur region when it signed a peace agreement with the rebels in 2020 in Juba. Then, the rebels who signed the peace agreement worked with Burhan, the TMC leader, to stage a coup against his partners in the FFC on October 25, 2021. Burhan worked to bring back the members of the ousted regime to work once more in the state's chambers.

The situation of press freedom in Sudan is bad. Despite the presence of the internet, the authorities tried to contain civil liberties, one of which is press freedom. It's important to mention that Sudan has ratified key international human rights instruments that guarantee the right to freedom of assembly and freedom of expression. But, according to the Freedom House report on Sudan in 2021, Sudan's freedom score is 17/100, which is very bad.

Sudan has a poor press freedom record, being among the worst countries on the World Press Freedom Index where it is ranked 159th out of 180 countries. Despite the success of the revolution to remove the Islamist regime of Al-Bashir in 2019, the same behavior has continued as the transitional government suspended the issuance of two newspapers in August 2021 (during the democratic transition) using the same law that the Al-Bashir regime used.

Sudan's geolocation is unique as it lies between Arabian and African nations. This location put Sudan under focus and it was targeted by the regional media which is so strong because of the existence of media networks such as Al-Jazeera and Al-Arabiya. These media outlets have an effect on public opinion in Sudan. The official language in Sudan is Arabic, which is also the most popularly used language in the regional media, which is one of the factors that led the regional media networks to assume more importance than local media outlets, which offer poor coverage.

According to the 2017 newspaper circulation report, there are 45 printed newspapers in Sudan (Eltigani). There is no data about the number of online news websites, but a huge number of news websites appeared after the Al-Bashir regime was ousted. These websites publish anonymously without releasing any information about the owners, editors or even the authors of the content.

Several practices reduce press freedom in Sudan, from pre-issuance censorship and bad laws, to withholding advertising (the government is the biggest advertiser in Sudan, giving it the power to shut out a media outlet from ads) These practices represent obstacles on Sudan's journey towards press freedom. The Press and Publications Law of the year 2009 mentioned the creation of a National Council for Press and Journalistic Publications to regulate the press industry. The law also mandates a licensing system for newspapers



with paying fees to establish institutions to strengthen the press. The law obliged all journalists to register in the Federal Union of the Sudanese journalists to have the right to work in journalism. These requirements affect press freedom because the council has the authority to suspend the issuance of newspapers under article 33(1)(d).

With the press freedom situation in Sudan, some news websites started to appear and numerous journalists started blogging to deliver their opinions and the facts to the public without restrictions. Despite this, blogging is not common in Sudan. Most Sudanese writers are writing on Facebook because it's the most popular platform that the Sudanese use.

SUDAN'S INTERNET PATTERN AND PENETRATION

Sudan received the first piece of information over the internet in 1996 (El Tigani). Since then, the number of internet users has risen, but it is still low in comparison with the population. Internet penetration is low in Sudan, with 30.9 percent of the population, representing 13.7 million people, using the internet as of January 2020 (Kemp). As of December 31, 2020, the total number of active SIM cards in Sudan is 34,251,690. This number does not represent the total number of the people who use mobile phones because many people have more than one SIM card and corporations use data SIM cards to access the internet.

Arabic is the most widely used language on the internet in Sudan. According to a study in 2014, the mobile cellular telephone is the most widely used means of internet access, more than 14 times higher than fixed telephone. The lack of electricity is the biggest impediment to using the internet in rural areas, where it is a problem nearly twice as bad as it is in urban areas (Mohamed Nour). According to a survey conducted by Afrobarometer in 2018, women in Sudan are nine percent less likely to access the internet regularly than men (Lardies et. al).

There are four main ISPs in Sudan: Sudatel, Canar, Zain Sudan and MTN Sudan. Sudatel is the only government-owned company but there are many foreign investors who are shareholders ("Sudatel Telecom Group Company Data - Mubasher Information"). Canar is owned by Bank of Khartoum (92.3 percent); the bank bought the ISP from the Emirates Telecommunications Group Company PJSC (Etisalat group) ("Canar Telecommunications Co. Ltd"). Bank of Khartoum is owned by many foreign investors from GCC and Middle East countries. Zain is a part of the Kuwaiti Group Zain; the group owns the company fully according to its annual report of 2020 ("Zain Annual Report 2020"). MTN is a part of the Southern African company MTN, which owns 85 percent of the company ("MTN Group Limited Integrated Report for the Year Ended 31 December 2012 - MTN Sudan").

Because of restrictions on civil liberties, the internet represents the main way that citizens and journalists can evade these restrictions to express their opinions. As mentioned above, journalists started blogging to publish the information that the authorities restricted offline publication of. With the advent of social media platforms such as Facebook and Twitter, blogging became rare in Sudan. Facebook has 1.3 million users in Sudan, which represents 2.8 percent of the population ("Facebook Users by Country 2022").

“ Internet penetration is low in Sudan, with 30.9 percent of the population using the internet as of January 2020 ”

Facebook is the most commonly used social media platform in Sudan because of the Facebook Zero initiative that provides free access to a stripped-down text-only version of the platform. Despite the rarity of blogging and the dependency on social media to easily interact with information, local media institutions are still the main source of news in Sudan because they have a strong presence online. The outlets developed their digital tools to be up to date, and established websites, email newsletters, WhatsApp groups and Telegram channels. These tools led the local media to invade the digital space and keep their position of providing information to the public.

METHODOLOGY

In this research, we combined the methodology used in Global Voices' previous work on media observatories with an in-depth analysis of the contextual issues around digital authoritarianism. The Civic Media Observatory (CMO) approach is primarily qualitative and looks beyond socio-technical causes to consider power analysis, offer a way to discuss effects, and to emphasise what works as well as what's negative.

