United Nations A/HRC/47/24/Add.2

General Assembly

Distr.: General
15 June 2021

English only

Human Rights Council
Forty-seventh session
21 June–9 July 2021
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Ending Internet shutdowns: a path forward

Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*

Summary

As a follow-up to his report on the rights to freedom of peaceful assembly and of association in the digital era, submitted to the Human Rights Council at its forty first session (A/HRC/41/41), the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément N. Voule, presents to the Human Rights Council a study of recent trends and the impact of Internet shutdowns in relation to peaceful protests, and makes recommendations to address this global phenomenon.

* Reproduced as received, in the language of submission only.

I. Introduction

1. In 2019, the Special Rapporteur presented to the Human Rights Council a thematic report examining the intersection between digital technologies and the enjoyment of the rights to freedom of peaceful assembly and of association.[1] While the report recognized that digital technologies have expanded opportunities for the enjoyment and exercise of peaceful assembly and association rights, it also raised concerns about the use of these technologies by state and non-state actors "to silence, surveil and harass dissidents, political opposition, human rights defenders, activists and protesters."[2]

2. Crucially, the report expressed alarm at the rise of internet shutdowns during critical democratic moments such as elections and peaceful protests and their harmful impacts. The report observed that these measures are a violation of the right to peaceful assembly provided for in Article 21 of the International Covenant on Civil and Political Rights and can never be considered a lawful restriction of this fundamental freedom.[3] It emphasized that "access to Internet and mobile telephony services should be maintained at all times, including during times of civil unrest. Access to and use of digital technologies during elections for assembly and association purposes should be specially respected, protected and promoted."[4] The report called on States to "refrain from, and cease, measures such as cutting off access to the Internet and telecommunications services." It recommended "repealing and amending any laws and policies that allow network disruptions and shutdowns and refraining from adopting such laws and policies."[5]

3. Since the report was submitted to the Human Rights Council, the Special Rapporteur has strived to promote the implementation of its recommendations, engaging with governments, civil society organizations and other key stakeholders. He issued several communications and press releases condemning shutdowns in countries around the world and participated in several public events raising concern about the troubling trend. He engaged on this issue with government authorities of Zimbabwe[6] and Sri Lanka[7] during his official visits to those countries. He also joined the international human rights community to ensure the United Nations speaks more clearly about these practices, including their impact on human rights during the Covid-19 pandemic.[8] For example, he worked with governments and civil society to ensure the 2020 Human Rights Council resolution[9] on human rights in the context of peaceful protests adopted stronger language against shutdowns. The Special Rapporteur engaged with the UN Human Rights Committee, as it developed general comment No. 37 on the right to peaceful assembly, to ensure the general comment included clear standards on the use of internet shutdowns relating to peaceful assemblies.

4. Notwithstanding the progress made, many States around the world have continued to hinder connectivity and impose internet shutdowns with the aim of clamping down on peaceful protests. Shutdowns have become an entrenched practice in certain regions, especially as a means for incumbent regimes to retain power and stifle dissent. Shutdowns are lasting longer, becoming harder to detect and targeting particular social media and messaging applications and specific localities and communities. Shutdowns have continued during the COVID-19 pandemic, impeding people's ability to access essential services during the ongoing health crisis and intensifying the closing of civic space around the world. Particularly in countries that have responded to the pandemic with a national militaristic approach,[10] these shutdowns have been adopted alongside other repressive tactics, including the criminalization of journalists and human rights defenders.

[1] A/HRC/41/41.
[2] A/HRC/41/41, para. 3.
[3] A/HRC/41/41, para 52.
[4] A/HRC/41/41, para. 74.
[5] A/HRC/41/41, para. 73, b).
[6] A/HRC/44/50/Add.2, paras. 57 and 58.
[7] A/HRC/44/50/Add.1, paras. 80 and 81.
[8] See, www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25788&LangID=E.
[9] Human Rights Council resolution 44/20 of 23 July 2020.
[10] *See* www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25788&LangID=E and

5. The objective of the present addendum is to increase understanding of the magnitude and severity of internet shutdowns as a means to suppress the right to peaceful assembly, with a view toward proposing a path forward to end this practice. Section II of the addendum provides an overview of the applicable international legal framework, while also drawing on the practice of States, regional mechanisms, and UN initiatives. Section III examines key trends and impacts of internet shutdowns recorded since the 2019 report was submitted to the Human Rights Council, and Section IV analyses promising practices and proposes a framework for what needs to be done to address the rising threat of shutdowns. The report concludes with a set of recommendations.

