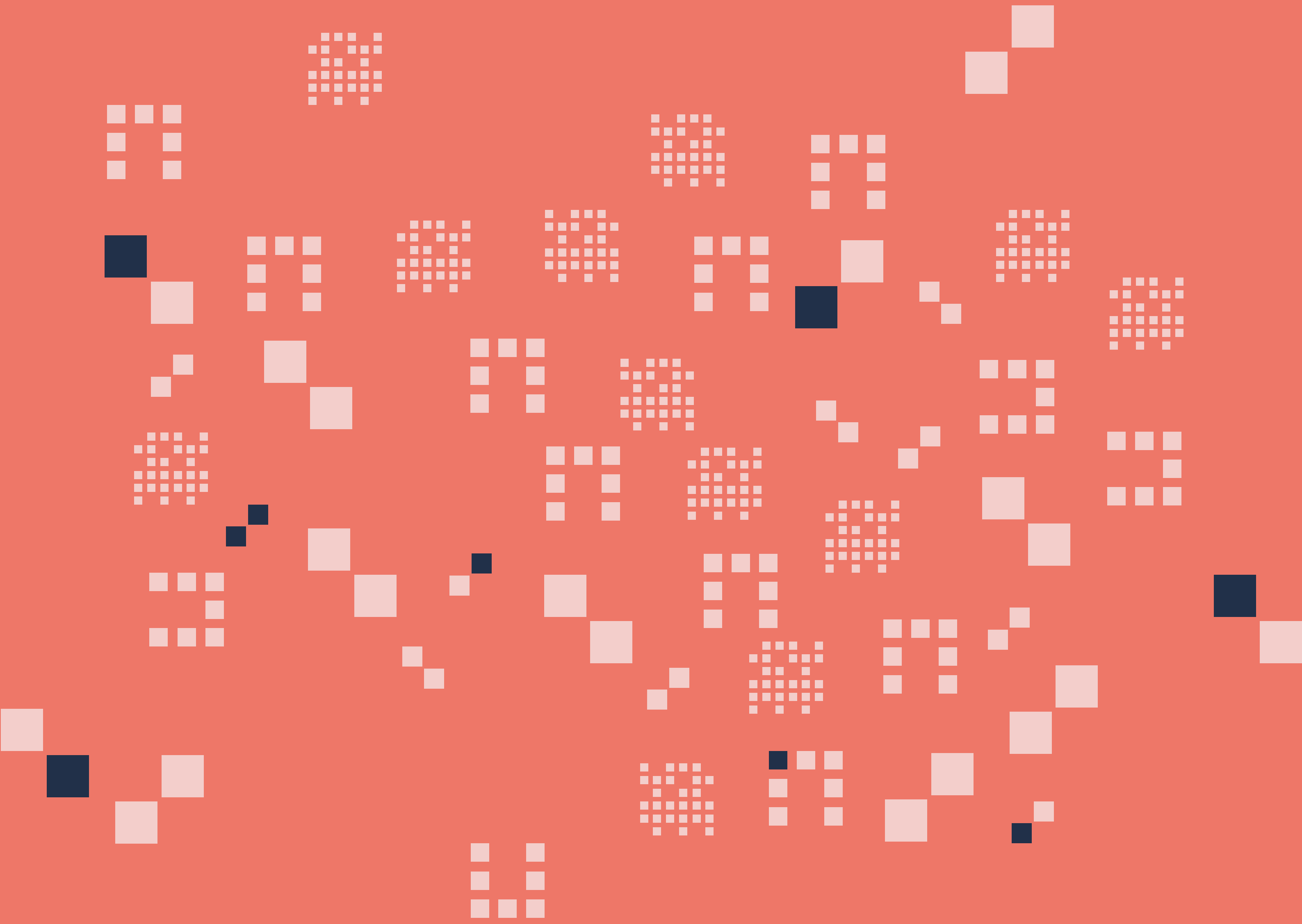
Evading accountability through internet shutdowns:

Trends in Africa and the Middle East



GLOBAL PARTNERS DIGITAL

accessnow

2023

Contents

ACKNOWLEDGMENTS

This report was authored by Jacqueline Rowe, Policy Lead at Global Partners Digital, with additional input from Felicia Anthonio, #KeepItOn Campaign Manager at Access Now and Bridget Andere, Africa Policy Analyst at Access Now. The author is especially grateful to Amelia Connor-Afflick, Research Assistant at Global Partners Digital for her support and contributions. This report was strengthened by feedback and insights from Saba Mah'derom, Board Member for Women of Tigray; Khattab Hamad, Researcher at Digital Rights Lab – Sudan; Qemal Affagnon, Regional Coordinator for West Africa, Internet Sans Frontieres; and Harold Adjaho, IT & Cybersecurity Consultant and President of The Internet Society's Benin Chapter.

The development of this report was made possible with support from Meta's Africa, Middle East and Turkey (AMET) regional team. Global Partners Digital and Access Now had full editorial independence on the content of the report.

SUMMARY

Governments around the world frequently use internet shutdowns (see Box 1 for definition) to disguise and evade accountability for grave human rights violations, including illegitimate grabs for power, state-sanctioned violence against peaceful protestors and even extra-judicial killings of political dissidents. This paper draws attention to key examples of this happening in recent years across Africa and the Middle East, and identifies common trends and factors driving the use of internet shutdowns in this way. The paper also makes recommendations for governments, the private sector, regulators and international human rights institutions as to how to call attention to and push back against this trend and ensure that victims of human rights abuses can properly call attention to their plight and access redress.

While internet shutdowns themselves constitute a violation of freedom of expression online regardless of context, this has been explored extensively elsewhere and is not the focus of this research paper.

METHODOLOGY

In terms of the international legal framework surrounding internet shutdowns, we base our analysis on international human rights law—primarily the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights, but also other core human rights treaties and instruments. International human rights law applies at all times and deals specifically with the obligations of states to respect, protect and fulfil human rights. Furthermore, we examine how internet shutdowns may also be used to cover violations of international humanitarian law, which applies during armed conflict and seeks to limit the effects of war by protecting people who are not participating in hostilities, and by restricting the means and methods of warfare. We rely, in our analysis, on the wealth of soft law guidance on internet shutdowns from the United Nations Office of the High Commissioner of Human Rights, which clearly states that blanket internet shutdowns violate international law and cannot be considered lawful or justified restrictions to the rights to freedom of expression or the rights to peaceful assembly in any circumstances.[1]

For this piece of research, we first used open-source data and public reports of internet shutdowns to investigate the frequency of internet shutdowns in the Africa and the Middle East regions in recent years. We then conducted a mapping of internet shutdowns in these regions in the last four years that have reportedly covered up governments' violations of the rights to assembly, to free and fair elections, to security and bodily integrity and to life. From this initial mapping of 54 incidents, five "case studies" were selected for more in-depth research based on their relevancy, recency and the severity of the human rights impacts that were covered up by the shutdown, as well as to ensure a variety of socio-political contexts would be covered through the case studies. These five incidents were investigated through desk-based research as well as consultation with local experts, who provided insight, feedback and additional issues for consideration as well as more nuanced information about the local regulatory frameworks governing each shutdown. The research paper draws upon existing data, desk research, the in-depth case studies and expert consultations to identify themes, trends, and potential routes forward for engagement and advocacy on this topic.

INTRODUCTION

Internet shutdowns are an increasingly common feature of global digital life. As internet connectivity rises around the world and more individuals than ever before are online, governments are increasingly weaponizing internet shutdowns to limit civic space and political freedoms in the digital world as well as the physical. The #KeepItOn coalition documented over 900 internet shutdowns in at least 76 countries globally between 2016 and 2021, and twelve countries shut down the internet more than ten times[2] during this period. Nearly half of these shutdowns occurred in a context of political turbulence,[3] and some lasted for weeks—or even months or years—severely impacting the day-to-day lives of millions of people.

India remains the world's leader in frequency of internet shutdowns, imposing over 600 shutdowns between 2016 and 2021. However, the Middle East and North Africa (MENA) and Sub-Saharan Africa (SSA) regions are also some of the worst hit by internet shutdowns. Of the 76 countries which experienced internet shutdowns between 2016 and 2021, 18 are in MENA[4] and 27 are from SSA. In total, 216 internet shutdowns were observed across these 45 countries during this period, constituting 23% of all internet shutdowns worldwide or 60% of all internet shutdowns worldwide excluding India (see Figures 1 and 2).[5] Internet shutdowns in the MENA and SSA regions have also increased in overall frequency since 2016 (see figure 2). In 2021 alone, nearly half of the countries in the MENA region and a quarter of the countries in the SSA region implemented some kind of shutdown, with Sudan and Iran shutting down the internet at least 5 times each.[6]

Box 1 **What is an internet shutdown?**

The term "internet shutdowns" encompasses a broad range of types of interference and limitations on people's communications and the technologies that underpin them. These can be achieved through a variety of methods and mechanisms, including by damaging or disabling fundamental infrastructure, interfering with routing information, manipulating domain name systems, implementing or mandating the use of filtering or deep-packet inspection (DPI) mechanisms, and throttling bandwidth speeds.[7]

The technical means through which each shutdown is implemented varies, depending on the nature of local telecommunications infrastructure, the degree of centralisation or government control over such infrastructure, and the impact that the shutdown is intended to achieve across a particular geographic area and range of communications services.[8] Some internet shutdown techniques are harder to detect or prove, or subject to weaker checks and balances or external scrutiny, making them more appealing to governments wishing to control communications without being detected or challenged.[9]

There are a number of different operational definitions of an internet shutdown, which serve different purposes for different groups.[10] In a recent paper on internet shutdowns, the Office of the High Commissioner for Human Rights defined them as:

> **"measures taken by a government, or on behalf of a government, to intentionally disrupt access to, and the use of, information and communications systems online."[11]**

For the purposes of this paper, we will use a slightly broader definition recently formulated by Access Now in their paper, The Taxonomy of a Shutdown:

> **"An interference with electronic systems primarily used for person-to-person communications, intended to render them inaccessible or effectively unusable, to exert control over the flow of information."[12]**

This definition better captures the varied and evolving techniques that are used to implement internet shutdowns, and also is not limited strictly to shutdowns imposed by governments. This allows for consideration of examples where non-state groups are imposing or implementing an internet shutdown, either during power grabs (e.g. through coup d'états) or as part of civil warfare (e.g. by damaging core telecommunications infrastructure). This definition includes content blocking of social media platforms—which are channels of communication in their own right—but not content blocking of websites like newspapers or NGOs.

PROPORTION OF GLOBAL SHUTDOWNS TAKING PLACE IN MENA AND SSA BETWEEN 2016 AND 2021

- ● Internet shutdowns in MENA region: 120
- ● Internet shutdowns in SSA region: 88
- ● Internet shutdowns in India: 567
- ● Internet shutdowns in other countries: 148

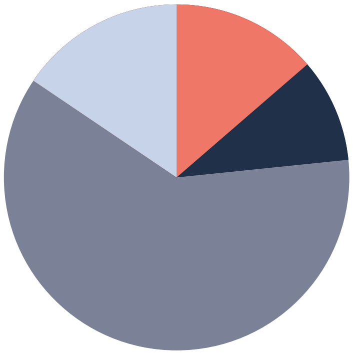


Figure 1 **Proportion of global shutdowns taking place in MENA and SSA between 2016 and 2021 (using Access Now STOP Data)**

PROPORTION OF GLOBAL SHUTDOWNS TAKING PLACE IN MENA AND SSA BETWEEN 2016 AND 2021 (EXCLUDING INDIA)

- ● Internet shutdowns in MENA region: 128
- ● Internet shutdowns in SSA region: 88
- ● Internet shutdowns in other countries: 148

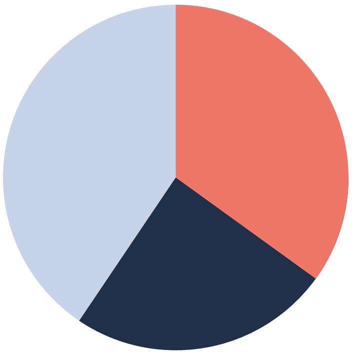


Figure 2 **Proportion of global shutdowns taking place in MENA and SSA between 2016 and 2021 (excluding India) (using Access Now STOP Data)**