This research method allows us to compare, draw lessons, and consolidate learning about the trends, systems and rules that influence what the Sudanese people know, and how they know it. It includes datasets of media items, structured analysis of context and subtext and recommended actions. We use Airtable, a relational database, for documentation and collaborative work.

FINDINGS

Because the internet is growing to be the main source of information and the main way to connect with people and other aspects of life, it can be a threat to a dictatorial regime because it's a wide space that is hard to manage and limit. To counter this, authoritarians began to plan methods and create tools to narrow it to a manageable size. The effort to frame the digital space is called digital authoritarianism.

Digital authoritarianism can be defined as the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations (Polyakova and Meserole). Authoritarian regimes have developed many techniques to repress the freedom of digital space, which has no international standards till date. These techniques can be framed under many themes, such as privacy violation, data protection, surveillance, repression of freedom of expression, narrowing the right to access the information, restricting access to the internet, and influencing public opinion. There is a lot of evidence that the Sudanese authorities practise digital authoritarianism.

EVENTS SHOWING THE EXISTENCE OF DIGITAL AUTHORITARIANISM IN SUDAN

Privacy

- In February 2014, the head of the communication committee in the parliament (National Assembly) claimed that the spying on phone calls and internet censorship would stop (Abubkr).
- On October 27, 2021, the military coup forces appeared to use Article 25 of the National Security Law to inspect individual's phones to remove documentation of human rights violations that were perpetrated by security forces ("Massive crackdown on opponents of the coup in Sudan").

- In July 2013, Citizen Lab, a Toronto-based interdisciplinary laboratory that does research at the intersection of technology and human rights, identified the presence of the Blue Coat ProxySG device on Canar network, a privately-owned Sudanese internet service provider (Marquis-Boire et. al pp. 14-15).
- General Intelligence Service (GIS) agents planted Blue Coat surveillance software on the phones and laptops of at least 11 activists during an out-of-country meeting and training (Freedom House).
- The Telecommunication and Post Regulation Authority (TPRA) obliged operators to register a person's ID when they want to subscribe to telecommunication services. This requirement prevents users from remaining anonymous (Freedom House).

Speech

Despite the laws that guarantee freedom of expression and freedom of assembly, the government in Sudan doesn't respect the law, because they don't allow peaceful protestors to practise their right to express their opinion. The disrespect does not describe only the military regimes; it's also applicable to the civilian-led governments.

During the Sudanese revolution in 2019, the Al-Bashir regime killed 246 people ("Sudan Doctors Committee: 1,702 people have been killed and injured since the outbreak of the revolution, and the longest strike in the world has been lifted"). Then, during the transitional period which was led by civilians, many peaceful protestors were killed by police forces (Awadalla and Eltahir). Coup forces are still killing citizens who reject the coup ("Sudan Coup Death Toll Climbs to 42").

Orwa Elsadig, a state worker, faced a lawsuit that was registered against him by Lt. Gen Burhan — who is also a state worker but he is the president — because Orwa criticised him publicly (Hamad, "Sudan's Revised Cybercrime Law Falls Short on Its Promise").

Access

One of the practices of digital authoritarianism is restricting access to the internet and communication tools. Internet shutdowns can technically be defined as an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information (Olukotun). Since 2018, the phenomenon of internet shutdowns started rising at an unexpected rate, but the shutdowns themselves didn't start in 2018.

“ Orwa Elsadig, a state worker, faced a lawsuit that was registered against him by Lt. Gen Burhan — who is also a state worker but he is the president — because Orwa criticised him publicly

”

The first shutdown in Sudan's history occurred in 2010, when the government blocked the access to YouTube over a video posted showing election fraud in Eastern Sudan ("Sudan reportedly blocks YouTube over electoral fraud video"). The second shutdown occurred in 2013, during the mass protests against the lifting of fuel subsidies (Micek). The third internet shutdown occurred in 2018, after the spark of the Sudanese revolution, when the government blocked social media to stop people from sharing information about the planned protests (Saba and Eltahir). Then, the TMC shutdown the internet after the massacre of Khartoum when the military and Rapid Support Forces killed more than 100 citizens (Hamad, "Internet Shutdowns in Sudan: The Story Behind the Numbers and Statistics"). This shutdown lasted thirty seven days and is considered as the longest internet disruption in Sudan's history.

In 2020, the transitional government shut down the internet twice. The first was in March during a tribal conflict, and the second was amid the secondary school exams — ostensibly to limit cheating (Fatafta). The transitional government shutdown the internet again during the secondary school exam of 2021 sessions for the same reason (Fatafta, "Internet Shutdowns During Exams: When MENA Governments Fail the Test").

Last but not least, the military shut down telecommunication synchronously with the coup d'état of October 25. This cut off lasted for 25 days ("Internet Connection Restored in Sudan."). The shutting down of telephone services happens frequently, and it affects emergency services, which can be considered as a crime against public safety.

Internet shutdown is not the only method that the state uses to narrow the access to telecommunications. The Value Added Tax (VAT) for telecommunication services is 40 percent, which is a considerable obstacle to ensuring equitable access to the internet for all citizens ("Sudan raises telecom taxes, increase in call and internet prices").

Information

The digital space in Sudan is filled with disinformation and misinformation, and malinformation appears from time to time. The campaigns don't only come from domestic actors; many foreign entities, countries and agencies release campaigns to impact the digital public opinion in Sudan.