6. In writing the present addendum, the Special Rapporteur benefited from civil society input gathered in three online expert meetings held on 16 December 2020, and 8 and 13 April 2021. He also consulted with other stakeholders bilaterally. The Special Rapporteur would like to thank all those who participated in these meetings and who shared their experiences and expertise to inform the report.

7. For the purposes of this addendum, internet shutdowns are understood broadly as "the intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information."[11] Shutdowns can then range from large-scale complete disconnection of the internet and mobile networks to other network disruptions, including the blocking of particular services or applications, such as social media platforms and messaging apps and throttling or the slowing down internet traffic to impede connectivity. [12]

II. International legal framework

A. Access to the internet

8. The right to access and use internet and other digital technologies for the purposes of peaceful assembly is protected under article 20 of the Universal Declaration of Human Rights and article 21 of the International Covenant on Civil and Political Rights. As indicated in general comment No. 37 of the Human Rights Committee on Article 21: The Right to Peaceful Assembly, "[a]lthough the exercise of the right of peaceful assembly is normally understood to pertain to the physical gathering of persons, article 21 protection also extends to remote participation in, and organization of, assemblies, for example online."[13] This protection covers those activities associated with peaceful assemblies that "happen online or otherwise rely upon digital services,"[14] including planning and organizing a gathering, mobilizing resources; disseminating information, preparing for and traveling to the event; communicating with other organizers and participants leading up to and during the assembly; monitoring or broadcasting the assembly. In turn, interference with such technologies can result in the violation of this fundamental freedom.[15]

9. International human rights law has developed well-established principles recognizing access to internet as a necessary precondition for the exercise and enjoyment of human rights online and offline, including the right to peaceful assembly. The Human Rights Council has consistently affirmed that "the same rights that people have offline must also be protected online" and has called upon all States to enhance the access to and use of the internet in order to promote the full enjoyment of human rights for all.[16] More recently and in the context of the Covid-19 pandemic, the Council emphasized the need for greater protection to internet access and connectivity. It stressed that "in times when physical assemblies are restricted,

[11] *See* Global Network Initiative, "Disconnected: A Human Rights Approach to Network Disruptions" (2017).
[12] A/HRC/35/22, para. 8.
[13] CCPR/C/GC/37, para. 13.
[14] CCPR/C/GC/37, para. 10.
[15] A/HRC/41/41.
[16] Human Rights Council resolution 20/8 of 5 July 2012. See also: Council resolutions 26/13 of 26 June 2014, 32/13 of 1 July 2016 and 38/7 of 5 July 2018.

[…] it is all the more necessary […] to ensure that access to the Internet extends to the entirety of the global population and that it is affordable, and fully respects and protects each individual's right to privacy."[17]

10. At the regional level, the Committee of Ministers of the Council of Europe has affirmed that "[a]ccess to the internet is a precondition for the exercise of rights and freedoms online," as enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms.[18] The Inter-American Commission on Human Rights (IACHR) has stressed that that access to the internet "is a condition *sine qua non* for the effective exercise of human rights today, especially including the rights to freedom of expression and opinion, association and assembly."[19] The African Commission on Human and People's Rights (ACHPR) has affirmed that "States shall recognize that universal, equitable, affordable and meaningful access to the internet is necessary for the realization of freedom of expression, access to information and the exercise of other human rights."[20]

11. The importance of access to internet is further reflected in international commitments towards achieving sustainable development and building knowledge societies. In several declarations and resolutions adopted within the framework of UN agencies and entities, States have pledged to take steps to ensure that high-quality, affordable, open and secure internet is available to all individuals without discrimination.[21] Notably, in the 2030 Agenda for Sustainable Development States committed to "significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020."