INCREASE IN INCIDENTS OF INTERNET SHUTDOWNS IN MENA AND SSA BETWEEN 2016 AND 2021

Internet shutdowns in MENA region ▬ Internet shutdowns in SSA region ▬

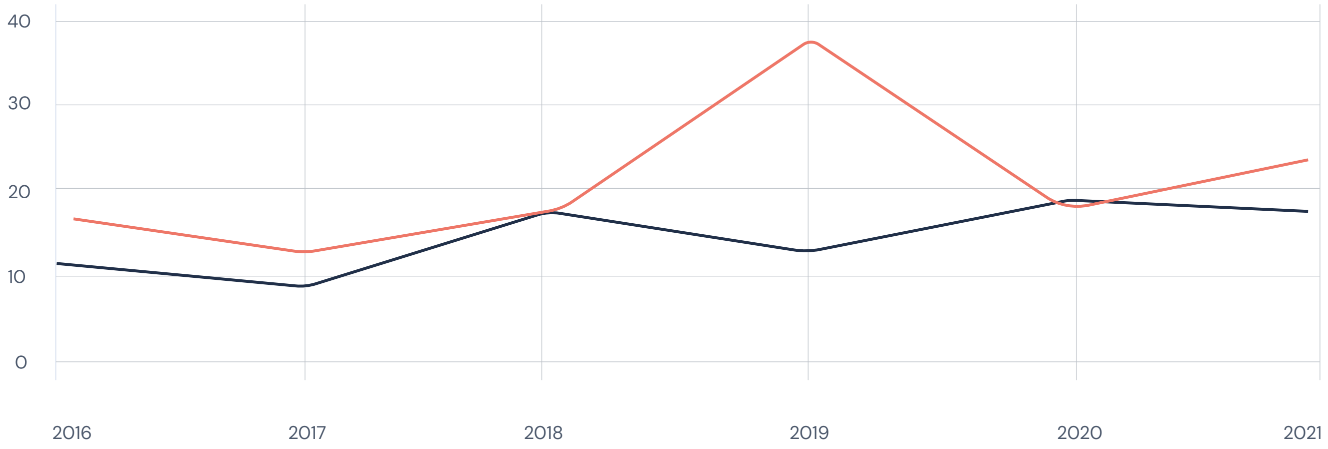


Figure 3 **Increase in incidents of internet shutdowns in MENA and SSA between 2016 and 2021 (using Access Now STOP Data).**

The human rights impacts of internet shutdowns are widely recognised. In preventing individuals from accessing the internet, internet shutdowns severely restrict freedom of expression and access to information, which in turn impacts other rights such as the rights to assembly and the right to participate in public affairs, including free and fair elections. Furthermore, internet shutdowns have negative impacts on individuals' economic, social and cultural rights. They disrupt work and livelihoods, preventing people from earning and trading as well as accessing or completing education and studies which rely on internet access. Shutdowns also prevent people from accessing healthcare and emergency services, and have adverse impacts on psychological wellbeing. They limit people's ability to organise and assemble around common causes, and place people's safety and well-being directly at risk—for example, when they make it impossible to warn people of impending danger. Many of these impacts are felt most keenly by already vulnerable or marginalised groups.[13]

This paper does not analyse the human rights impacts of internet shutdowns themselves or how international and regional human rights frameworks[14] apply to internet shutdowns, as these topics have been explored in detail elsewhere.[15] Instead, we focus on how governments in the MENA and SSA regions seem to be employing internet shutdowns as a tool for covering up and evading accountability for egregious offline human rights abuses, including distorting electoral processes, perpetrating violence against peaceful demonstrators and arresting or killing political dissidents. These human rights abuses may be experienced by all, not just those who are already online or using the internet for day-to-day life. Drawing on in-depth case studies from 2021 and 2022 in the MENA and SSA regions, this paper builds on existing research and efforts to draw attention to the severity of internet shutdowns in particular contexts, and to draw insights from recent examples to assist in current and future advocacy efforts.

In section 1, we explore how internet shutdowns have been implemented to cover up violations of political rights, violations of the integrity of the person,[16*] or violations of humanitarian law in conflict situations, providing details from case studies from Burkina Faso, Chad, Ethiopia, Iran and Sudan. In section 2 we explore common themes, trends and government narratives across these diverse cases, and in section 3 we highlight the work of advocates and activists working to push back against both human rights violations and internet shutdowns, and to seek accountability from authorities.

[*] We use this as an umbrella term to cover a range of human rights abuses that result from physically violent treatment, including arbitrary deprivation of life, disappearance, torture and inhuman or degrading treatment or punishment.

1. HOW HAVE INTERNET SHUTDOWNS BEEN USED TO DISGUISE HUMAN RIGHTS VIOLATIONS IN AFRICA AND THE MIDDLE EAST?

Internet shutdowns disguising violations of political rights

Between 2018 and 2022, at least 48 documented internet shutdowns in Africa and the Middle East occurred alongside violations of individuals' rights to assembly[17] and/or their rights to participate in political and public life, including through free and fair elections.[18] In about half of these incidents, the shutdown lasted less than three days, imposed as short term restrictions to quell protests or to stop the spread of disinformation or restrict information sharing during electoral periods. Recent examples include the August 2022 shutdown in Somalia's self-declared Republic of Somaliland, which was imposed in response to demonstrations that protested the postponement of the presidential election[19]; Uganda's suspension of internet services nationwide in January 2021 on the eve of its general elections[20]; and Jordan's throttling of internet access and Facebook Live services in August 2020[21] and March 2021[22] in response to protests about teachers' pay and COVID-19 restrictions.

Below, we explore two cases of internet shutdowns implemented in contexts of electoral interference and manipulation of political processes in greater detail: the 2022 shutdown after a coup d'etat in Burkina Faso, and the 2021 shutdown in Chad coinciding with violence towards and arrest of an opposition politician.

CASE STUDY 01

Burkina Faso's January 2022 shutdown

In some instances, an internet shutdown is implemented in order to disguise or conceal the occurrence of a coup d'état, or to confuse narratives around a grab for power by non-state authorities. This was the case in Burkina Faso after a military coup d'état in January 2022.

Tensions had been rising for some time over the perceived failure of President Kaboré's government to address rising attacks from Islamist militants in the North of Burkina Faso since 2016. In the weeks and months before the coup d'état, the government had already shut down the internet twice—first for several days in November 2021 to quell anti-government protests in the north of the country, and second in early

January 2022 in response to a suspected coup plot, where Facebook and WhatsApp were also blocked. On 23 January 2022, military officer Paul-Henri Damiba led a coup against President Kaboré, detaining and then deposing him from his post. Damiba's forces announced that the parliament, government and constitution had been dissolved, closing national borders and establishing nationwide overnight curfews. They also imposed an internet shutdown, slowing internet traffic to 12.5% of normal levels with leading internet service providers Orange, FasoNet and Telecel Faso most heavily disrupted.[23] This internet disruption continued for approximately 35 hours, and soldiers also surrounded and took control of the state broadcaster *Radio Télévision du Burkina*, further impeding citizens' access to information about the developments. No official statement was made regarding the decision to cut internet access, but at the end of January the military junta restored the constitution and appointed Damiba, the leader of the coup, as interim president and head of the new Patriotic Movement for Safeguarding and Restoration (MPSR).[24]

Public reaction to the coup was mixed. Pro-military groups celebrated the end of Kaboré's regime and thousands marched in support of Damiba serving as interim president.[25] However, many citizens and members of the international community denounced the coup and Economic Community for West African States (ECOWAS) and the African Union suspended Burkina Faso's membership. Just eight months later, Damiba was deposed by a second coup, led by another military leader named Traoré, on 30 September 2022. While television channels were cut during this event, no nationwide internet disruption was observed.

Regardless of whether Damiba enjoyed popular support at the time, the January 2022 coup constituted a severe violation of Burkinabés' rights to free and fair elections. The internet disruption was implemented at a pivotal time during the coup, when power was being consolidated by the military junta and citizens were left in the dark and unable to organise to protest or to defend their political rights. Furthermore, the continued political instability after the power grab has eroded confidence in national institutions, with long-term implications for international investment.[26]

CASE STUDY 02

Chad's February 2021 internet shutdown

Chad's February 2021 shutdown, imposed shortly after security forces sought to arrest an opposition leader at his home, illustrates how authoritarian governments use internet shutdowns to evade accountability for oppression or violence towards political rivals, particularly in the lead up to electoral periods.

Former President of Chad Idriss Déby ruled from 1990 to 2021. Despite establishing a system of multi-party rule in 1992, Déby increasingly ruled in an authoritarian fashion. His electoral victories were disputed by domestic and international observers,[27] and opposition leaders who publicly criticised the government were frequently harassed and arrested by government forces.[28] He attempted to change the Chadian constitution in 2018 to allow himself to stay in power until 2033, and in his last few years in power he increasingly used internet shutdowns to control the flow of information and suppress protests. The most lengthy and disruptive shutdowns took place in 2016,[29] 2018[30] and 2020.[31]

The January 2021 shutdown took place against continued protests against Déby's rule and against his standing in the April 2021 elections. Yaya Dillo, the leader of the opposition and a longstanding critic and opponent of Déby's rule, was influential in organising these campaigns. On the morning of Sunday 28 February 2021, members of the Presidential Guard went to Yaya Dillo's home, supposedly with a warrant for his arrest in relation to a defamation case,[32] and killed at least two members of his family. Reports of what occurred at Dillo's house are disputed, but a video of the incident posted to Twitter showed a military tank advancing on a house as a crowd of individuals threw objects at it.[33] Shortly after this incident, national network connectivity dropped to less than half of ordinary levels for more than 6 days.[34]

The timing of the internet shutdown served to cover up evidence and information about the disproportionate use of force, which likely implicated violations of the right to life, the right to liberty and security of person, and the right to due process in a court of law. The shutdown also severely limited Chadians' ability to organise and mobilise protests against this incident quickly and effectively, violating their right to peaceful assembly and following the previous pattern by the government of imposing internet shutdowns to evade accountability and suppress political criticism.[35] A Chadian observer also noted that the shutdown impeded the work of human rights defenders to corroborate reports and raise awareness of the incident, created obstacles to democratic processes and contributed to the erosion of trust in the government.

The period after this incident and the accompanying shutdown was indeed characterised by extreme political instability and governmental distrust, with a controversial election in April 2021, the death of President Déby during conflict with the Front for Change and Concord in Chad (FACT) military group, and the appointment of Mahamat Déby (Idriss Déby's son) as head of a Transitional Military Council (TMC) in place of the elected government and national assembly.[36] More recently, Mahamat Déby has adopted resolutions extending his rule by a further two years and allowing himself to stand in the next elections, prompting widespread dissent and protests by Chadians and concern from the international community.[37]

These cases demonstrate the severe information disorder that is introduced by the implementation of an internet shutdown to disguise or conceal interference with electoral processes or political rivals.

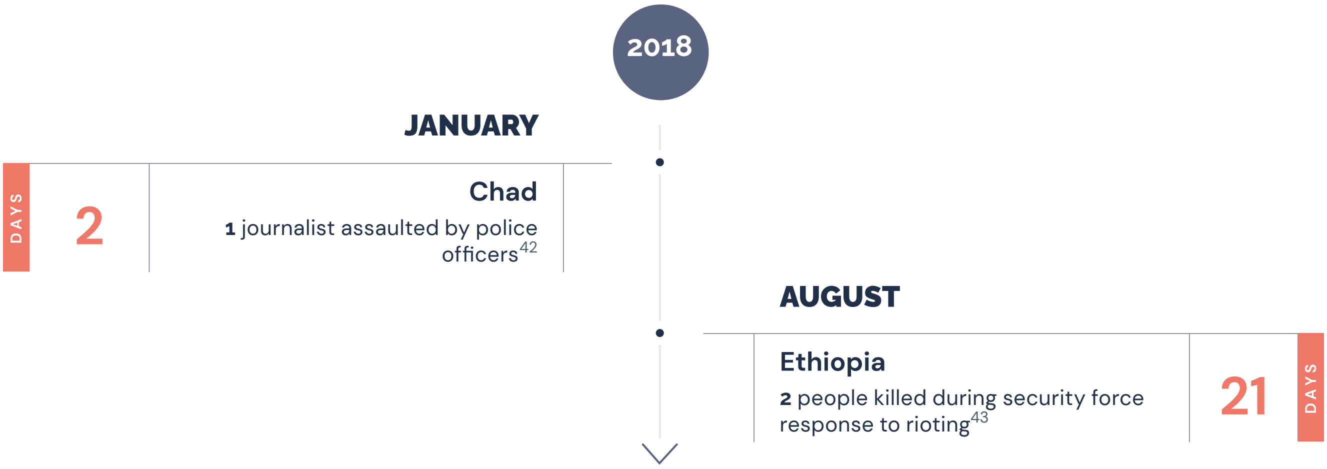
Shutting down the internet at these key moments also prevents citizens from calling on the international community to support them, or to place pressure on the government or leaders of the coup to uphold relevant human rights standards. Open and democratic political discourse is essential for healthy and stable societies, and the silencing of political criticism and dissent erodes authorities' accountability to citizens.

Internet shutdowns disguising violations of the integrity of the person[38]*

Many internet shutdowns in Africa and the Middle East have been imposed shortly before, during or shortly after incidents of state violence against protestors or particular groups of citizens. These incidents include wrongful or arbitrary arrests of critics or dissidents or violence by law enforcement against peaceful protestors, which can result in violations of the rights to liberty and security of person,[39] of the right to freedom from torture and degrading treatment,[40] and even—in the most egregious cases—of the right to life.[41] By preventing information about or documentation of these incidents from being freely shared online both within and outside of national borders, governments can make it incredibly difficult for victims to seek justice and for perpetrators to be held to account.