The regime of the National Congress Party — the party of Al-Bashir — was one of the first authoritarian regimes that worked to manipulate the digital space as it established a unit in the National Intelligence and Security Service (NISS) called Cyber-Jihadist (Abubkr). This unit represents the technical support arm of the intelligence service. Its mission is not limited to providing digital solutions such as equipment or programs; it also works in manipulating the digital space to affect the independence of public opinion.

Facebook deleted accounts, pages and groups for engaging in foreign interference — which is coordinated inauthentic behaviour — from its platform in October 2019. Facebook said these accounts originated in Russia and targeted many countries including Sudan (Gleicher).

Facebook also said they observed a campaign that originated inside Sudan in May 2021. The campaign has been linked to individuals in Sudan, including those associated with the “Future for Reform and Development” movement, a political party established at the end of 2019 (“May 2021 Coordinated Inauthentic Behavior Report”).

Stanford Internet Observatory published a report in December 2020 about Russian interest in Sudan and about the disinformation campaigns Russia runs (Grossman et. al). A statement issued by representatives of the UK, the US and Norway mentioned that the Wagner group — a Russian private military services company — has a presence in Sudan, and they work to manipulate the Sudanese cyberspace with disinformation (Eltahir and Abdelaziz).

The paramilitary militia Rapid Support Forces (RSF) — formerly called Janjaweed — practises disinformation through foreign actors using CIB (Beam Reports).

THE MAIN CONTOURS OF DIGITAL AUTHORITARIANISM IN SUDAN

The stories above led us to study what motives authoritarian forces in Sudan have to practise digital dictatorship, so we could map out the contours of networked authoritarianism in Sudan.

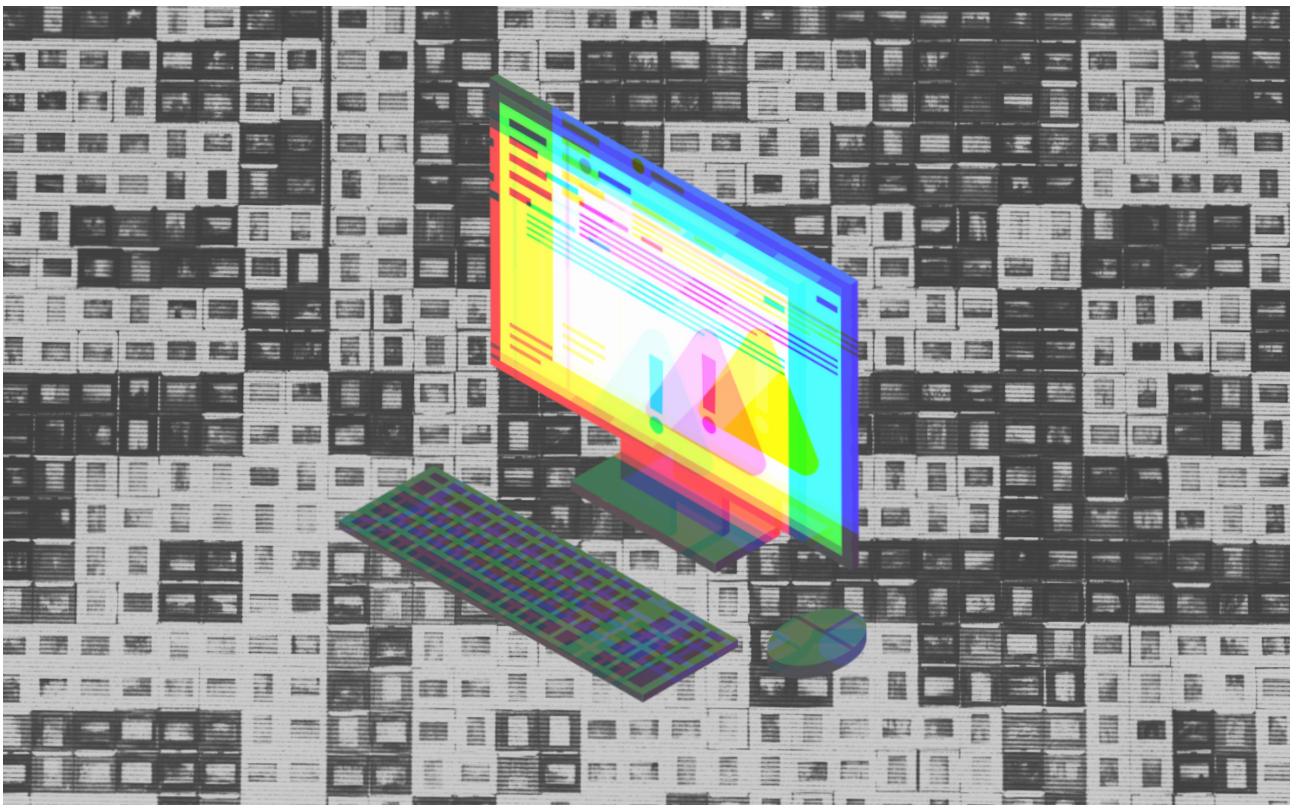
Some of those motives are below:

a. Fear of accountability

The authorities blocked YouTube in 2010 and shut down the internet in June 2019, to stop the sharing of documented human rights violations online. This footage could be used against the government as clear pieces of evidence of violations of human rights. The fear of being accountable is moving the authorities to create new methods to protect themselves.

b. Fear of losing power

The authorities used the state's digital resources to support their rule so they can retain power for the most possible time. The NCP regime monitored the situation in Egypt during the Egyptian revolution when the Egyptian youth used Facebook to coordinate planned protests which resulted in the ousting of the former president, Hosni Mubarak. To counter this, the authorities established the Cyber-Jihadist Unit to manipulate information on Facebook to decrease the impact of the opposition, which was calling on the people to protest against the dictator. The internet disruptions imposed in the Al-Bashir and Al-Burhan eras stopped the opposition from planning protests and coordinating among themselves.



c. Protecting private and family interests

Mohamed Hamdan Daglo — known as Hemeti — the commander of RSF, has numerous businesses in Sudan that have privileges above the rest of the commercial and production activities in Sudan. Hemeti and his family are outcasts in Sudanese society, so he must try to protect his business; one of the methods is by using established IT tools to his benefit.