B. Internet shutdowns

12. Article 21 of the Covenant promotes an expansive understanding of the right to peaceful assembly, where full exercise is the norm, and restrictions the exception to that right. States bear the burden of justifying any restriction. Authorities must be able to show that restrictions meet the requirement of legality and are also both necessary in a democratic society for and proportionate to at least one of the permissible grounds for restrictions enumerated in article 21. The Human Rights Committee stressed that "the imposition of any restrictions should be guided by the objective of facilitating the right, rather than seeking unnecessary and disproportionate limitations on it. Restrictions must not be discriminatory, impair the essence of the right, or be aimed at discouraging participation in assemblies or causing a chilling effect."[22]

13. Internet shutdowns fail to meet all of these conditions, a point that the Human Rights Committee emphasized when it affirmed that "States parties must not block or hinder internet connectivity in relation to peaceful assemblies. The same applies to geo-targeted or technology-specific interference with connectivity or access to content."[23] Similarly, the U.N. General Assembly[24] and the Human Rights Council[25] have called upon States to refrain from implementing internet shutdowns and to ensure internet is available at all times, including during peaceful protests.[26] The Special Rapporteur and other mandate holders have joined regional experts to condemn internet shutdowns, reaffirming that "using communications

[17] Human Rights Council resolution 44/20 of 17 July 2020.

[18] Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies), para, 1.

[19] IACHR. Standards for a Free, Open and Inclusive Internet (2017), para. 32.

[20] ACHPR. Declaration of principles on freedom of expression and access to information in Africa, adopted in 2019. See also, 362 Resolution on the Right to Freedom of Information and Expression on the Internet in Africa - ACHPR/Res.362(LIX)2016.

[21] See, for example, General Assembly resolution 70/1 of 21 October 2015.

[22] CCPR/C/GC/37, para. 10.

[23] CCPR/C/GC/37, para. 34.

[24] General Assembly resolution 73/173 of 17 December 2018.

[25] Council resolutions 20/8 of 5 July 2012, 26/13 of 26 June 2014, 32/13 of 1 July 2016 and 38/7 of 18 July 2018.

[26] Council resolutions 38/11 of 6 July 2018 and 44/20 of 23 July 2020.

'kill switches' (i.e. shutting down entire parts of communications systems) are measures which can never be justified under human rights law,"[27] and urging States to refrain from adopting such measures, including for the purposes of preventing peaceful assemblies.[28] In the 2020 Roadmap for Digital Cooperation the UN Secretary-General stressed that "blanket internet shutdowns and generic blocking and filtering of services are considered by UN human rights mechanisms to be in violation of international human rights law."[29]

14. Regional bodies have also emphasized that internet shutdowns infringe upon human rights norms. The ACHPR affirmed the principle of non-interference with access to internet and stressed that States "shall not engage in or condone any disruption of access to the internet and other digital technologies for segments of the public or an entire population."[30] The Economic Community of West African States (ECOWAS) Community Court ruled that shutting down internet access is a violation of the right to freedom of expression."[31] The Council of Europe called on States to recognize "in law and in practice that disconnecting individuals from the Internet, as a general rule, represents a disproportionate restriction of the right to freedom of expression," as provided for in the European Convention on Human Rights.[32]

15. The incompatibility of internet shutdowns with article 21 of the Covenant must be emphasized. First, to satisfy the requirement of legality, restrictions on assemblies must have a formal basis in law, as must the mandate and powers of the restricting authority. Laws must be publicly accessible, be drafted clearly and narrowly, and with sufficient precision to limit authorities' discretion while enabling an individual to act accordingly.[33] Domestic laws must also be aligned with the relevant international norms and standards. Internet shutdowns imposed during peaceful assemblies are often ordered covertly and without legal basis. When shutdowns are recognized, authorities often invoke executive or administrative orders or antiquated or ambiguous norms that provide impermissible discretion to authorities.[34]