Between 2018 and 2022, at least 29 documented internet shutdowns in Africa and the Middle East occurred alongside some form of state violence against citizens, including police brutality, extra-judicial arrests and killings by security forces.. These took place across 12 countries, often the result of escalations of protests or electoral information disorder, with a median duration of six days. These incidents are illustrated in the timeline below:

TIMELINE OF INTERNET SHUTDOWNS IN THE MENA AND SSA REGIONS SINCE 2018 THAT HAVE TAKEN PLACE ALONGSIDE STATE VIOLATIONS OF THE INTEGRITY OF THE PERSON



2018

JANUARY

DAYS 2

Chad

1 journalist assaulted by police officers[42]

AUGUST

Ethiopia

2 people killed during security force response to rioting[43]

21 DAYS

* We use this as an umbrella term to cover a range of human rights abuses that result from physically violent treatment, including arbitrary deprivation of life, disappearance, torture and inhuman or degrading treatment or punishment.

DECEMBER

Sudan

8 protestors killed by security forces[44]

68 DAYS

2019

JANUARY

Zimbabwe

12 dead, **>300** injured, **>600** arrested[45]

6 DAYS

APRIL

Benin

Several protestors killed by security forces[46]

1 DAYS

JUNE

Ethiopia

1 dead and several injured[47]

5 DAYS

Sudan

>100 protestors killed by security forces in the "Khartoum massacre"[48]

30 DAYS

Mauritania

Arbitrary arrests and police brutality towards protestors[49]

8 DAYS

JULY

Iraq

Security forces killed at least **30** protestors and injured hundreds[50]

2 DAYS

OCTOBER

Iraq

>20 protestors killed and **>600** injured[51]

6 DAYS

NOVEMBER

Iraq

6 protestors killed and **38** injured[52]

7 DAYS

Iran

323-1500 protestors killed by security forces[53]

11 DAYS

2020

JANUARY

Ethiopia

Reports of **dozens** of civilians killed by security forces[54]

~90 DAYS

JUNE

DAYS 23

Ethiopia

155 civilians and **11** security forces dead, **167** injured and over **1,000** arrested[55]

JULY

Mali

11 killed, **140** injured and dozens arrested[56]

5 DAYS

JULY - AUGUST

DAYS 60

Chad

1 dead and 1 injured after altercation with police officer[57]

OCTOBER

Tanzania

9 killed by security forces[58]

3 DAYS

NOVEMBER

ONGOING

Ethiopia

Thousands displaced, victims of sexual violence, physical abuse and extra-judicial killings by state and rebel armed forces[59]

2021

FEBRUARY

Chad

2 killed and five wounded[60]

1 DAYS

Iran

>10 civilians killed by security forces"[61]

3 DAYS

Niger

470 protestors arrested and at least **2** dead[62]

10 DAYS

OCTOBER

DAYS 1

Eswatini

2 protestors injured by security forces[63]

DAYS 30

Sudan

17 people killed and over **250** injured[64]

NOVEMBER

Burkina Faso

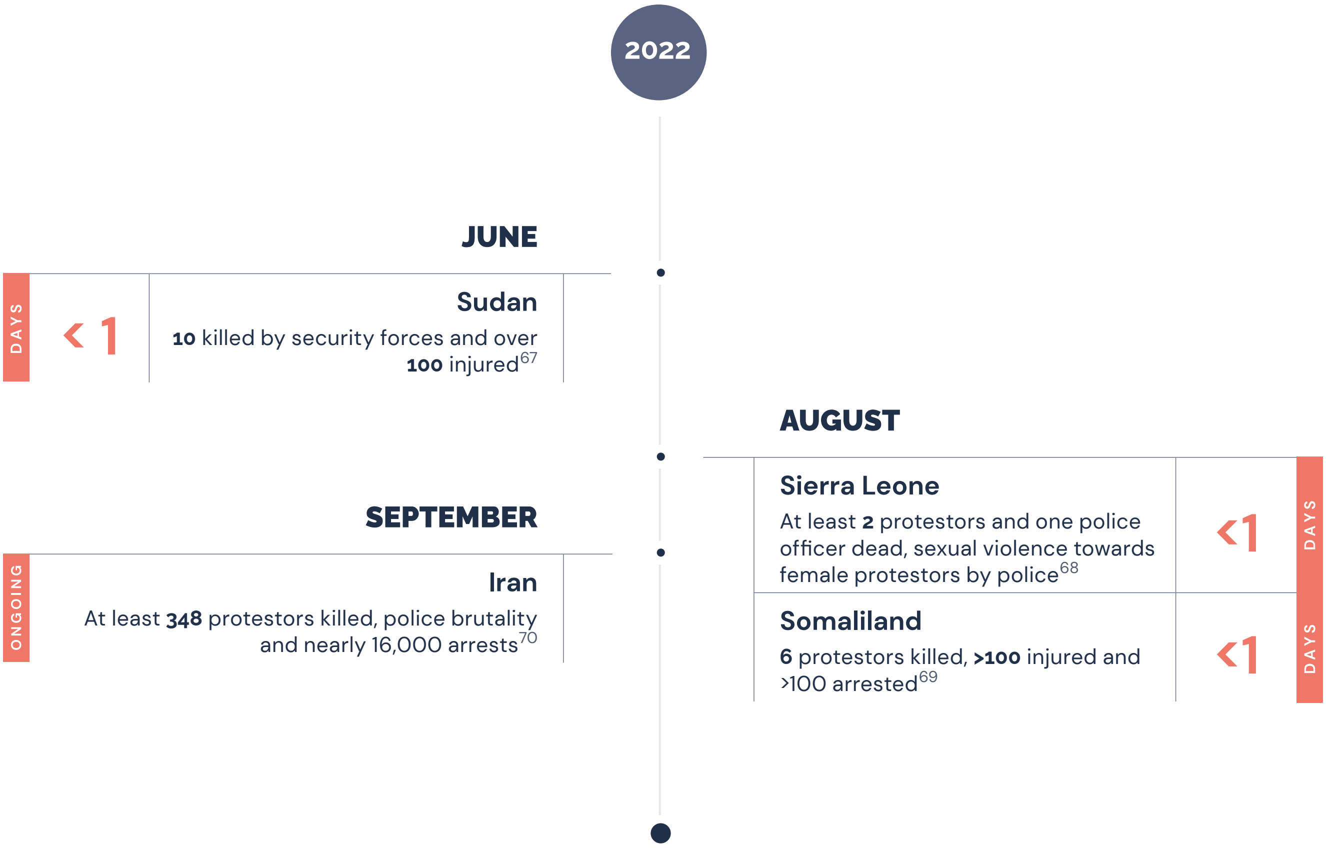
3 protestors injured by French security forces[65]

8 DAYS

Iran

Police brutality[66]

2 DAYS



2022

JUNE

DAYS <1

Sudan

10 killed by security forces and over **100** injured[67]

AUGUST

Sierra Leone

At least **2** protestors and one police officer dead, sexual violence towards female protestors by police[68]

<1 DAYS

Somaliland

6 protestors killed, **>100** injured and >100 arrested[69]

<1 DAYS

SEPTEMBER

ONGOING

Iran

At least **348** protestors killed, police brutality and nearly 16,000 arrests[70]

To explore two recent examples in more depth, we conducted a "deep-dive" into the circumstances leading up to the internet shutdowns in Sudan in October 2021 and Iran in September 2022. In both of these examples, internet shutdowns have obscured violence and made it difficult to hold government forces accountable for abuse and killings of peaceful protestors, including children.

CASE STUDY 03

Sudan's October 2021 shutdown

Sudan has a long history of using internet shutdowns to cover up instances of state violence under former dictator Omar Al-Bashir. For example, he imposed a nationwide internet shutdown in September 2013 to cover up arrests of over 700 people and the extrajudicial killing of dozens of individuals.[71] Even after Al-Bashir had been ousted by a military coup in April 2019, the Transitional Military Council (TMC)—headed by the Inspector of the Armed Forces General Abdel Fattah al-Burhan—continued to deploy the same strategy, most famously in the aftermath of the tragic Khartoum massacre in June 2019. The military forces of the TMC opened fire on pro-democracy protesters and killed over 100 people, and mobile internet from providers MTN, Zain, Kanartel and Sudatel were subsequently cut, resulting in a near-total internet blackout for over one month.[72]

After the Khartoum Massacre, the TMC and the Forces of Freedom and Change (FFC) coalition agreed on the formation of a transitional "Sovereignty Council" that would lead the country to the next elections instead of the TMC, and appointed a new Prime Minister, Abdalla Hamdok. However, two years later, on 24 October 2021—following a period of rising tensions between pro-military and pro-democracy groups—military forces arrested Prime Minister Abdalla Hamdok and other senior government figures, declared a state of emergency and announced the dissolution of the government and the Sovereignty Council. These actions were declared to be illegal and unconstitutional by the FFC, government ministries, industry bodies and international bodies.[73] The military also implemented a near total internet blackout, even shutting down phone and SMS services for two days ahead of a nationwide pro-democracy march planned for 30 October.[74] The Khartoum Court ordered the country's three primary telecommunications providers to restore internet access across Sudan on 11 November 2021 following a lawsuit by the Sudanese Society for Consumer Protection (SSCP), but the next day the Telecommunications and Post Regulatory Authority ordered the shutdown to remain in place in the interests of national security.[75] Eventually, internet access returned on 18 November after 25 days of blackout, with Zain and MTN the first to come back online followed by Sudatel and later by other providers.[76]

During this blackout, many protesters took to the streets to protest both the military coup and the internet shutdown, which constituted a grave violation of individuals' rights to political participation through free and fair elections. Security forces responded with violence, and over 100 people were killed—including at least 18 children according to the Sudanese Doctors Committee.[77] As well as severely limiting individuals' ability to protest, therefore, the shutdown also served to obscure violations of the right to life and the right to liberty and security of person. One researcher highlighted that emergency healthcare service lines were also impacted by the blackout, impeding access to emergency services for those requiring medical assistance and disrupting the operations and communications of humanitarian organisations.

The military junta has continued to use sporadic internet disruptions to curb or limit protests since the October 2021 coup; yet local researchers have noted that the deployment of these shutdown tactics displays considerable political bias. For example, while shutdowns were deployed to quell pro-democracy protests throughout December 2021 and January 2022 and around anniversary marches in June and October 2022, when the pro-military group "Sudan People's Appeal Initiative" protested in front of the UN buildings in Khartoum in June 2022 against what they perceived to be UN interference with Sudanese domestic affairs, the military did not shut down the internet.[78] This would suggest that military leaders are strategically using internet shutdowns to further their own interests, rather than as a genuine attempt to protect national security.

CASE STUDY 04

Iran’s ongoing internet shutdown

Iranian authorities have been tightening their grip on internet communications and critical telecommunications infrastructure for many years through legislative and policy measures,[79] including through the establishment of the Supreme Council of Cyberspace (SCC) and the development of the National Information Network (NIN)—a domestic and state-controlled intranet which includes a domestic video sharing platform, search engine, messaging app,[80] email service and e-commerce apps—and by shutting down the internet during periods of protest or dissent. Previous examples of this include the nationwide shutdown implemented on 16 November 2019 in response to protests against fuel prices, during which security forces killed at least 300 people,[81] and the regional shutdown in Sistan and Baluchistan Province in February 2021 in response to protests over the deaths of 10 people at the hands of security forces.[82]

The most recent internet shutdown began in September 2022. On 19 September an Iranian woman named Mahsa Jina Amini was arrested and killed by police wearing her hijab “improperly”, stoking longstanding frustration around the government’s restrictive treatment of women, state violence and authoritarian rule.[83] Protests erupted around the country,[84] and in response the government ruthlessly cracked down on demonstrators, with security forces violently arresting and using indiscriminate force and live rounds against protesters.[85] During this period, while essential digital services remained largely available on the NIN, authorities severely disrupted internet services through a range of sophisticated techniques:

- **Imposing curfews on mobile network operators** (including Iran Mobile Communications Company (MCI), Rightel, IranCell and Mobinnet);
- Implementing **regional internet shutdowns and restrictions**, for example in Kordestan and Khuzestan provinces and in Sistan-Baluchistan;
- Blocking **protocols** used for transferring web data securely;
- Blocking **encrypted Domain Name Systems (DNS)**;
- Blocking the last remaining **social media platforms** available in Iran, including Instagram, WhatsApp, LinkedIn and Skype; and
- Blocking **app stores** (and also limiting app store downloads of VPNs)[86]

The complexity, precision and rapidity of these aggressive disruptions is largely unprecedented,[87] reportedly supported by a system called SIAM which allows authorities to remotely manipulate individual cellular connections, including throttling them or disconnecting them entirely, and to force them onto 2G networks which are more vulnerable to data hacking.[88] The internet shutdowns made it far harder for Iranians to share evidence of and protest against police brutality and to mobilise peacefully and safely.[89] It also forced more Iranians to rely more on the less secure internet services run on the NIN—such as Iran's "super-app" Rubika or its domestic version of YouTube, Aparat—which are also prone to government interference and surveillance.[90] While the nightly curfews on mobile network operators ceased in mid-October, several of the other restrictions remained in place for some time, and app stores and social media platforms remain blocked as of January 2023.[91]

The mistreatment and killing of Mahsa Jina Amini in itself constitutes a grave violation of her right to liberty and security of person, right to freedom from torture and degrading treatment, right to a fair trial and right to life. Security forces have also committed grave human rights violations in response to the largely peaceful nationwide protests triggered by Amini's death. As of 16 November 2022, at least 358 protestors (including 29 children) had been killed by security forces, while authorities reportedly attempted to cover up many of the causes of their deaths by swearing their families to secrecy and pressuring medical professionals to falsify death certificates.[92] Nearly 16,000 protestors have been arrested, and some have already been sentenced to death and publicly executed.[93] Amnesty International has also documented extensive evidence of torture, ill-treatment and sexual violence against protestors by security forces.[94] Iran's actions were widely condemned by the international community as violating its international human rights commitments, with many governments and coalitions calling on the authorities to end the violence and restore full internet access.[95]

Internet shutdowns disguising violations of international humanitarian law

Internet shutdowns have also been observed in regions experiencing civil war and internal conflict in Africa and the Middle East in recent years. In Palestine, for example, Israeli forces have deliberately targeted internet and communications networks in the Gaza strip in order to restrict Palestinians' connectivity,[96] and in Yemen there is evidence of Saudi- and UAE-led airstrikes targeting core telecommunication infrastructure in Hodeidah.[97] Internet shutdowns are justified by state forces as necessary to limit the capacity of rebels or militia to organise and to fight. However, reports indicate that, in reality, internet shutdowns during periods of conflict may have covered up grave violations of human rights and of international humanitarian law, including serious war crimes perpetrated by parties to the conflict on civilians.