Darfur 24, a reliable news website, reported that RSF tried to buy Zain Sudan, a telecom company that has the largest number of subscribers in Sudan, but RSF released a statement denying this claim.

d. Protecting the existence of regional or international alliances

Because it was under US economic sanctions, Sudan started to search for other alliances to empower its capabilities. Sudan built good relationships with Russia, China, and Iran. This alliance tried to empower Sudan in many areas, including military, agriculture, and technology because Sudan brings to the alliance many resources such as metals, agriculture, animals, and manpower. For this, the Cyber-Jihadist unit has used its capabilities to paint the US in a negative light, while holding China and Russia up as better. They used the Islamic angle to evoke identification with Iran to push people to normalize ties with it.

e. Ideological motives

Sudan was ruled by the (Islamist) National Congress Party (NCP). Like any ideological regime, the Islamist regime is always attached to the ideological fear of losing power to the left. This fear led the NCP to broadcast a rhetoric of demonisation on social media, against communist and liberal parties and ideological parties that adopt Arab unity, using the religious sentiment rooted in a large part of the Sudanese people to enable its rule.

Despite losing power, NCP members still use this method to demonise other parties in order to reclaim power.

THE TOOLS AND METHODS THEY USE

THE METHODS THE STATE USED TO APPLY DIGITAL AUTHORITARIANISM

Sudanese authorities use diverse methods — technological, economical and legal — to apply digital authoritarianism to citizens.

Technologies

These are some of the techniques used by the Sudanese authorities, and uncovered by foreign sources:

Remote Control System

In 2014, Citizen Lab published a report stating that Sudan imported Remote Control System (RCS) from the Italian company Hacking Team (Marczak). The report said that Citizen Lab identified one RCS endpoint in Sudan (VisionValley: 41.78.109.91), in a range of eight addresses called “Mesbar” (an Arabic word meaning a device used to “probe”). Vision Valley is a small ISP that provides internet to enterprises.

RCS enables government surveillance of a target’s encrypted internet communications, even when the target is connected to a network that the government cannot wiretap. It also confers the ability to copy files from a computer’s hard disk, record Skype calls, emails, instant messages, and passwords typed into a web browser. Furthermore, RCS can turn on a device’s webcam and microphone to spy on the target.

According to a document from Wikileaks, RCS can monitor and log any action performed by means of a smartphone (Vincenzetti and Bedeschi).

A leaked invoice shows that the Sudanese government paid EUR 480,000 to Hacking Team as a 50 percent payment for using RCS (“Hacking Team Company Sold Surveillance Tools to Sudan”).

BlueCoat Proxy SG

In 2013, a report published by Citizen Lab, Canada Center for Global Security Studies, Munk School for Global Studies, Sarah McKune and Scott-Railton identified that Sudan has BlueCoat Proxy SG — despite the US sanctions — in the Canar telecommunication network, one of the main ISPs in Sudan (Marquis-Boire et. al 14-15). According to another report published by Citizen Lab, Blue Coat devices capable of filtering, censorship, and surveillance are being used around the world (Marquis-Boire).

“ RCS enables surveillance of a target’s encrypted internet communications, even when the target is connected to a network that cannot be wiretapped. It also confers the ability to copy files from a computer’s hard disk, record Skype calls, emails, instant messages, and passwords typed into a web browser.

”

It's important to mention that the Sudanese government doesn't publish any information about importing surveillance equipment.

However, the government has access to all telecommunication providers' data centres, which lets them access all the data of any subscriber, including current location, citizens' movements and the citizen's social network.

Legal methods

The Sudanese authorities are using laws to repress civil liberties. Sudan has issued laws related to information and technology, such as the Right to Access Information Act and the cybercrimes law, which is known as the Informatics Crimes Law. These laws have vague terms that the state interprets to threaten the opponents and activists.

The Right to Access Information Act 2015

The parliament approved the "Right to Access Information Act" in 2015. This law is the first law related to information accessibility in Sudan. Even though the law has been enacted, nothing is being done to implement it. For example, the law requires the establishment of a Commission for the Right to Access Information, to be responsible for all information employees in any public institution. But nothing has been done to set up this commission, which means citizens still cannot exercise their right to information.

In 2014, Transparency International issued a report considering Sudan one of the top three most corrupt countries in the world (Transparency International). Then, the Sudanese parliament accused the organisation of being "suspicious and operating on a political basis" (Abdelhadi). A member of parliament mentioned that "Sudan should work quickly to enact the freedom of information act, which allows every citizen to view government procedures and ensure their validity and compliance with applicable laws," in order to reflect the real image of Sudan. So, the law was issued to reply to the report to silence the organisation and to whitewash the government's bad history, but it has lain idle since the date it was issued.

The law has many shortcomings that limit the freedom of access to information. It lists 12 types of classified information that are restricted from citizens, including information related to national security and foreign policy (Suliman, "The Case for Reforming the Sudanese Access to Information Act"). These terms are vague, which allows the authorities to limit the ability of the public to fully access information, which narrows the path to transparency and accountability.