16. Beyond the legality requirement, restrictions on assemblies must also protect a specific legitimate interest from actual harm. As a result, general or vague assertions that internet shutdowns are necessary for maintaining public order or protecting national security (or other permissible ground for restriction) are inconsistent with article 21. The protection of national security and public order are often invoked to justify internet shutdowns. While protecting national security and public order is a legitimate purpose under article 21, the mere possibility that a peaceful assembly may provoke adverse or even violent reactions from some members of the public cannot be used to justify restrictions under those grounds, including an internet shutdown National security, in particular, cannot be invoked as rationale for restrictions "where the very reason for the deterioration of national security is the suppression of human rights."[35]

17. As indicated by the Human Rights Committee, "restrictions on peaceful assemblies must not be used, explicitly or implicitly, to stifle expression of political opposition to a government, challenges to authority, including calls for democratic changes of government, the constitution or the political system, or the pursuit of self-determination. They should not be used to prohibit insults to the honour and reputation of officials or State organs."[36] As such, internet shutdowns may never be invoked as a justification for suppressing advocacy

[27] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15921&LangID=E

[28] See www.ohchr.org/Documents/Issues/FAssociation/joint-declaration-democratic-governance/declaration-en.pdf

[29] A/74/821, para 41.

[30] ACHPR, Declaration of principles on freedom of expression and access to information in Africa (2019).

[31] Economic Community of West African States (ECOWAS) Community Court, Jud No. ECW/CCJ/JUD/09/20.

[32] Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom.

[33] CCPR/C/GC/37, para. 39.

[34] A/HRC/41/41 para 52 and A/HRC/35/22, para 9 and 10. See also, ECOWAS Community Court, Jud No. ECW/CCJ/JUD/09/20.

[35] CCPR/C/GC/37, para. 42.

[36] CCPR/C/GC/37, para. 49.

of democracy and human rights. Nor can they be used to curtail monitoring, reporting on, and ensuring accountability for gross human rights violations in relation to peaceful protests.

18. Under necessity and proportionality conditions, restrictions to the right to peaceful assembly must be appropriate, must be the least intrusive measure to achieve a legitimate interest, and must not be overbroad. States are obliged to take all reasonable measures that do not impose disproportionate burdens upon peaceful assemblies to protect all participants and to allow them to take place in an uninterrupted manner.[37]

19. To be considered "necessary in a democratic society", authorities must demonstrate that shutdowns are appropriate responses to a pressing social need, relating to one of the permissible grounds listed in article 21.[38] By contrast, shutdowns have been found extremely counterproductive,[39] creating serious risks to the rule of law, political pluralism, and human rights. Given the purpose of the right to peaceful assembly as a potential tool of political and social participation,[40] shutdowns imposed to prevent unrest around contested elections are particularly troubling.[41] The Special Rapporteur has stressed that during elections, when tensions are at their highest, access to internet is actually needed to provide accurate information and dispel rumours.[42] States are under the obligation to identify and implement alternative means to maintain public order in these critical times, in accordance with international human rights norms and standards.

20. Shutdowns are thus inconsistent with proportionality requirements. They impose extreme burdens on those exercising expression and peaceful assembly rights and exert significant chilling effects on decisions regarding whether to participate in public assemblies. These chilling effects hold direct implications on participatory democracy, whose existence depends upon an active and informed citizenry capable of engaging with a range of ideas. Those on the margins of society are most impacted by these chilling effects. Large-scale shutdowns of communication networks, in particular, have been deemed a form of collective punishment.[43] Moreover, internet shutdowns generate a wide variety of harms to human rights, economic activity, public safety and emergency services that outweigh the purported benefits. Shutdowns also threaten to undermine the rights to liberty and personal integrity, by impeding the access of protestors to emergency help and contact with family and friends.[44]