CASE STUDY 05

Ethiopia's ongoing shutdown

The ongoing internet and telecommunications shutdown in the Tigray region of Ethiopia is one of the longest and most severe shutdowns that has ever been recorded, with some areas of the region having had no internet access for over two years.

On 3 and 4 November 2020, armed forces loyal to the Tigrayan People's Liberation Front allegedly attacked government bases in the Tigray region. In response, the federal government issued a state of emergency, suspended all government services, and deployed regional and national military forces along with the Eritrean Defence Force (EDF).[98] From 01:00 am local time on 4 November 2020, internet and telecommunications services for the Tigrayan region—including broadband, mobile internet and phone lines—were cut off,[99] resulting in a near total communications blackout. Some of these services were restored in parts of Tigray in the following weeks and months;[100] but frequent electricity cuts also prevented even those with intermittent signal or internet access from communicating outside of Tigray.[101] In June 2021, as the Tigrayan Defence Force (TDF) retook large areas of Tigray and the Ethiopian National Defence Forces (ENDF) were forced to retreat, the federal government again disconnected telecommunications and electricity infrastructure, and since then internet and communications access has continued to be sporadic or non-existent.[102]

Despite its tight control over internet and telecommunications infrastructure, [103] the federal government has repeatedly denied responsibility for these shutdowns, claiming that the disruption is due to cyber attacks or due to Tigray forces damaging core telecommunications infrastructure such as power sources or fibre optic cables.[104] International investigations, however, have indicated that it was in fact the Federal government which suspended internet and telecommunications services in November 2020 and June 2021, and sought to suppress communications about the conflict through other means as well.[105] A peace agreement was made between the federal government and the TPLF in November 2022, and authorities have begun to make efforts to restore access to telecommunications and other essential services throughout the Tigray region; but progress is slow, and internet access remains sporadic and limited for many in the region.[106]

The internet shutdown has had a multifaceted and devastating effect on the civilian population. An Ethiopian correspondent described the "layered" impacts of the shutdown as follows:

1. Crippling existing community systems, including education, healthcare, business, banking and other systems critical for everyday life;

2. Depriving individuals from the opportunity to prevent, monitor, report, corroborate or initiate responses to reported atrocities, making it nearly impossible for victims to seek accountability and allowing those with mandates and power to respond to remain silent;
3. Facilitating the weaponization of misinformation, disinformation and propaganda, including extremist narratives and hate speech targeting the Tigrayan population which incited further violence;
4. Eroding social connections both within Tigray, and between Tigray and the rest of the country and the world, making it harder to raise awareness of the state of affairs in the region among international journalists, investigators, the diplomatic community, and the international community.

> **"We would hear about atrocities but we could not amplify it because we could not corroborate. It was impossible to get timely information."** ~ Ethiopian human rights defender.

Through in-depth investigations with the Ethiopian Human Rights Commission published in November 2021 and September 2022, the United Nations Office of the High Commissioner for Human Rights has found evidence that all sides to the conflict have perpetrated grave violations of international law, including extrajudicial killings and executions, torture, arbitrary detention, destruction of property, "staggering" levels of sexual and gender-based violence, and forcible displacement of civilians.[107] These incidents constitute severe violations of the right to life and right to freedom from torture and degrading treatment, and some constitute violations of international humanitarian law governing non-international conflicts. UN investigators also found reasonable grounds to believe that some of these incidents were severe enough to constitute crimes against humanity and war crimes under international law.[108] The destruction of essential infrastructure and services has also dramatically increased food insecurity and disrupted the work of emergency humanitarian services, posing further human rights risks to civilians caught up in the conflict. [109]

2. IN WHAT CONTEXTS ARE GOVERNMENTS MOST LIKELY TO SHUT DOWN THE INTERNET TO COVER UP HUMAN RIGHTS ABUSES?

It is clear that a government which is actively committing or condoning human rights violations is less likely to be concerned as to whether or not citizens have access to the internet, and therefore such governments are more likely to shut down the internet to evade accountability. However, beyond this basic correlation, our research indicates that there are a number of additional factors which increase the likelihood of a government using an internet shutdown to cover up its human rights abuses.

Factor 1: History of state control over information ecosystems

Many of the governments which choose to implement internet shutdowns see them as a logical continuation of a longstanding history of state control over press, journalism, and civic spaces in general. Countries with autocratic or long-serving governments, who have continually manipulated the flow of information in their favour even before internet technologies were widely adopted by their populations, have been found to be more likely to shut down the internet.[110] These circumstances tend to coincide with minimal checks and balances and weak rule of law, meaning that technologies which are generally deployed proportionately by democratic governments are more likely to be misused in these states for the purposes of disrupting or interfering with internet communications. This is clearly observed in the case of deep-packet inspection technology, used by many democratic states for the purposes of detecting child abuse alongside multiple checks and balances, but increasingly deployed by authoritarian states to prevent users from accessing certain sites and internet services which host dissenting or critical political speech. [111]

Factor 2: An enabling regulatory environment

Many countries in the Middle East and Africa regions have passed laws or regulations which provide “legal” means of shutting down the internet or taking over telecommunications platforms in the interests of national security or public order, or to fight terrorist, cybercrime or hate speech.[112] Examples from the MENA and SSA regions include Egypt’s 2003 Telecommunications Regulation Law;[113] The Democratic Republic of Congo’s 2002 Telecommunications Framework Law;[114] and Turkey’s 2014 Regulation on Information and Communication Technologies. [115] Governments also sometimes claim a legal basis even where one is not clear; for example, Ethiopian authorities have claimed that the 2013 Law Re-establishing the Information Network Security Agency provides the Agency with the power to cut internet access for national security purposes, even though this is not stated anywhere in the law.[116]

Box 2 **The International Telecommunications Union**

Some states have argued that Articles 34 and 35 of the Constitution of the International Telecommunication Union (ITU) provide a legal basis for internet shutdowns, as these articles permit states to cut off telecommunications services where they “may appear dangerous to the security of the State or contrary to its laws”. [117]

The UN Special Rapporteur on the Rights to Assembly and Association has stated that interpreting these provisions of the ITU Constitution (which predates internet communications) as permitting internet shutdowns contravenes human rights norms and standards, as well as the ITU's own values and commitments. The Special Rapporteur has further called upon the ITU to issue guidance clarifying that "these provisions should never be understood as authorising internet shutdowns." [118]

Factor 3: An enabling infrastructural environment

It is easier for a state to impose an internet shutdown where a greater proportion of the core infrastructure which underpins internet technologies is already under the state's control. Many governments in the MENA and SSA regions have sought to centralise fundamental telecommunications infrastructure and expand their control over private telecommunications companies. For example, in Ethiopia the state-controlled Ethio telecom was historically the sole access provider in the country, only recently joined by Safaricom.[119] And, while Iran did decentralise its control over national internet gateways after 2019,[120] it retains an incredibly tight grip on the practices of internet service providers through a multiplicity of other measures, such as through the SIAM system (see Case Study 4). This highly sophisticated and granular level of control over internet access is unprecedented.

Box 3 **The complex role of telecommunications companies**

The focus of this research paper is on how *states* are using internet shutdowns to cover up human rights abuses. Yet telecommunications companies play a complex role in enabling such government-mandated shutdowns to take place. Under the UN Guiding Principles on business and human rights (UNGPs), private entities are required to respect human rights and to conduct due diligence around the human rights impacts of their operations and business decisions, and shutting down internet services clearly runs contradictory to these responsibilities. However, companies are also subject to local laws and contractual obligations, and in many cases governments have threatened to close operations or arrest telecommunications company staff if the company does not comply with shutdown orders.[121]

Many telecommunications companies maintain close relationships with authoritarian governments in order to facilitate smoother business operations. For example, many members of the boards of directors of such companies in authoritarian developing countries are wealthy elites who themselves have benefited from the incumbent regime.[122] There may be little appetite or motivation, therefore, for such companies to oppose or push back on government demands, even where customers or international shareholders are demanding more accountability.[123]

While telecommunications companies and their shareholders are not responsible for a government's authoritarian practices and cannot be expected to solve existing human rights issues beyond their business operations, they can take steps to improve their human rights due diligence around internet shutdowns and to be more transparent when such incidents do occur. Telecommunications companies can, and should:

- Require governments to provide legal justifications for authorisation of a particular shutdown;
- Publish correspondence wherever possible and be transparent about actions taken in response to government demands;
- Work in coalitions to challenge and push back against shutdown restrictions. [124]

Perhaps the most detailed guidance and framework for how telecommunications companies should respond to shutdown requests in accordance with human rights principles has been developed by the Global Network Initiative (GNI). The GNI Principles include commitments for telecommunications companies relating to freedom of expression and privacy, responsible company decisionmaking, multi-stakeholder collaboration and governance, accountability and transparency. These are accompanied by extensive Implementation Guidelines, which detail how companies should balance risks to staff members against human rights concerns and what human rights due diligence processes should be in place to manage internet shutdown requests. GNI member companies are assessed regularly for their consistent implementation of these principles with improvements over time.

Factor 4: An existing history of internet shutdowns

States which have already shut down the internet several times are more likely to do so again. Only three of the 25 countries in the MENA and SSA regions that shut down the internet in 2016 have not shut it down for a second time since the 2016 incident.[125] Discussing a spate of recent internet shutdowns in Burkina Faso, Felicia Anthonio of Access Now pointed out that "once a government flips the kill switch, they gain the confidence to do it again".[126] The history of internet shutdowns also does not seem to be tied to an individual leader or political party, as even leaders who have taken over after long-standing heads of state are ousted or overthrown have continued to shut down the internet, including Buhari in Nigeria, Ahmed in Ethiopia, Sall in Senegal and Al-Sisi in Egypt.[127] This would indicate that temptation to shut down the internet based on precedent is grounded institutional and infrastructural factors, as well as perhaps a perceived lack of consequences for previous internet shutdowns.

Factor 5: Political instability or conflict

Political instability and conflict tend to coincide with internet shutdowns in the MENA and SSA regions. The recent UN report on internet shutdowns stated that:

> **“Almost half of all shutdowns recorded by civil society groups between 2016 and 2021 were carried out in the context of protests and political crisis, with 225 shutdowns recorded during public demonstrations.”[128]**

In extreme cases, where a non-state group is making a grab for power through a coup d’état, states of emergency are common and rule of law is jeopardised. In Burkina Faso, both internet access and radio channels were cut for nearly two days after the coup against President Kaboré, when military leader Paul Henri-Damiba dissolved the country’s parliament, government and constitution, closed national borders and imposed nationwide overnight curfews. Amid such extreme information disorder and contestation of legitimacy, and where democratic principles have already been firmly violated, an internet shutdown may be particularly appealing for emerging political leaders hoping to quickly consolidate their power and suppress dissent.

Non-factors

It is also worth noting a few circumstances which, while seeming likely to discourage the use of internet shutdowns, do not appear at present to be having this effect (bearing in mind that it is difficult to measure what would or could have taken place had these circumstances not been at play).

First, despite a wealth of guidance at the international and regional level articulating why internet shutdowns violate human rights and are impermissible under international human rights law, states which have ratified core human rights treaties continue to utilise internet shutdowns at will. This is either because the link between internet access and enjoyment of human rights is still not well understood, or because it is well understood but continually disregarded by governments.

Second, despite the lack of evidence to support the claim that internet shutdowns are effective in curbing protests or preventing riots, violence or the spread of misinformation, governments continue to implement them in the interests of “public safety” and “national security”. While it may indeed become more difficult to organise mass protests without internet access, demonstrators are often able to find ways around the shutdown. Indeed, a shutdown may, paradoxically, have the effect of forcing more people into the streets in order to exchange information or have their voices heard. In Sudan, for example, despite the prolonged internet shutdown in 2019, protesters continued to demonstrate peacefully in the streets; and in some cases internet disruptions have been shown to precede escalations in violence when people become frustrated with prolonged information disorder and/or believe that they can act with impunity.[129] Either governments are unaware of the potential risks of inciting violence when ordering an internet shutdown, or they are aware but continue to use narratives of national security and reducing violence as an excuse.