Article 10(g) further undermines citizens' ability to access information by empowering any public institution to enforce fees on citizens requesting information (Hamad and CIPESA). The act does not oblige the information holders of any duty to proactively disclose information in their possession (Khalil).

The law explicitly says that the request for information can be made orally by citizens with disabilities, but the same law does not mention how and in which shape the materials will be provided to the requesters who are with disabilities (Abdalla).

The Cybercrimes Law

The first law to combat cybercrimes in Sudan was issued in 2007. In 2018, a new law was enacted but it wasn't published in the Gazette. (The Gazette is the official newspaper of the Ministry of Justice. When a law is published in the Gazette, it is seen as a declaration of the validation of the law or amendment, because the citizens can read it.) Then, the transitional government amended it in 2020 but they published only the amendments to the articles, and not the text of the whole new law. It's important to know that the amendment was limited to amending the severity of the penalty, with the harshest one being up to five years imprisonment as a punishment for spreading pornography.

“ A key problem with this article is that the terms in the article are not defined. This opens up the possibility of abuse, enabling government institutions to crack down on basic freedoms. ”

The law was used by the Sudanese Armed Forces to threaten activists and even state workers who spoke out against the Commander-in-Chief. For this, the army said they appointed a special commissioner to bring lawsuits against individuals who “insult” the army, including activists and journalists, both in and outside of Sudan, who write online (Osman).

The law has many shortcomings.

Article 5-3

The article relates to hacking or stealing data and it says: “Anyone who enters a network of information or a network of communication directly or remotely with the purpose of getting data or information related to the national security or national economy or telecommunication infrastructure or sensitive information will be punished for 10 years or fine or both.”

A key problem with this article is that the terms in the article are not defined. This opens up the possibility of abuse, enabling government institutions to crack down on basic freedoms. Moreover, the law does not mention which institutions are supposed to interpret these broad categories. Is it the Intelligence Service? The Sudanese Police? Military intelligence or RSF intelligence? It's simply unclear and that is worrying.

Article 6

This article relates to the same subject as Article 5, but focuses on the responsibilities of government staff: “Any government employee who enters or makes it easy for others to enter an information system related to the entity where he/she is working without any authorization will be jailed for five years or fined or both.” The new amendment increased punishment to eight years. The same problems related to the lack of clear definitions and interpretation bodies apply.

Article 7

Article 7 relates to network shutdowns. The article criminalises any shutdown triggered by a citizen or a group of citizens but has nothing to say about what should happen if the government itself shuts down the telecommunication networks — something digital activists consider a very grave crime.

Article 19

It discusses matters related to public order, even if the new post-NCP government canceled the Public Order Law itself. This leads to a confusing situation. Public order restrictions have historically been related to (for example) dress, sexual acts, and alcohol. Article 19 focuses mostly on pornographic production: “anyone who produces any kind of pornography using cyberspace or a communication network will be punished for five years or fine or both.”

Article 23

Article 23 criminalises the violation of one’s privacy if committed by a citizen, according to the 2018 law, but not if the violation of privacy occurs as a result of a judiciary or prosecutorial or other “competent authority.” The law does not define what a competent authority is.

Article 24

This tackles publishing lies and fake news. Anyone who publishes lies or fake news in cyberspace will be punished for one year, fined or both. The new amendment increased punishment to four years. The issue here is that the authorities want to judge the citizens against fake news while it is not transparent and doesn’t provide information to the public — how do the citizens know the truth?

These laws are not the only ones that have been used to implement digital authoritarianism in Sudan. There are other laws such as the National Security Law 2010. Article 25 of the law says: “Security has the right to request information, data, documents or things from any person to verify or take.” This article gave the security service the right to legally violate a citizen’s privacy without asking for permission.

The coup forces used vague articles from numerous laws to legalise an internet shutdown for 25 days. They used Article 6 (d) of the Armed Forces Act, which says that the Sudanese Armed Forces are required to “respond to legally defined emergency situations.” The government used Article 8 (2) of the Law on Emergency and Public Safety of the year 1997 as it gives the president power to legislate anything without concerning the legislative authority or the “the parliament” (Hamad, “In Sudan, the Court Stands on the Side of Unrestricted Access to the Internet”).

HOW DO CITIZENS RESPOND TO THE STATE'S NETWORKED AUTHORITARIANISM

The Sudanese people used some circumvention methods and tools to bypass digital authoritarianism. They can be categorised according to the type of violation as per below:

TELECOMMUNICATION SHUTDOWN

To communicate safely during telecommunication shutdowns, the citizens in Sudan used SMS, international calls to connect the two citizens — because domestic calls were down during some events — and satellite phones.

Physical inspection of digital equipment

The security forces frequently ran phone inspection campaigns against protestors, people on the street and the travellers through airports. For this, some digital security experts created simple guidance to protect the phone's contents from extraction in case the security forces took the phone (Salah).

Tracking online activities

Writers, journalists, and human rights defenders used to publish anonymously to prevent being followed by security forces.

Though regional safeguards against digital authoritarianism in Sudan do not exist, numerous international organisations, such as Access Now and Human Rights Watch, have condemned the internet shutdowns (Access Now; Human Rights Watch). RSF condemned the serious consequences of the Sudanese coup on the freedom to report the news and access information ("Press Freedom Under Siege After Military Coup in Sudan").

ANALYSIS AND CONCLUSION

There is a clear digital divide in Sudan as the number of internet users is a very low part of the population. Despite the high contribution of the telecommunication field to the GDP, the Sudanese authorities are not using this contribution to enhance and develop the ICT field to fill the gap of digital illiteracy. Instead, they use taxpayer money to buy expensive equipment for censorship, without publishing these deals.