C. Responsibilities of digital technology companies

21. In his 2019 report, the Special Rapporteur affirmed that the global framework for assessing digital technology companies' responsibilities to respect human rights is provided by the Guiding Principles on Business and Human Rights.[45] Guiding principles 11–24 recognize that business "should respect human rights" by avoiding infringing on the human rights of others and by addressing adverse human rights impacts with which they are involved. In order to fulfil this obligation, business enterprises should have in place human rights policies and processes – including a policy commitment to meet their responsibility to respect human rights; a human rights due diligence process to identify, prevent, mitigate, and account for how they address their human rights impacts; and processes to enable the remediation of any adverse human rights impacts that they cause or to which they contribute.[46] The Guiding principles provide guidance on how to address of internet shutdowns, including the adoption of mitigation strategies and transparency measures. In keeping with these principles, companies should require that shutdowns requests be made in

[37] CCPR/C/GC/37, para. 34.
[38] CCPR/C/GC/37, para. 40.
[39] A/HRC/35/22, para 14.
[40] Human Rights Council resolution 15/21 of October 2010.
[41] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26988&LangID=E
[42] A/HRC/41/41, para. 53.
[43] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24909&LangID=E and www.achpr.org/pressrelease/detail?id=8
[44] A/HRC/41/41, para 53.
[45] A/HRC/17/31.
[46] A/HRC/41/41, para 18.

writing and present a clear explanation of their legal basis and institutional authority to issue the request. Companies should explore all legal options for challenging requests and disclose all relevant information about shutdowns and mitigate the impact of gag orders or other non-disclosure laws.[47]

III. Overview of key trends and impacts

22. Since the submission of his 2019 report to the Human Rights Council, the Special Rapporteur has been monitoring reported instances of internet shutdowns during peaceful protests across the world, including in the context of elections. Along with data collected by civil society groups, monitoring activities conducted by the Special Rapporteur reveal a set of global trends and impacts related to the imposition of these shutdowns, which are examined in this section. The country situations mentioned here refer to events recorded in the period of January 2019 - May 2021. They have been the subject of communications sent to Governments, as well as press releases and reports issued by special procedures mandate holders, high-level United Nations officials and entities and regional human rights mechanisms. The report also relies on aggregated data collected and made publicly available by civil society organizations.

A. Trends and modalities of shutdowns

23. Internet shutdowns are a growing global phenomenon. The #KeepItOn Coalition[48] has recorded at least 768 government-ordered internet disruptions in about 63 countries since 2016. A total of about 187 internet shutdowns relating to peaceful assemblies, while about 55 shutdowns in the context of elections have also been documented from 2016 to May 2021. From January 2019 through May 2021, the coalition has documented at least 79 incidents of protest-related shutdowns, including in the context of elections.

24. **The number of governments imposing internet shutdowns during mass demonstrations continues to grow**, with many States adopting these extreme measures for the first time in this period. The practice is not limited to authoritarian regimes. Shutdowns have been observed in long-established democracies and more recent democracies alike, in line with broader trends of democratic recession across the world. In Latin America, for example, shutdowns were recorded only in Nicaragua and Venezuela as of 2018, but since then, Colombia[49], Cuba[50] and Ecuador[51] have reportedly adopted shutdowns in connection to mass protests.

25. **Shutdowns are increasing in length, scale, and sophistication.** This period saw the longest shutdowns ever registered, with Bangladesh adopting a mobile internet blackout for 355 days in the Cox's bazar refugee camps.[52] The shutdown was imposed in retaliation against Rohingya refugees for staging a peaceful demonstration commemorating the second anniversary of the Myanmar military's ethnic cleansing campaign in Rakhine State ("Genocide Day") on 25 August 2019.[53] This shutdown affected about 900,000 people living in these camps. Ethiopia's three-week shutdown in July 2020[54] affecting a population of more than 100 million people is another example of this trend.

26. More and more of these prolonged shutdowns involve a range of disruption techniques, with governments implementing nation-wide internet blackouts along with harder to detect and targeted network disruptions. For instance, in Belarus, the government

[47] A/HRC/35/22.

[48] The KeepItOn Coalition is comprised of more than 240 organizations from 105 countries around the world. More information here: https://www.accessnow.org/keepiton/#coalition

[49] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27093&LangID=E

[50] See IACHR, Annual Report 2020, Chapter IV b), the Situation of Human Rights in Cuba, paras 76-81.