Third, as internet connectivity rates increase, so too do the costs of implementing shutdowns, because a greater proportion of GDP generation relies on internet technologies.[130] However, many wealthier governments are increasingly able to circumvent this through more sophisticated and complex shutdown techniques (see Factor 4: an enabling infrastructural environment). For governments without the resources for such infrastructure, connectivity rates are generally lower and therefore the cost of implementing a shutdown is less prohibitive in the first place.

3. HOW CAN CIVIL SOCIETY, GOVERNMENTS AND INTERNATIONAL ORGANISATIONS BEST ADVOCATE AGAINST INTERNET SHUTDOWNS IN AFRICA AND THE MIDDLE EAST?

There are a great many tools and initiatives to mitigate internet shutdowns and to help users to regain access or circumvent restrictions where possible. These have been explored in detail elsewhere.[131] The focus of this section is on advocacy strategies at both the domestic and international level which may be useful for ending or preventing internet shutdowns.

Domestic Efforts

Run campaigns and coalitions

Domestic campaigns can be effective in calling the government to account for an internet shutdown. This may be easier when a shutdown is regional and therefore the campaign can be coordinated by groups in other parts of the country. For example, Internet Sans Frontières developed a campaign in early 2019 around the hashtag #Maalla_Gatétou to enable Chadian activists to call attention to the country's frequent shutdowns. Tigrayan activists around the world have also used the hashtag #ReconnectTigray to draw attention to the ongoing two-year long shutdown happening in Ethiopia's Tigray region. Creative suggestions from researchers for effective domestic campaigning on this topic include:

- advocating for the creation of a national digital rights organisation;
- maximising the financial cost of a shutdown by advocating for reimbursement for affected subscribers;
- maximising the reputational costs of ordering or participating in shutdowns, for example through "naming and shaming" lists or coordinated boycotts; or
- highlighting the technical and security risks of internet shutdowns for network protocols and internet routing.

Document human rights abuses during a shutdown

When a shutdown is taking place, it is vital to continue to document the human rights abuses that it may be obscuring, both to ensure that shutdowns are not seen as effective means of silencing dissent and evading accountability by the government in the future, and to ensure that victims are able to call perpetrators to account. Useful tools for this include Advocacy Assembly and Witness' "Documenting Human Rights Violations During Internet Shutdowns" course[132] and Optima's Internet Shutdowns Resource Library.[133] The International Committee of the Red Cross has also established a phone hotline in Tigray to help affected individuals communicate with their loved ones and share their stories of what has happened to them.[134]

Push the government to commit to not shut down

For states which have only used shutdowns sporadically, pushing in advance for public commitments not to shut down the internet around politically sensitive periods like elections has proven an effective strategy. For example, Kenyan and Ghanaian authorities have publicly committed to not shutting down the internet ahead of elections.[135] Even partial commitments may go some way to discouraging further internet shutdowns; for example, the Zambian Information and Communication Authority agreed in March 2022 not to act outside its legal authority to interrupt access to the internet, and to inform the public of the reason for any internet shutdown within 36 hours of implementation in the future. [136]

Strategically litigate against shutdowns

Disputing the legality of an internet shutdown before a national or regional court has proven effective in certain countries in recent years. For example, ECOWAS the Community Court of Justice ruled in 2020 that the Togolese internet shutdown during general elections in 2017 was unlawful, in response to a lawsuit filed by Amnesty International Togo and other applicants.[137] The Court ruled that access to the internet should be protected by law, regardless of "national security concerns", and ordered Togo not to shut down the internet again. Additionally, in 2022 the Court declared the seven months long Twitter shutdown in Nigeria in 2021 unlawful following a lawsuit against the Nigerian government by Nigerian civil society organisations, including the Socio-Economic Rights and Accountability Project (SERAP) and Paradigm Initiative.[138]

Litigation has also proven an effective tactic in Sudan, where—despite the absence of a specific law on shutdowns—telcos are obliged by their subscriber contracts to maintain their network connections. Based on this, a lawyer sued his mobile network provider for cutting off his access during the June 2019 shutdown, and was successful in restoring his own internet access. He then filed a class action suit, and the court again ordered in his favour, ordering MTN, Sudani and Zain to restore services for all their customers.[139]

Reviewing several of these strategic litigation cases, the African Internet Rights Alliance highlight that the success or effectiveness of such an approach will depend on multiple factors, including:

- capacity and resourcing constraints of the complainants;
- the independence of national and regional courts;
- the effectiveness of national, regional and international human rights frameworks;
- opportunities for engagement due to *locus standi* and the exhaustion of local remedy requirements (before regional courts/mechanisms);
- the capacity of judicial officers, including their knowledge of digital rights issues;
- the enforceability of judicial pronouncements;
- the time taken to determine the case;
- the degree of collaboration between activists, CSOs, lawyers and concerned citizens.[140]

Encourage decentralisation of telecommunications infrastructure

Where possible, encouraging a greater diversity of private and non-state actors within the telecommunications infrastructure of a country may provide greater protection against government-mandated shutdowns, or at least increase the inconvenience of imposing one. This will strongly depend on the national regulatory framework surrounding telecommunications providers and internet services; but new and emerging technologies may also offer new options for more decentralised internet access through connection sharing. Access Now point out that technologies such as Starlink, Amazon's Sidewalk protocol, the Helium Network and distributed Virtual Private Networks (VPNs) reduce the expense of deploying internet access infrastructure and, if adopted, could potentially reduce a government's control over individuals' internet access.[141]

Box 4 **Who to target with advocacy efforts?**

Depending on the context, different actors may hold different degrees of influence over a government contemplating implementing or continuing an internet shutdown.

Where a country has a strong and independent judiciary, strategic litigation may be a particularly effective means of holding the government to account. Within governments, different departments may be more receptive to advocacy from civil society; for example, Ministries of Health or Education may be more aware of the damage and disruption that internet shutdowns may cause to citizens, and could raise these issues with the executive branch. Some countries have strong national human rights institutions, or individual political leaders or parties which may be active on these topics and able to platform civil society concerns.

In some cases, domestic institutions may provide virtually no recourse to redress or assistance to victims, in which case international mechanisms—such as the Human Rights Council's Universal Periodic Review (UPR) or Special Experts processes—may be more able to apply external pressure. While in MENA there is no regional human rights mechanism, the African Commission on Human and People's Rights may also issue statements or guidance on issues affecting member states, and other regional bodies can introduce resolutions and set precedents within their own jurisdictions and continue to draw attention to the human rights impacts of internet shutdowns globally.

While individual private sector actors may not be able to effect change or influence a government's decisions, industry coalitions may carry more weight. It is also important to educate citizens on their rights in relation to internet shutdowns and to encourage them to raise awareness and advocate against shutdowns through local political processes.[142]

International efforts

Pressure the government from the outside

In some cases, individual countries have issued statements on internet shutdowns occurring in Africa and the Middle East, condemning their use and calling for internet access to be restored. For example, in 2019 the US government criticised Cameroon's internet shutdown in the Anglophone region and called on the Cameroonian government to respect the rights of their citizens.[143] International and multilateral organisations have also jointly condemned internet shutdowns; for example, the 36 member states of the Freedom Online Coalition recently issued a joint statement calling on the Iranian government to "immediately lift restrictions intended to disrupt or prevent their citizens from accessing and disseminating information online and from communicating safely and securely."[144] The European Union also issued a statement condemning the Iran shutdown for "blatantly violat[ing] freedom of expression."[145] Such international pressure is also a focal point of some campaigns—for example, in addition to coordinating joint letters to the Ethiopian government on the Tigray internet shutdown,[146] Access Now have also organised a coalition calling on the African Union to denounce it and demand that authorities restore access immediately.[147]

In some cases, even multinational companies have weighed in publicly. Twitter's Public Policy Team, for example, raised concern over disruption to internet services observed in Tanzania in October 2020,[148] and has expressed support for the #KeepItOn campaign.[149] Orange also publicly criticised the use of internet shutdowns in Guinea in October 2020.[150] The international shareholders of local telecommunications companies may also be able to exert pressure on the local government, and can also push for greater transparency from the company on compliance with internet shutdown orders in line with ESG investment principles.

Clarify the international legal framework

Recent reports by the UN Human Rights Council have provided concrete guidance and standards on the human rights implications of internet shutdowns.[151] The 2022 report from the OHCHR, for example, recommended that:

> **"Given their indiscriminate and disproportionate impacts on human rights, States should refrain from the full range of Internet shutdowns. Blanket shutdowns in particular inherently impose unacceptable consequences for human rights and should never be imposed.[152]**

In Africa, too, regional guidance on the human rights implications of internet shutdowns is also available.[153] There is a continued need to sensitise policymakers to this guidance and potentially to build their capacity and understanding of the human rights impacts of shutting down the internet. The ITU should also issue guidance clarifying that the Constitution should not be interpreted to authorise the use of internet shutdowns (see Box 2).

Make the case for an open, safe and secure internet

The deeper trend of digital authoritarianism underpinning the rise of internet shutdowns requires consistent and sustained engagement and advocacy for a more open and democratic model of internet governance. Many global forums are seeking to build consensus around the need for an open and secure internet and to condemn politically motivated interference with information and communications technologies, as evidenced by the G7 statement on open societies,[154] the US-led Declaration for the Future of the Internet (which has been backed by over 60 countries),[155] and the African Union's Declaration on Internet Governance and Development of Africa's Digital Economy.[156] Other multistakeholder initiatives are also contributing to this work. For example, civil society groups developed the African Declaration on Internet Rights and Freedom in 2014;[157] and the UN's Internet Governance Forum recently established a Policy Network on Internet Fragmentation.[158]

The Freedom Online Coalition's Task Force on Internet Shutdowns has also developed extensive resources and guidelines for its 36 member states for diplomatic engagement on the topic of internet shutdowns, including providing tools, messaging and good practices.[159]

Support those working to document internet shutdowns

A number of organisations work to detect and report the prevalence of internet shutdowns around the world. Verifying and confirming user reports of shutdowns through telemetry and monitoring techniques play a vital part in holding governments to account. This work requires continued resourcing and is strengthened by transparent collaboration within and between monitoring organisations, private sector actors and on-the-ground reporters.

Notes

[1] United Nations Human Rights Council (UNHRC) "Rights to freedom of peaceful assembly and of association: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association" A/HRC/41/41, 2019, https://digitallibrary.un.org/record/3822961; UNHRC, "Ending Internet shutdowns: a path forward: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", A/HRC/47/24/Add.2, 2021, https://digitallibrary.un.org/record/3929056; UNHRC, "Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights: Report of the Office of the United Nations High Commissioner for Human Rights", A/HRC/50/55, May 13, 2022, https://digitallibrary.un.org/record/3977326

[2] "STOP data", #KeepItOn Project, Access Now, https://www.accessnow.org/keepiton/ (accessed November 24, 2022)

[3] UNHRC, Report A/HRC/50/55, para. 25, https://digitallibrary.un.org/record/3977326

[4] There is no clear definition of which countries are included in the MENA Region, but it is typically considered to include at least Algeria, Bahrain, Djibouti, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Libya, Malta, Morocco, Oman, Qatar, Saudi Arabia, Syria, Tunisia, the United Arab Emirates, Palestine, and Yemen. For the purposes of this paper, we also include Mauritania, Somalia, Sudan and Turkey in the group referred to as "MENA".

[5] Access Now, "STOP data"

[6] *The Return of Digital Authoritarianism: Internet shutdowns in 2021* (Access Now, 2022)

[7] *Taxonomy of a shutdown: 8 ways governments restrict access to the internet, and how to #KeepItOn* (Access Now, 2022); Steven Feldstein, *Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?* (Carnegie Endowment for International Peace, 2022) pp.9–10

[8] Ryzdak notes that network resilience is generally higher if more domestic telecommunications service providers have direct connections to foreign providers at international internet gateways. See Jan Rydzak, *Disconnected: A human rights based approach to internet shutdowns* (Global Network Initiative, 2016) p.8.

[9] Several research participants pointed out that different internet shutdown techniques will impact groups within different—and often discriminatory—ways. One noted that the young, insecurely housed or financially disadvantaged are more dependent on mobile internet connections, whereas large companies and those that are wealthy can afford WiFi access. An internet shutdown which cuts mobile internet access, therefore, will adversely impact those that are already disadvantaged on other metrics. Another noted that the economic shocks provoked by internet shutdowns are felt over long periods of time, "greatly exacerbating pre-existing social and economic inequalities".

[10] Sigi Waigumo Mwanzia, Victor Kapiyo, and Odanga Madung, *Study on Internet Shutdowns in Africa*, (African Internet Rights Alliance, 2021), pp.7–8

[11] UNHRC, Report A/HRC/50/55, para. 25, https://digitallibrary.un.org/record/3977326

[12] Gustaf Björksten, *A Taxonomy of Internet Shutdowns: The technologies behind network interference*, (Access Now, 2022), pp.5-6.