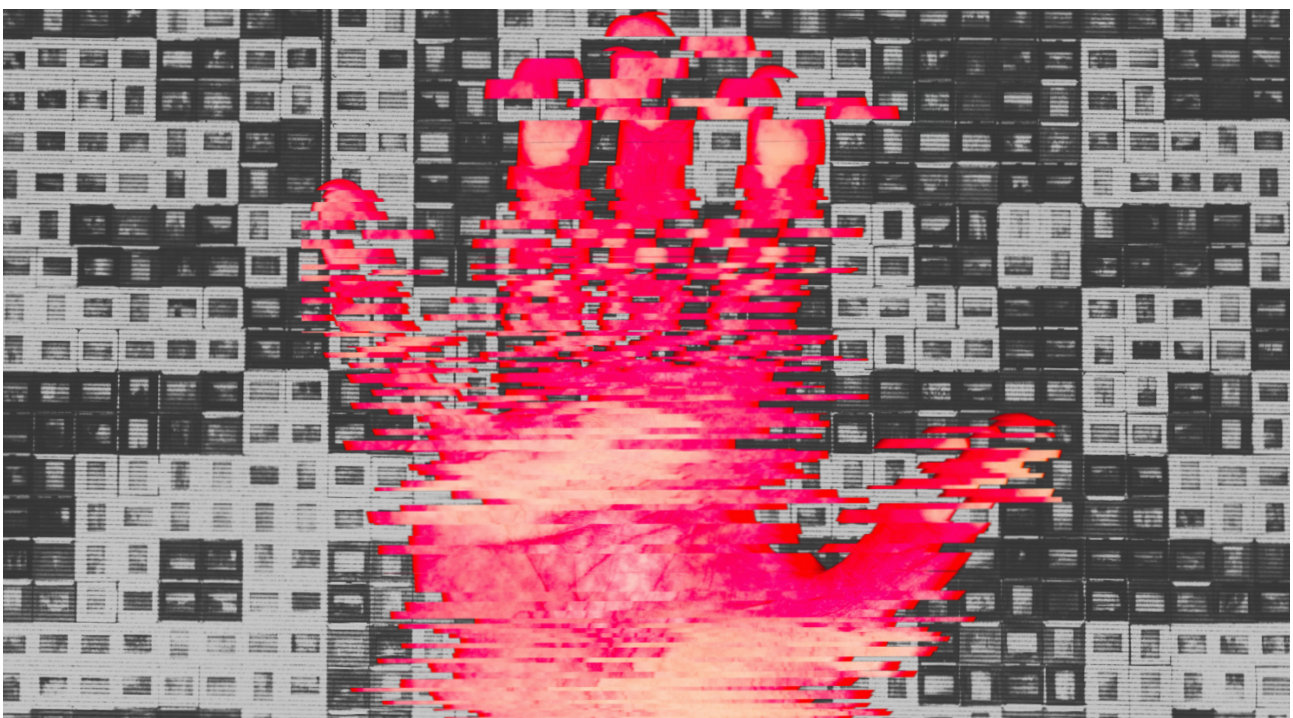
Restricting the freedom of expression and using the state's violence to repress fundamental rights and civil liberties are rooting the image of the authoritarian state in the minds of the citizens which may lead to a state of lack of rights awareness.

Using and amending laws to protect the government interests indicates that the government will enact other laws to restrict the digital space in order to make access to information increasingly difficult.

Government access to ICT infrastructure in Sudan will suppress net neutrality during political crises, affecting people economically and socially, specifically in relation to education and small businesses.

Sudan has low transparency, frequently violates physical privacy, uses unlawful communication shutdowns, an idle access to information act, no freedom of expression, vague laws, and online surveillance, making it easy to say that digital authoritarianism is rooted in Sudan. Digital authoritarianism affects opportunities for foreign investment, stability of life, and social security.

All this is despite the fact that Sudan is a signatory to international treaties that guarantee digital rights — the signing doesn't enforce obligations on states to apply their standards.