[51] See www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25188&LangID=E

[52] Access Now/#KeepItOn Coalition, "Shattered Dreams and Lost Opportunities," (2020).

[53] BGD 2/2019.

[54] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26115&LangID=E.

adopted a nationwide shutdown amid mass protests contesting election results in August 2020. When connectivity was restored, authorities then targeted pro-democracy gatherings regularly convened every Sunday from September until December 2020, by slowing down connection to social media (throttling).[55] These measures continued during the hours of the protests and directly affected the areas where protestors gathered in the city of Minsk. These tactics reportedly lasted for 121 days, with Telegram and Virtual Private Networks (VPNs) still blocked as the time of writing.

27. Notably, in the context of the February 2021 military coup, Myanmar has ordered several national internet blackouts and other disruptions aimed at curbing the free flow of information and interfering with activism to defend democracy.[56] Just before the coup began on 1 February 2021, the military junta plunged the entire country into a blackout for a few hours.[57] As mass protests began to spread in cities across the country, the junta ordered a second large-scale shutdown that dropped down connectivity to 14% on 7 February. All telecommunications companies were ordered to block Facebook, Twitter, and Instagram, along with certain Virtual Private Networks (VPNs) being used to circumvent the restrictions. While on 8 February, connectivity seemed to have been restored, authorities began implementing routine shutdowns during night time hours between 14 and 22 February, disrupting protesters' organizing activities and communications with the international community, while limiting interference with businesses and the government activities during the day. The Special Rapporteur on the situation of human rights in Myanmar highlighted that these shutdowns also provided "impunity for security forces carrying out arrests and violent crackdowns throughout the night."[58] Pro-democracy protests nonetheless continued to grow, with hundreds of thousands of people joining demonstrations. On 2 April 2021, the military reportedly ordered telecommunication companies and Internet Service Providers (ISPs) to shut down all wireless broadband services, "until further notice." Civil society groups informed the Special Rapporteur that as of April 28, fiber optic and fixed cable connectivity is apparently available. While this is a positive development, they cautioned that this measure still leaves the vast majority of people in Myanmar – who access the internet using mobile networks - disconnected.

28. **Bandwidth throttling – or deliberately reducing Internet speeds –is becoming increasingly common.** Some governments are resorting to the extensive use of throttling, a more subtle way of shutting down the Internet than the "kill switch", but with equally effective results.[59] By slowing internet traffic or access to specific apps or services, States ensure the internet becomes effectively unusable for protest activity, preventing the circulation of photos and videos because they require greater bandwidth. When these types of shutdowns are imposed, affected individuals report the internet is drastically slowed, and does not generally permit access to video calls or livestreaming apps or social media sites. These measures are much harder to document and respond to and States may seek to justify access limitations on technical grounds. In countries that already suffer from poor connectivity, throttling can be harder to detect and easily be confused with connection problems, shielding governments from scrutiny.

29. **Most shutdowns target applications and services used by protesters.** States are designing shutdowns to directly block access to the communications platforms and services most used by protesters, like Facebook, Twitter, WhatsApp, or Telegram. States are also targeting internet shutdown circumventions tools, such as VPN services. Social media and messaging were partially blocked in Mali for 5 days in July 2020 amid mass protests seeking political reforms.[60] Venezuela restricted access to Twitter, Facebook, and Instagram in 2019 in the context of mass protests across the country.[61] By intentionally hindering access to the apps and services most used by peaceful demonstrators, these shutdowns not only

[55] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26164&LangID=E.

[56] AL MMR 1/2021. See also, A/HRC/46/56.

[57] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26705&LangID=E.

[58] A/HRC/46/56, para 74.

[59] From January 2019 to May 2021, 14 instances of throttling relating to peaceful protests were documented by the #KeepItOn coalition.

[60] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26124&LangID=E.

[61] AL VEN 2/2019.

illegitimately target peaceful protests but may also increase the risks of protesters and human rights defenders being subjected to unlawful government surveillance and criminalization. Civil society groups consulted in preparation for this report, for example, expressed concerns that shutdowns of social media in the Islamic Republic of Iran pushes protesters towards government-controlled apps and services.