[13] See, for example: Sandra Aceng, "The gendered impact of intentional internet shutdowns", Digital Human Rights Lab, August 3, 2022, https://digitalhumanrightslab.org/blog/the-gendered-impact-of-intentional-internet-shutdowns/; Advocacy Assembly, "Pride month, internet shutdowns and the effect on LGBTIQ groups", June 30, 2022, https://advocacyassembly.org/en/news/227/; Skylar Thompson and Felicia Anthonio, "Shutdown impact stories: how internet shutdowns affect women in Iran", Access Now, June 23, 2022, https://www.accessnow.org/how-internet-shutdowns-affect-women-in-iran/; Mohammed Kimbugwe, PWDs bear the brunt of internet shutdowns, NTV, January 18, 2021, https://www.ntv.co.ug/ug/commentaries/pwds-bear-the-brunt-of-internet-shutdowns-3261046

[14] Note that the MENA region has no regional human rights mechanism.

[15] See footnote 1, as well as: *Iran: Tightening the Net 2020, After Blood and Shutdowns*, (ARTICLE19, 2020) pp. 15-16; Tomiwa Ilori, *Life Interrupted: Centering the Social Impacts of Network Disruptions in Advocacy in Africa* (Global Network Initiative, 2021) pp.17-23; Legal Guidance on Internet Restrictions and Shutdowns in Africa, (International Commission of Jurists, 2022); Anthonio, "The Kill Switch"

[16] We use this as an umbrella term to cover a range of human rights abuses that result from physically violent treatment, including arbitrary deprivation of life, disappearance, torture and inhuman or degrading treatment or punishment.

[17] International Covenant on Civil and Political Rights (ICCPR), Article 13.

[18] ICCPR, Article 25.

19 "#KeepItOn in Somaliland: authorities cannot quash public protest and access to information", Access Now, August 11, 2022, https://www.accessnow.org/keepiton-in-somaliland/

20 Unwanted Witness, "Uganda 2021 General Elections: Internet shutdown and it's Ripple Effects", APC, January 27, 2021, https://www.apc.org/en/news/uganda-2021-general-elections-internet-shutdown-and-its-ripple-effects

21 "Jordan bans coverage of teachers' protests", Reporters Without Borders, August 12, 2020, https://rsf.org/en/jordan-bans-coverage-teachers-protests

22 "Jordan's internet throttling to censor protesters must end", Access Now, March 19, 2021, https://www.accessnow.org/jordan-protest-throttling/

23 João Tomé, "Burkina Faso experiencing second major Internet disruption this year", Cloudflare, January 1, 2022, https://blog.cloudflare.com/internet-disruption-in-burkina-faso/

24 "Burkina Faso restores constitution, names coup leader president", Aljazeera, January 31, 2022, https://www.aljazeera.com/news/2022/1/31/burkina-faso-restores-constitution-names-coup-leader-president

25 Sam Mednick, "Hundreds march in Burkina Faso to show support for new junta", AP News, January 25, 2022, https://apnews.com/article/ouagadougou-burkina-faso-africa-religion-islamic-state-group-91977eb12fe1667142334b131880ec45; Declan Walsh, "Gunfire Rattles Burkina Faso's Capital as Soldiers Revolt", New York Times, January 23, 2022, https://www.nytimes.com/2022/01/23/world/africa/burkina-faso-mutiny-gunfire.html

26 Ana Monteiro, "US to Cut Burkina Faso From Africa Trade Program After Counter-Coup", Bloomberg, November 2, 2022, https://www.bloomberg.com/news/articles/2022-11-02/us-to-cut-burkina-faso-from-africa-trade-plan-after-counter-coup

27 Moki Edwin Kindzeka, "AU: Despite Irregularities, Chad Poll Credible", Voice of Africa, April 14, 2016, https://www.voanews.com/a/au-despite-irregularities-chad-poll-credible/3285269.html; "Chad: Freedom in the World 2022: Chad", Freedom House, https://freedomhouse.org/country/chad/freedom-world/2022 (accessed November 24, 2022).

28 Daniel Eizenga, "The unstable foundations of political stability in Chad", *West African Papers*, No. 12, OECD Publishing, 2018; "Chad: Account for 'Disappeared' Opposition Leaders", Human Rights Watch, February 28, 2008, https://www.hrw.org/news/2008/02/26/chad-account-disappeared-opposition-leaders; "Chad: Alleged Coup Attempt No Excuse to Ignore Rights", Human Rights Watch May 9, 2013, https://www.hrw.org/news/2013/05/09/chad-alleged-coup-attempt-no-excuse-ignore-rights

29 Aboubacar Barma, "Tchad: l'addition salée des 235 jours de restriction d'accès à internet", La Afrique Tribune, December 7, 2016, https://afrique.latribune.fr/afrique-centrale/2016-12-07/tchad-l-addition-salee-des-235-jours-de-restriction-d-acces-a-internet.html; "Joint submission to the United Nations Human Rights Council Universal Periodic Review 2018 Cycle – Chad", Internet Sans Frontières, Access Now, and Utopie Nord-Sud, 2018, https://internetwithoutborders.org/wp-content/uploads/2018/04/UPR_Chad_English.pdf

30 Juliet Nanfuka, "Chad Is Blocking Social Media And Messaging Apps… Again!", CIPESA, April 5, 2018, https://cipesa.org/2019/03/cipesa-open-net-africa-among-80-organisations-denouncing-extended-social-media-shutdown-in-chad/

31 Felicia Anthonio,"#ShutdownStories: how Chad's fixation on social media blackouts hurts citizens", Access Now, September 22, 2020, https://www.accessnow.org/shutdownstories-how-chad-fixation-on-social-media-blackouts-hurts-citizens/

32 "Chad opposition leader says several relatives killed in home raid", Aljazeera, February 28, 2021, https://www.aljazeera.com/news/2021/2/28/chad-opposition-candidate-says-security-forces-raided-his-home; Samira Sawlani (@samirasawlani) "Ahead of April polls- @netblocks confirm internet block in Chad after incident @ opposition candidate Yaya Dillo's home", Tweet, February 28, 2021 https://twitter.com/samirasawlani/status/1366039028508860420?s=20&t=W7OLIg2FxPOA0IKcbR1XVg

33 At least two killed in skirmish at Chad opposition candidate's house", Thomson Reuters Foundation, February 28, 2021, https://news.trust.org/item/20210228121308-wn8wd/; "Chad opposition chief flees after security operation kills two", Radio France internationale, March 1, 2021, https://www.rfi.fr/en/africa/20210301-chad-opposition-chief-flees-after-security-operation-kills-two

34 "Tchad : internet coupé depuis dimanche", Tchadinfos, 1 March 2021, https://tchadinfos.com/politique/tchad-internet-coupe-depuis-dimanche/; Google, "Traffic and Disruptions to Google", https://transparencyreport.google.com/traffic/overview?group=REGION&disruption_history=product:1;size:4;p:NDoyOjpBTEw6Og&lu=fraction_traffic&fraction_traffic=start:1613955600000;end:1615575600000;product:19;region:TD (accessed November 24, 2022).

[35] "Chad: Internet shutdowns impeding freedom of expression", Amnesty International, April 29, 2021, https://www.amnesty.org/en/latest/press-release/2021/04/tchad-les-coupures-internet-une-entrave-la-liberte-dexpression/

[36] "Message To The Nation From The President Of The Transitional Military Council, President Of The Republic, Head Of State, Army Corps General". Statement by Mahamat Deby, Presidency of the Republic of Chad, April 27, 2021, https://presidence.td/economie-sante/; "Rebels threaten to march on capital as Chad reels from president's battlefield death", Reuters, April 21, 2021, https://www.reuters.com/world/africa/rebels-threaten-march-capital-chad-reels-presidents-battlefield-death-2021-04-21/

[37] For more detail, see Lewis Mudge, "Chad: How Much Longer Will the Military Council Stay?", Human Rights Watch, April 20, 2022, https://www.hrw.org/news/2022/04/20/chad-how-much-longer-will-military-council-stay; Sioudina Dominique, "Chad's military transition bottleneck and deadlocks in the constitution-making process, Constitution Net, November 29, 2021, https://constitutionnet.org/news/chads-military-transition-bottleneck-and-deadlocks-constitution-making-process

[38] See footnote 16 for definition of the term.

[39] ICCPR, Article 9.

[40] ICCPR, Article 7.

[41] ICCPR, Article 6.

[42] "Publisher Djimet Wiché attacked by Chadian police while covering protests", Reporters Without Borders, 15 February 2018, https://ifex.org/publisher-djimet-wiche-attacked-by-chadian-police-while-covering-protests/

[43] "Internet in eastern Ethiopia shut down after regional violence", Reuters, 8 August 2018, https://www.reuters.com/article/us-ethiopia-internet-idUSKBN1KT0T4

[44] "Sudan protests turn deadly as demonstrators clash with police", BBC News, 20 December 2018, https://www.bbc.co.uk/news/world-africa-46642251

[45] "On the days of darkness in Zimbabwe", Zimbabwe Human Rights NGO Forum, 18 January 2019, https://www.hrforumzim.org/on-the-days-of-darkness-in-zimbabwe/; UN High Commissioner for Human Rights, "Press briefing note on Zimbabwe", OHCHR, 18 January 2019, https://www.ohchr.org/en/press-briefing-notes/2019/01/press-briefing-note-zimbabwe?LangID=E&NewsID=24087

[46] "Benin: Freedom in the World 2022", Freedom House, https://freedomhouse.org/country/benin/freedom-world/2022 (accessed November 24, 2022)

[47] "Ethiopia failed coup: Fifth death, national mourning, mastermind killed", Africa News, 24 June 2019, https://www.africanews.com/2019/06/24/ethiopia-failed-coup-fifth-death-national-mourning-mastermind-killed/. The death and injuries were in relation to a foiled coup plot. It is unclear from reports whether the perpetrators posed an immediate threat to life or public safety and therefore it is unclear whether this was a legitimate or illegitimate use of force.

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

[49] "MFWA Condemns Social Media Disruption, Violence against Protesters", Media Foundation West Africa, 25 June 2019, https://www.mfwa.org/country-highlights/mfwa-condemns-social-media-disruption-violence-against-protesters/

[50] "Iraq: Protect the right to peaceful demonstration, release all detained demonstrators and reopen access to the Internet / Assassination of human rights lawyer Jabbar Mohammed Al-Karm in Basra", Gulf Centre for Human Rights, 24 August 2018, https://www.gc4hr.org/news/view/1912

[51] Patrick Cockburn, "Iraq on brink of mass popular uprising as internet shut down and indefinite curfew imposed by officials", The Independent, 4 October 2019, https://www.independent.co.uk/news/world/middle-east/iraq-protests-baghdad-internet-blackout-curfew-a9141686.html

[52] Ahmed Rasheed and John Davison, "5-Iraqi forces kill six protesters in Baghdad, southern port blocked", Reuters, 7 November 2019, https://www.reuters.com/article/iraq-protests-idUKL8N27N0V1

[53] Amnesty, "A Web of Impunity: The killings Iran's shutdown hid", https://iran-shutdown.amnesty.org/ (accessed November 24, 2022); "Special Report: Iran's leader ordered crackdown on unrest - 'Do whatever it takes to end it'", Reuters, 23 December 2019, https://www.reuters.com/article/us-iran-protests-specialreport-idUSKBN1YR0QR

[54] Ermias Tasfaye, "Amid blackout, western Oromia plunges deeper into chaos and confusion", Ethiopia Insight, 14 February 2020, https://www.ethiopia-insight.com/2020/02/14/amid-blackout-western-oromia-plunges-deeper-into-chaos-and-confusion/. The numbers of civilian fatalities at the hands of the military during this period of internet shutdown are disputed.

[55] Agence France-Presse, "166 die during protests after shooting of Ethiopian singer", The Guardian, 4 July 2020, https://www.theguardian.com/world/2020/jul/04/166-dead-following-protests-at-shooting-of-ethiopian-pop-star

[56] "Mali: Bloody repression of protesters and attacks against the media", ARTICLE19, 15 July 2020, https://www.article19.org/resources/mali-bloody-repression-of-protesters-and-attacks-against-the-media/

[57] "Chad slows down internet to curb 'hate speech' on social media", Aljazeera, 4 August 2020, https://www.aljazeera.com/news/2020/8/4/chad-slows-down-internet-to-curb-hate-speech-on-social-media

[58] "Zanzibar: Opposition claims 9 killed, leader held ahead of polls", Aljazeera, 27 October 2020, https://www.aljazeera.com/news/2020/10/27/zanzibar-opposition-say-leader-held-three-dead-ahead-of-polls. Reports indicate that these individuals were trying to stop the army from distributing ballot boxes which they suspected contained pre-ticked votes. It is unlikely that they posed any immediate threat to life or public safety and this use of force is likely to have been illegitimate.