Works Cited

- Abdelhadi, Emad. [Sudanese government condemnation of the Global Transparency Report], *Al-Jazeera*, 08 Dec. 2014, <https://bit.ly/3HkcvRj>
- Abdalla, Alradi, "Sudanese Information Law stipulates", 23 Aug. 2019, *Twitter @alradiabdalla*, <https://twitter.com/alradiabdalla/status/1164982201240489984>
- Abubkr, Lemia. "Online Surveillance and Censorship in Sudan | Association for Progressive Communications." *APC*, 11 Apr. 2014, www.apc.org/en/blog/online-surveillance-and-censorship-sudan.
- AfricaNews. "Internet Connection Restored in Sudan." *Africanews*, 18 Nov. 2021, www.africanews.com/2021/11/18/internet-connection-restored-in-sudan/.
- Al-Hassan, Wael. ["Flog girls with a non-Islamic dress-up" is a reprehensible campaign in Sudan faced with popular and official rejection... and with some support], *Annahar AlAraby*, 30 Mar. 2021, <https://www.annaharar.com/arabic/news/arab-world/egypt-sudan/29032021123628665>
- Awadalla, Nadine, and Nafisa Eltahir. "Two Killed as Protesters Mark Anniversary of Massacre in Sudan." *Reuters*, Edited by Dan Grebler, 12 May 2021, <https://www.reuters.com/world/africa/two-killed-protesters-mark-anniversary-massacre-medics-protest-group-2021-05-11/>
- Awad, Abdalhameid. [Awareness revolution, youth], *AlSudani*, 18 Jun. 2020, <https://www.alsudaninews.com/ar/?p=76854>
- Beam Reports. [How Rapid Support Forces seeks to improve its image through foreign interfaces] *Beam Reports*, 14 Feb. 2022, <https://bit.ly/3Oh7r2v>
- "Canar Telecommunications Co. Ltd." *Bank of Khartoum*, 19 Nov. 2018, bankofkhartoum.com/sudan/canar-telecommunications-co-ltd.
- D. Vincenzetti and V. Bedeschi, "Remote Control System V5.1", *Hacking team*, Qtd. in Wikileaks, Accessed 20 Feb. 2022, https://wikileaks.org/spyfiles/document/hackingteam/31_remote-control-system-v5-1/31_remote-control-system-v5-1.pdf
- Eltahir, Nafisa, and Khalid Abdelaziz. "Sudan's Foreign Ministry Denies Presence of Russian Wagner Group." *Reuters*, 22 Mar. 2022, www.reuters.com/world/africa/sudans-foreign-ministry-denies-presence-russian-wagner-group-2022-03-22.
- Eltahir, Nafisa, and Khalid Abdelaziz. "Sudan's Foreign Ministry Denies Presence of Russian Wagner Group." *Reuters*, 22 Mar. 2022, www.reuters.com/world/africa/sudans-foreign-ministry-denies-presence-russian-wagner-group-2022-03-22.
- Eltigani, Eman. "Sudan", *Media Landscapes*, <https://medialandscapes.org/country/sudan/media/print>. Accessed 20 Apr. 2022.
- El Tigani M. El Fatih. "Sudan Internet and .sd Experience", *ITU*, <https://www.itu.int/itudoc/itu-t/workshop/cctld/cctld050.pdf>. Accessed 20 Apr. 2022.
- "Facebook Users by Country 2022." *World Population Review*, worldpopulationreview.com/country-rankings/facebook-users-by-country. Accessed 20 Apr. 2022.

Freedom House. "Sudan." Freedom House, 2020, freedomhouse.org/country/sudan/freedom-net/2020.

Freedom House. "Sudan." Freedom House, 2021, freedomhouse.org/country/sudan/freedom-net/2021.

Fatafta, Marwa. "Internet Shutdowns During Exams: When MENA Governments Fail the Test." *Access Now*, 8 July 2021, <https://www.accessnow.org/mena-internet-shutdowns-during-exams>.

Gleicher, Nathaniel. "Removing More Coordinated Inauthentic Behavior From Russia." *Meta*, 24 Mar. 2021, about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-russia.

Gosnell, Harold F. "The 1958 Elections in the Sudan." *Middle East Journal*, vol. 12, no. 4, 1958, pp. 409–417, <http://www.jstor.org/stable/4323052>. Accessed 20 Apr. 2022.

"Hacking Team Company Sold Surveillance Tools to Sudan." *Radio Dabanga*, www.dabangasudan.org/en/all-news/article/hacking-team-company-sold-surveillance-tools-to-sudan. Accessed 21 Apr. 2022.

Hamad, Khattab. "How Burhan's Coup Could Halt Sudan's Return to the International Community." *Global Voices*, 4 Nov. 2021, globalvoices.org/2021/11/04/how-burhans-coup-could-stop-sudans-return-to-the-international-community.

Hamad, Khattab. "Sudan's Revised Cybercrime Law Falls Short on Its Promise." *Global Voices*, 16 Apr. 2021, globalvoices.org/2021/03/04/sudans-revised-cybercrime-law-falls-short-on-its-promise.

Hamad, Khattab and CIPESA. "Sudan's Bad Laws, Internet Censorship and Repressed Civil Liberties." *CIPESA*, 31 Dec. 2021, cipesa.org/2021/12/sudans-bad-laws-internet-censorship-and-repressed-civil-liberties.

Hamad, Khattab. "In Sudan, the Court Stands on the Side of Unrestricted Access to the Internet." *Global Voices*, 16 Dec. 2021, globalvoices.org/2021/12/16/in-sudan-the-court-stands-on-the-side-of-unrestricted-access-to-the-internet.

Human Rights Watch. "Sudan: End Network Shutdown Immediately." *Human Rights Watch*, 12 June 2019, www.hrw.org/news/2019/06/12/sudan-end-network-shutdown-immediately.

Infoplease. "Sudan." *InfoPlease*, 24 Mar. 2022, <https://bit.ly/3AE6GuR>

James L. Chiriyankandath. "1986 Elections in the Sudan: Tradition, Ideology, Ethnicity: And Class?" *Review of African Political Economy*, no. 38, 1987, pp. 96–102, <http://www.jstor.org/stable/4005902>. Accessed 20 Apr. 2022.

Khalil, Ali. "THE SUDANESE ACCESS TO INFORMATION ACT 2015: A STEP FORWARD", ch. 7, Pretoria University Law Press, https://www.pulp.up.ac.za/images/pulp/books/edited_collections/access_to_information/Chapter%207%20Ali%20Access.pdf

Kemp, Simon. "Digital in Sudan: All the Statistics You Need in 2021." *DataReportal – Global Digital Insights*, 12 Feb. 2021, datareportal.com/reports/digital-2021-sudan.

Lardies, Carmen Alpin, et al. "African Women Have Less Access to the Internet Than African Men Do. That's a Problem." *Washington Post*, 8 Mar. 2020, www.washingtonpost.com/politics/2020/03/06/african-women-have-less-access-internet-than-men-do-thats-problem.

Mohamed nour, Samia. "Overview of the Use of ICT and the Digital Divide in Sudan", *Research Gate*, 2014, https://www.researchgate.net/publication/297192758_Overview_of_the_Use_of_ICT_and_the_Digital_Divide_in_Sudan/citation/download

[Massive crackdown on opponents of the coup in Sudan], Alquds Al-Araby, <https://bit.ly/3NSSMKV>.

Marquis-Boire et. al. "Some Devices Wander by Mistake", *Citizen Lab*, 9 Jul. 2013, <https://citizenlab.ca/storage/bluecoat/CitLab-PlanetBlueCoatRedux-FINAL.pdf> pp. 14-15

Micek, Peter Esq. "Update: Mass Internet Shutdown in Sudan Follows Days of Protest." *Access Now*, 30 June 2020, www.accessnow.org/mass-internet-shutdown-in-sudan-follows-days-of-protest.

"May 2021 Coordinated Inauthentic Behavior Report." *Meta*, 2 June 2021, about.fb.com/news/2021/06/may-2021-coordinated-inauthentic-behavior-report.

Marczak, Bill. "Mapping Hacking Team's 'Untraceable' Spyware." *The Citizen Lab*, 8 July 2017, citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware.

Marquis-Boire et. al. "Some Devices Wander by Mistake", *Citizen Lab*, 9 Jul. 2013, <https://citizenlab.ca/storage/bluecoat/CitLab-PlanetBlueCoatRedux-FINAL.pdf> pp. 14-15

Marquis-Boire, Morgan. "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools." *The Citizen Lab*, 10 July 2017, citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools.

"MTN Group Limited Integrated Report for the Year Ended 31 December 2012 - MTN Sudan." *MTN*, www.mtn-investor.com/mtn_ar2012/ops-sudan.php#. Accessed 20 Apr. 2022.

Osman, Mohamed. "Sudan's Army Threatens Activists, Journalists with Lawsuits." *Human Rights Watch*, 28 Oct. 2020, www.hrw.org/news/2020/07/24/sudans-army-threatens-activists-journalists-lawsuits.

"Press Freedom Under Siege After Military Coup in Sudan." *RSF*, 5 Nov. 2021, rsf.org/en/news/press-freedom-under-siege-after-military-coup-sudan.

"'Precautionary' Mobile Internet Slowdown in Sudan's Kassala." *Radio Dabanga*, 17 Mar. 2020, www.dabangasudan.org/en/all-news/article/precautionary-mobile-internet-slowdown-in-sudan-s-kassala.

Polyakova, Alina, and Chris Meserole. "Exporting Digital Authoritarianism." *Brookings*, 9 Mar. 2022, www.brookings.edu/research/exporting-digital-authoritarianism.

Saba, Yousef, and Nafisa Eltahir. "Sudan Restricts Social Media Access to Counter Protest Movement." *Reuters*, 2 Jan. 2019, www.reuters.com/article/us-sudan-protests-internet-idUSKCN1OW0Z7.

Salah, Reem. [Digital security experts in Sudan], Twitter @ReemooSalah, 7 Nov. 2021, <https://twitter.com/ReemooSalah/status/1457385022353248265>.

"Sudan." *CRS Reports*, 26 May 2015, www.everycrsreport.com/reports/R43957.html.

"Sovereign Council appoints new Sudan's chief justice", *Sudan Tribune*, 26 Nov. 2021, <https://sudantribune.com/article226409/>

Sudan New Agency, [Ministry of Health: Rumors and misinformation pose a challenge to the Ministry], *Sudan New Agency*, 13 Sep. 2020, <https://suna-sd.net/read?id=722533>

Sky Sudan, [Because of a "rumour", for the first time, the price of the dollar rose in Sudan], *Sky Sudan*, 11 Jan. 2022, <https://www.skysudan.net/21424/>

"Sudan Date of Elections", *Inter-Parliamentary Union*, archive.ipu.org/parline-e/reports/arc/SUDAN_1968_E.PDF. Accessed 20 Apr. 2022.

"Sudan reportedly blocks YouTube over electoral fraud video", *Sudan Tribune*, 22 Apr. 2010, <https://sudantribune.com/article34622/>

[Sudatel Telecom Group Company Data - Mubasher Information] *Mubasher*, www.mubasher.info/markets/ADX/stocks/SUDATEL/profile. Accessed 20 Apr. 2022.

[Sudan raises telecom taxes, increase in call and internet prices], *Al-Ain news*, 2 Jan. 2021, <https://al-ain.com/article/sudan-raises-value-added-tax-telecommunications>.

[Sudan Doctors Committee: 1,702 people have been killed and injured since the outbreak of the revolution, and the longest strike in the world has been lifted]" 2 July 2019, *Radio Dabanga*, <https://bit.ly/3xuUTO0>.

"Sudan Coup Death Toll Climbs to 42." *Radio Dabanga*, 25 Nov. 2021, www.dabangasudan.org/en/all-news/article/sudan-coup-death-toll-climbs-to-42.

"Sudan reportedly blocks YouTube over electoral fraud video", *Sudan Tribune*, 22 Apr. 2010, <https://sudantribune.com/article34622/>

Suliman, Mohamed. "The Case for Reforming the Sudanese Access to Information Act." *Global Voices*, 24 Aug. 2020, globalvoices.org/2019/08/28/the-case-for-reforming-the-sudanese-access-to-information-act.

Transparency International. "2014 Corruptions Perceptions Index" *Transparency.Org*, 22 Jan. 2022, www.transparency.org/en/cpi/2014.

"Zain Annual Report 2020." *Zain*, zain.com/AR2020/en/world-of-zain/africa. Accessed 20 Apr. 2022.