[59] UNHRC, "Report of the International Commission of Human Rights Experts on Ethiopia", A/HRC/51/46, September 20, 2022, https://reliefweb.int/report/ethiopia/report-international-commission-human-rights-experts-ethiopia-ahrc5146-advance-unedited-version

[60] "At least two killed in skirmish at Chad opposition candidate's house", Reuters, 28 February 2021, https://news.trust.org/item/20210228121308-wn8wd/

[61] "Iran: Internet shutdowns curb protests and conceal human rights violations in Sistan and Baluchistan", ARTICLE19, 26 February 2021, https://www.article19.org/resources/iran-internet-shutdowns-curb-protests-and-conceal-human-rights-violations-in-sistan-and-baluchistan/

[62] Victor Oluwole, "#WhatsHappeningInNiger: The internet shutdown in Niamey threatens Niger's democracy and its people's right to free speech", Business Insider Africa, 6 March 2021, https://africa.businessinsider.com/local/leaders/whatshappeninginniger-the-internet-shutdown-in-niamey-threatens-nigers-democracy-and/p7l4nhk

[63] "Eswatini pro-democracy protests continue to mount as government blocks internet, social media", News24, 15 October 2021, https://www.news24.com/news24/africa/news/eswatini-pro-democracy-protests-continue-to-mount-as-government-blocks-internet-social-media-20211015

[64] "Internet shutdowns and blockings continue to hide atrocities of military coup in Sudan", Access Now, 23 November 2021, https://www.accessnow.org/update-internet-shutdown-sudan/

[65] Sam Mednick, "3 protesters wounded by French soldiers in Burkina Faso", AP News, 20 November 2021, https://apnews.com/article/africa-niger-west-africa-blockades-burkina-faso-955d259d852af2aeae534264a46e0323

[66] "URGENT: Iran Human Rights Calls on International Community to Stop Bloody Crackdown of Isfahan Protests", Iran Human Rights, 26 November 2021, https://iranhr.net/en/articles/4992/

[67] Mohamed Amin, "Sudan: Ten killed as pro-democracy protests sweep country", Middle East Eye, 30 June 2022, https://www.middleeasteye.net/news/sudan-pro-democracy-protests-killed

[68] "Protesters killed, internet shut down and curfew imposed amidst deadly protests in Sierra Leone", Media Foundation West Africa, 12 August 2022, https://www.mfwa.org/protesters-killed-internet-shut-down-and-curfew-imposed-amidst-deadly-protests-in-sierra-leone/

[69] "Somaliland: Clashes between protesters, police turn deadly", Aljazeera, 12 August 2022, https://www.aljazeera.com/news/2022/8/12/several-people-killed-100-hurt-in-somaliland-protests

[70] David Gritten, "Iran hands out more death sentences to anti-government protesters", BBC, 15 November 2022, https://www.bbc.co.uk/news/world-middle-east-63648629.

[71] Peter Micek, "Update: Mass internet shutdown in Sudan follows days of protest", Access Now, October 15, 2013, https://www.accessnow.org/mass-internet-shutdown-in-sudan-follows-days-of-protest/

[72] Tom Wilson, "Sudan internet blackout forces battered protesters to rethink", Financial Times, 11 June 2019, https://www.ft.com/content/b1848126-8c0f-11e9-a1c1-51bf8f989972

[73] See, for example, "Statement by the Troika, the European Union and Switzerland", Norwegian Ministry of Foreign Affairs, November 12, 2021, https://www.norway.no/en/sudan/norway-sudan/news-events/statement-by-the-troika-eu-and-switzerland/; UNHRC, "32nd Special Session of the Human Rights Council on the implications of the ongoing situation in the Republic of the Sudan - Statement by the UN High Commissioner for human Rights, Michelle Bachelet," November 5, 2021, https://reliefweb.int/report/sudan/32nd-special-session-human-rights-council-implications-ongoing-situation-republic-sudan

[74] "Authorities in Sudan must stop imposing telecommunication blackouts to control information flow during military coup, Access Now, October 25, 2021, https://www.accessnow.org/sudan-internet-shutdown-military-coup/; "Internet shutdowns and blockings continue to hide atroc-

ities of military coup in Sudan", Access Now, November 21, 2021 https://www.accessnow.org/update-internet-shutdown-sudan/; João Tomé and Carlos Azevedo, "Sudan was cut off from the Internet for 25 days," Cloudflare, November 22, 2021, https://blog.cloudflare.com/sudan-internet-back-25-days/

[75] Ibid.

[76] Tomé and Azevedo, "Sudan was cut off from the Internet for 25 days"

[77] Noha Elhennawy, "Sudan doctors: 8 people killed in mass rallies against coup," AP News, June 30, 2022, https://apnews.com/article/technology-africa-middle-east-sudan-f4ac2322682f42cd9e1f66114f50fe1f

[78] "Hundreds demonstrate against the UN in Sudan," Africa News, June 1, 2022, https://www.africanews.com/2022/06/01/hundreds-demonstrate-against-the-un-in-sudan/

[79] Such as the Computer Crimes Law of 2010 and the User Protection Bill of 2022.

[80] Sophie Bushwick, "How Iran Is Using the Protests to Block More Open Internet Access", The Scientific American, October 13, 2022, https://www.scientificamerican.com/article/how-iran-is-using-the-protests-to-block-more-open-internet-access/

[81] Amnesty, "A Web of Impunity: The killings Iran's shutdown hid"

[82] Shutdown Monitor: What is Happening in Sistan and Baluchestan?", Filter Watch, February 26, 2021, https://filter.watch/en/2021/02/26/shutdown-monitor-what-is-happening-in-sistan-and-baluchestan/

[83] "'We are risking death': Iranians on Mahsa Amini protests", The Guardian, September 23, 2022, https://www.theguardian.com/global-development/2022/sep/23/mahsa-amini-protests-iranian-women-risking-death

[84] Jon Gambrell, "Iran protests reach 19 cities despite internet disruption", PBS, October 12, 2022, https://www.pbs.org/newshour/politics/iran-protests-reach-19-cities-despite-internet-disruption

[85] Joyce Sohyun Lee, Stefanie Le, Atthar, Mirza & Bebash Dehghanpisheh, "Tactics of repression: How Iran is trying to stop Mahsa Amini protests", The Washington Post, October 5, 2022, https://www.washingtonpost.com/investigations/2022/10/05/iran-protests-crackdown-deadly/; "Iran detains journalists and celebrities as death toll from "ruthless" crackdown on protests climbs" CBS News, September 30, 2022, https://www.cbsnews.com/news/mahsa-amini-iran-protests-deaths-ruthless-crackdown-journalists-celebrities/

[86] OONI, IODA, M-Lab, Cloudflare, Kentik, Censored Planet, ISOC, Article19, "Technical multi-stakeholder report in Internet shutdowns", OONI, November 29, 2022, https://ooni.org/post/2022-iran-technical-multistakeholder-report/#disruptions-to-network-infrastructure; "Iran Will Restrict Internet Access As Long As Protests Go On", Iran International, September 9, 2022, https://www.iranintl.com/en/20220929933; See also Basso, S., Xenon, M., Filastò, A. & Meng, A. (2022), Iran blocks social media, app stores and encrypted DNS amid Mahsa Amini protests, (see reference 30); Simone Basso, Maria Xynou, Arturo Filastò and Amanda Meng, "Iran blocks social media, app stores and encrypted DNS amid Mahsa Amini protests", OONI, November 29, 2022, https://ooni.org/post/2022-iran-blocks-social-media-mahsa-amini-protests/; Doug Madory and Peter Micek, "Suppressing Dissent: The Rise of the Internet Curfew", Kentik, November 16, 2022, https://www.kentik.com/blog/suppressing-dissent-the-rise-of-the-internet-curfew/

[87] Sanya Burgess, "Iran protests: Government uses internet 'kill-switch' as tech savvy youth continue to evade digital censorship", Sky News, October 18, 2022, https://news.sky.com/story/iran-protests-government-uses-internet-kill-switch-as-tech-savvy-youth-continue-to-evade-digital-censorship-12723012

[88] Recently-leaked documents from Iranian telecoms provider Ariantel expose details of SIAM; see Sam Biddle and Murtaza Hussain, "Hacked Documents: How Iran Can Track And Control Protesters' Phones", The Intercept, October 28, 2022, https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/

[89] Yasmin Green, "Iran's Internet Blackouts Are Part of a Global Menace", WIRED, October 19, 2022, https://www.wired.com/story/iran-mahsa-amini-internet-shutdown/; Nadia Al-Faour, "How Iran is manipulating the online narrative to cover up its violent crackdown on protests," Arab News, October 4, 2022, https://www.arabnews.com/node/2175206/media

[90] Alijani Ershad, "How the WhatsApp, Instagram blackout is impacting millions of Iranians", 16 January 2023, The Observers, https://observers.france24.com/en/middle-east/20230116-instagram-whatsapp-internet-blackout-iran-protests

[91] Bushwick, "How Iran Is Using the Protests to Block More Open Internet Access"

[92] "Iran Protests: At least 234 Including 29 Children Killed/ Families and Doctors Pressured to Confirm False Scenarios", Iran Human Rights, October 25, 2022, https://iranhr.

net/en/articles/5535/; “Iran: At least 23 children killed with impunity during brutal crackdown on youthful protests,”, Amnesty, October 13, 2022, https://www.amnesty.org/en/latest/news/2022/10/iran-at-least-23-children-killed-with-impunity-during-brutal-crackdown-on-youthful-protests/

[93] David Gritten, “Iran hands out more death sentences to anti-government protesters”, BBC, November 15, 2022, https://www.bbc.co.uk/news/world-middle-east-63648629; Iran Human Rights, “Iran Protests: At least 234 Including 29 Children Killed”; Patrick Wintour, Maryam Foumani and Oliver Holmes, “Scores of executions feared in Iran as 23-year-old hanged in public killing”, The Guardian, December 12, 2022, https://www.theguardian.com/world/2022/dec/12/scores-of-executions-feared-in-iran-as-23-year-old-hanged-in-public-execution

[94] “Iran: Leaked documents reveal top-level orders to armed forces to ‘mercilessly confront’ protesters”, Amnesty, September 30, 2022, https://www.amnesty.org/en/latest/news/2022/09/iran-leaked-documents-reveal-top-level-orders-to-armed-forces-to-mercilessly-confront-protesters/

[95] For example, The US and EU imposed new sanctions on senior Iranian officials, law enforcement bodies and cyber-related entities; several UN bodies and experts made public statements urging Iranian authorities to ease the crackdown and provide redress for victims; the Freedom Online Coalition issued a joint statement calling upon Iranian authorities to end the network disruptions and respect Iran’s international human rights obligations and the #KeepItOn coalition has organised a joint letter to Iranian authorities from dozens of civil society groups.

[96] “Many Gazans cut off from the world as Israel targets communications and internet networks,” Euro Med Monitor, May 18, 2021, https://euromedmonitor.org/en/article/4398/Many-Gazans-cut-off-from-the-world-as-Israel-targets-communications-and-internet-networks

[97] “Aid group says death toll from Yemen prison airstrike at 87,” AP News, January 23, 2022, https://apnews.com/article/technology-internet-access-middle-east-yemen-red-sea-3fa7feb290baa404d3f2d554f237a649

[98] “Ethiopia declares state of emergency in Tigray”, Aljazeera, November 4, 2020, https://www.aljazeera.com/news/2020/11/4/ethiopia-declares-state-of-emergency-in-opposition-tigray-region

[99] Aggrey Mutambo, “Ethiopia shuts down telephone, internet services in Tigray”, The East African, November 5, 2020, https://www.theeastafrican.co.ke/tea/rest-of-africa/ethiopia-telephone-internet-services-tigray-2731442

[100] “Ethio Telecom Restores 363 Mobile Sites In Tigray”, Fanabc, February 8, 2021, https://www.fanabc.com/english/ethio-telecom-restores-363-mobile-sites-in-tigray/; Ethiopia Current Issues Fact Check (@ETFactCheck), “Restoration of Telecom and Electricity Services in Tigray Region”, Tweet, December 14, 2020, https://twitter.com/ETFactCheck/status/1338395070089846785.

[101] Catherine Byaruhanga, “Ethiopia’s Tigray conflict: Nasa shows how a war zone faded from space”, BBC News, October 20, 2022, https://www.bbc.co.uk/news/world-africa-63315388.

[102] UNHRC, “Report of the International Commission of Human Rights Experts on Ethiopia”, A/HRC/51/46, September 20, 2022, https://reliefweb.int/report/ethiopia/report-international-commission-human-rights-experts-ethiopia-ahrc5146-advance-unedited-version

[103] Note that after the June 2021 elections the Information Network Security Agency – a government entity that has de facto authority over the internet with a mandate to protect the communications infrastructure and prevent cybercrime – was placed directly under the supervision of Prime Minister Ahmed. See “Freedom on the Net: Ethiopia”, Freedom House, 2022, https://freedomhouse.org/country/ethiopia/freedom-net/2022.

[104] Zecharias Zelalem, “Six million silenced: A two-year internet outage in Ethiopia”, Context, September 29, 2022, https://www.context.news/digital-rights/six-million-people-in-the-dark-tigrays-two-year-internet-outage; Nikolaj Nielsen, “Cyberattack behind Tigray blackout, says Ethiopia,” EU Observer, December 14, 2020, https://euobserver.com/world/150369; Ethio Telecom (@Ethiotelecom), “Clarification on Tigray Region Telecom Services Current Situation”, Tweet, December 2, 2020, https://twitter.com/ethiotelecom/status/1334122968931328000?s=20&t=X-FgxG32Z__zNrX_bNajaSw; Ethiopia Current Issues Fact Check (@ETFactCheck), “Ethio Telecom’s CCTV camera footage from the premises of the Mekelle Core Center,” Tweet, December 14, 2020, https://twitter.com/ETFactCheck/status/1338484976124309505?s=20&t=vRXUYUN-w1jvuykbO8-FT_Q; Office of the Prime Minister - Ethiopia (@PMEthiopia), “Statement on the Tigray Region Rule of Law Operations”, Tweet, March 3, 2021, https://twitter.com/PMEthiopia/status/1367136074938597381?s=20&t=BFz-PlZ_6Uhu84jM7XpFywQ; “Ethio Telecom Claims Regional Operations in Meqelle Tampered With”, Embassy of Ethiopia to Belgium, Luxembourg and E.U., December 12, 2020, https://ethiopianembassy.be/ethio-telecom-claims-re-

gional-operations-in-meqelle-tampered-with/;

105 OHCHR, "Report of the Ethiopian Human Rights Commission (EHRC)/Office of the United Nations High Commissioner for Human Rights (OHCHR) Joint Investigation into Alleged Violations of International Human Rights, Humanitarian and Refugee Law Committed by all Parties to the Conflict in the Tigray Region of the Federal Democratic Republic of Ethiopia", 2021; James Jeffrey, "Ethiopia's Tigray conflict and the battle to control information", Aljazeera, 16 February 2021, https://www.aljazeera.com/news/2021/2/16/ethiopias-tigray-conflict-and-the-battle-to-control-information; Salem Solomon, "Ethiopia Government Clamps Down on War Coverage," Voice of America, December 1, 2021, https://www.voanews.com/a/ethiopia-government-clamps-down-on-war-coverage/6335716.html

106 After years in the dark, Tigray is slowly coming back online", 1 February 2023, Access Now, https://www.accessnow.org/tigray-shutdown-slowly-coming-back-online/

107 UNHRC Report A/HRC/51/46 para. 55.

108 UNHRC, Report A/HRC/51/46 paras 97-99; OHCHR "Report of the Ethiopian Human Rights Commission", paras. 353-354.

109 Giulia Paravicini, "Nearly half the people in Ethiopia's Tigray in 'severe' need of food aid, World Food Programme says", Reuters, August 20, 2022, https://www.reuters.com/world/africa/nearly-half-people-ethiopias-tigray-need-food-aid-wfp-2022-08-19/; Lizzy Davies, "Tigray ceasefire: aid workers demand telecoms be restored", The Guardian, July 2, 2021, http://www.theguardian.com/global-development/2021/jul/02/tigray-ceasefire-aid-workers-demand-telecoms-be-restored

110 Ilori, *Life Interrupted*, p.14. CIPESA also reports that 77% of the 22 African countries where internet disruptions were ordered between 2015 and 2019 were authoritarian; see Mwanzia, Kapiyo, and Madung, *Study on Internet Shutdowns in Africa*, section 2.2.

111 Feldstein, *Government Internet Shutdowns Are Changing*, p.13. See also Peter Guest, "In the Dark: Seven years, 60 countries, 935 internet shutdowns: How authoritarian regimes found an off switch for dissent", Rest of World, April 26, 2022, https://restofworld.org/2022/blackouts/

112 Global Network Initiative (GNI), "Country Legal Frameworks Resource" (CLFR), https://clfr.globalnetworkinitiative.org/ (accessed November 24, 2022). See also Mwanzia, Kapiyo, and Madung, *Study on Internet Shutdowns in Africa*

113 GNI, "CLFR: Egypt", https://clfr.globalnetworkinitiative.org/country/egypt/ (accessed November 24, 2022, last updated May 2017).

114 GNI, "CLFR: Democratic Republic of Congo", https://clfr.globalnetworkinitiative.org/country/dr-congo/ (accessed 25 November 2022, last updated May 2017).

115 GNI, "CLFR: Turkey", https://clfr.globalnetworkinitiative.org/country/turkey/, (accessed November 24, 2022, last updated May 2017)

116 Kinfe Yilma "The Legal Justification of Sorts for Ethiopia's Internet Shutdowns,", Addis Fortune, July 18, 2020, https://addisfortune.news/the-legal-justification-of-sorts-for-ethiopias-internet-shutdowns/

117 International Telecommunications Union, *Constitution and Convention of the International Telecommunication Union*, 1992

118 UNHRC, Report A/HRC/47/24/Add.2, pp. 16-17.

119 Dawit Endeshaw, "Kenya's Safaricom launches network in Ethiopia as first private operator", Reuters, October 6, 2022, https://www.reuters.com/business/media-telecom/kenyas-safaricom-launches-network-ethiopia-first-private-operator-2022-10-06/

120 The Iranian government formerly controlled internet traffic through the IPM International and TIC gateways, but has since decentralised these gateways and allowed local internet providers to connect directly to the international network. It is interesting to note that the authorities did not utilise their control over these gateways in implementing the 2019 shutdown, instead choosing to order multiple ISPs to shut down. This method was slower but less costly and disruptive. For more information, see *Iran: Tightening the Net 2020*.

121 UNHRC, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", A/HRC/35/22, paras. 31, 49 and 79; 2017, http://undocs.org/A/HRC/35/22; UNHRC, Report A/HRC/50/55, para. 30.

122 Mwanzia, Kapiyo and Madung, *Study on Internet Shutdowns in Africa*, p.14 (citing the Open Tech Fund)

123 *Internet shutdowns in Africa: Addressing the Human Rights Responsibilities of Telecommunication Companies* (Business and Human Rights Resource Centre, 2022)

124 See also David Sullivan, "Five Ways Telecommunications Companies Can Fight Internet Shutdowns", Lawfare, August 23, 2020, https://www.lawfareblog.com/five-ways-telecommunications-companies-can-fight-internet-shutdowns; *Internet shutdowns in Africa*: *Addressing the Human Rights Responsibilities of Telecommunication Companies*, Business and Human Rights Resource Centre, March 2022.

125 Using Access Now "STOP Data". The three countries are Saudi Arabia, Bahrain and The Gambia.

126 "Burkina Faso must immediately end its internet shutdown, not extend it," Access Now, January 25, 2022, https://www.accessnow.org/burkina-faso-internet-shutdown/

127 Mwanzia, Kapiyo, and Madung, *Study on Internet Shutdowns in Africa*

128 UNHRC, Report A/HRC/50/55, p.7 (drawing on Access Now STOP Data).

129 Jan Rydzak, Moses Karanja and Nicholas Opiyo, "Dissent Does Not Die in Darkness: Network Shutdowns and Collective Action in African Countries," *International Journal of Communication* 14 (2020): 4264–4287, p. 4280.

130 For example, the 2016 Deloitte Study on the cost of internet shutdowns differentiates between high, medium and low connectivity economies, with internet shutdowns costing $23.6 million, $6.6 million and $0.6 million per 10 million population per day respectively. See Deloitte, *The economic impact of disruptions to Internet connectivity: A report for Facebook* (The Global Network Initiative, 2016); *A Framework for Calculating the Economic Impact of Internet Disruptions in Sub-Saharan Africa* (CIPESA, 2017).

131 See, for example, Feldstein, *Government Internet Shutdowns Are Changing*, pp. 20-23

132 Witness, "Documenting Human Rights Violations During Internet Shutdowns," Online Course, Advocacy Assembly, https://advocacyassembly.org/en/courses/62/#/chapter/1/lesson/1 (accessed November 24, 2022)

133 "Prepare, Prevent, Resist: The OPTIMA Internet Shutdowns Resource Library", Optima, https://preparepreventresist.org/ (accessed 22 November 2022)

134 International Committee of the Red Cross Ethiopia, "ICRC and Ethiopian Ethiopian Red Cross Phone Call Service", Facebook Video, 16 February 2021, https://www.facebook.com/ICRCEthiopia/videos/icrc-and-ethiopian-ethiopian-red-cross-phone-call-service/3528789113916327/

135 Moses Muoki, "Kenya Says Won't Shut Internet Over Hate Speech", All Africa, June 30, 2021, https://allafrica.com/stories/202107010480.html; Anthonio, "The Kill Switch", p.15

136 "Chapter One Foundation Ltd v Zambia Information and Communications Technology Authority (HP 955 of 2021) [2022] ZMHC 3", High Court of Zambia, March 17, 2022.

137 Felicia Anthonio, Natalia Krapiva, Berhan Taye, Peter Micek and Laura O'Brien, "ECOWAS Court upholds digital rights, rules 2017 internet shutdowns in Togo illegal", Access Now, June 25, 2020, https://www.accessnow.org/internet-shutdowns-in-togo-illegal/

138 "ECOWAS Court victory: Twitter ban in Nigeria declared unlawful", Access Now, July 14, 2022, https://www.accessnow.org/ecowas-court-nigeria-unlawful-twitter-ban/

139 "Litigating Internet Disruptions in Africa: Lessons from Sudan", CIPESA, March 3, 2022, https://cipesa.org/2022/03/litigating-internet-disruptions-in-africa-lessons-from-sudan/. Although this litigation was successful, it should be noted with caution that authorities retaliated against one of the applicants of the class action suit (The Consumer Protection Organization) by de-registering their organisation and seizing their property and bank accounts.

140 Mwanzia, Kapiyo, and Madung, Study on Internet Shutdowns in Africa, Section 3

141 *Taxonomy of a shutdown: 8 ways governments restrict access to the internet, and how to #KeepItOn*, p. 35.

142 Anthonio, "The Kill Switch"

143 United States House of Representatives, "Calling on the Government of Cameroon and armed groups to respect the human rights of all Cameroonian citizens, to end all violence, and to pursue a broad-based dialogue without preconditions to resolve the conflict in the Northwest and Southwest regions", H.Res.358, July 23, 2019

144 "Joint Statement on Internet Shutdowns in Iran", Freedom Online Coalition, October 2022

145 Council of the European Union, "Iran: Declaration by the High Representative on behalf of the EU", 25 September 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/09/25/iran-declaration-by-the-high-representative-on-behalf-of-the-eu/

146 "#KeepItOn in Tigray: Ethiopia must lift the blackout from conflict zone", Access Now, July 29, 2021, https://www.accessnow.org/cms/assets/uploads/2021/07/Tigray_Ethiopia_KeepItOn_Statement.pdf; "Open letter to Prime Minister Abiy Ahmed Ali: Keep the internet open and secure throughout the upcoming elections and thereafter," Access Now, June 18, 2021, https://www.accessnow.org/keepiton-open-letter-ethiopia-election-2021/

147 "Tell The African Union To Help Reconnect The Internet In Tigray And Across Ethiopia," Access Now, November 4, 2022, https://act.accessnow.org/page/116140/action/1

148 Twitter Public Policy (@Policy), "Ahead of tomorrow's election in #Tanzania, we're seeing some blocking and throttling of Twitter,", Tweet, October 27, 2020, https://twitter.com/Policy/status/1321106129208922113

149 Monique Meche, "#KeepItOn: Making your voice heard to end Internet shutdowns", Twitter Blog, May 26, 2020, https://blog.twitter.com/en_us/topics/company/2020/keep-it-on-making-your-voice-heard-to-end-internet-shutdowns

150 "France's Orange says Guinea network suffered cuts without prior warning", Reuters, October 26, 2020, https://

www.reuters.com/article/ozabs-uk-guinea-election-orange-idAFKBN27B0U9-OZABS

151 See footnote 1.

152 UNHRC Report A/HRC/50/55, para. 66.

153 For more information, see Ilori, Life Interrupted, pp.17-23; Mwanzia, Kapiyo, and Madung, *Study on Internet Shutdowns in Africa*, Table 4; *Legal Guidance on Internet Restrictions and Shutdowns in Africa*.

154 G7, "Open Societies Statement," July 12, 2021, https://www.consilium.europa.eu/media/50364/g7-2021-open-societies-statement-pdf-355kb-2-pages.pdf

155 US Department of State, "Declaration for the Future of the Internet", April 2022

156 African Union, "Declaration on Internet Governance and Development of Africa's Digital Economy", AU/Decl.3, January 29, 2018, https://www.saigf.org/AU-Declaration%20on%20IG.pdf

157 "The African Declaration on Internet Rights and Freedoms", African Internet Rights, 2014, https://africaninternetrights. org/en/declaration

158 For more information, see the Internet Governance Forum Policy Network on Internet Fragmentation webpage, https://www.intgovforum.org/en/content/policy-network-on-internet-fragmentation Policy Network's Webpage (accessed November 24, 2022)

159 For more information, see the Freedom Online Coalition *Task Force on Internet Shutdowns* webpage, https://freedomonlinecoalition.com/task_forces_and_wg/task-force-on-internet-shutdowns/ (accessed November 24, 2022)