30. **Shutdowns are used as pre-emptive tools against peaceful assemblies, especially in the context of elections.** Many of the shutdowns recorded since 2019 appear to be aimed at curbing the free flow of information and tightening civic space during times considered politically sensitive or of public discontent. Elections are perhaps the best example. In this period, election-related internet shutdowns were documented in Benin, Belarus, the Democratic Republic of Congo, Malawi, Uganda, Kazakhstan, and other countries globally.[62] For instance, Uganda implemented a country wide internet shutdown for 5 days (13-18 January 2021) before, during, and after their general elections (14 January 2021)[63] to curtail knowledge of opposition arrests and to stifle any opposition against proclaimed results. The blackout followed several days of blocking social media and messaging apps.

31. **Marginalized and at-risk populations are especially targeted.** Some States intentionally use shutdowns to target certain communities, localities and groups of individuals, including members of national, ethnic, and linguistic minorities, who are generally more vulnerable to State repression during peaceful assemblies. These shutdowns exert a greater chilling effect on the right to peaceful assemblies of historically vulnerable communities and further marginalize them. For instance, in August 2019, Indonesian authorities shut down internet access in Papua in response to protests against discrimination and renewed calls for an independence referendum.[64] Kashmiris and other ethnic minorities in India have faced historically long targeted internet shutdowns, with India implementing a months-long regional shutdown in 2019 in Kashmir and Jammu states.[65] Rohingya and other displaced ethnic minorities have also been regularly subjected to mobile shutdowns both in Myanmar[66] and in the world's largest refugee camp in Bangladesh.[67] The Special Rapporteur stresses that for displaced peoples and those in conflict situations, internet shutdowns have severe impacts beyond their ability to organize and collectively voice their concerns. The Internet serves as a lifeline for vulnerable populations, without which they are prevented from accessing crucial services. Shutdowns also inflict greater suffering, by impeding communications with their loved ones and the outside world.

B. Impacts

32. Internet shutdowns not only violate the rights to freedom of peaceful assembly and freedom of opinion and expression, but are, unequivocally, harmful to many other human rights, which in the digital age depend on many digital technologies. Shutdowns can affect the rights to life and personal safety, personal liberty and access to justice, free elections, and political participation as well as many social, economic, and cultural rights.

33. The Special Rapporteur is especially concerned about the fact that, under cover of an information blackout, internet shutdowns facilitate abuses and gross human rights violations committed in the context of peaceful protests. As mentioned earlier, internet shutdowns are often implemented hand in hand with other repressive tactics against protesters, effectively thwarting efforts to report on and hold government accountable for human rights violations committed in the context of peaceful protests. Civil society and human rights groups have stressed that these shutdowns make it nearly impossible to document and report on human rights violations in real-time; to expose the crimes being committed against peaceful protesters; and to galvanize the response of domestic actors and the international community. Shutdowns also allow States to control the information and narratives relating to the protests,

[62] Access Now/#KeepItOn Coalition, "Shattered Dreams and Lost Opportunities," (2020).
[63] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26988&LangID=E.
[64] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24990&LangID=E.
[65] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24909&LangID=E.
[66] A/HRC/46/56, para 14.
[67] BGD 2/2019.

especially as internet shutdowns are almost always implemented alongside other measures restricting media freedom.

34. For instance, immediately after the shutdown was imposed by the Government of Bangladesh in Rohingya refugee camps near Cox's Bazar, large numbers of military, police, and Rapid Action Battalion police reportedly entered the camps. The Special Rapporteur received reports of arrests, beatings, and extrajudicial killings, with those arrested being denied access to legal representation.[68] A curfew was vigorously enforced, while authorities confiscated thousands of mobile phones and banned refugees from buying SIM cards. According to the information received protest organizers and other human rights defenders were subjected to government surveillance and smear campaigns. Non-governmental organizations working in the refugee camps had their activities suspended.[69]

35. In Ethiopia, for example, the internet was cut across most of the country on 30 June 2020 amid protests following the shooting of prominent Oromo singer Haacaaluu Hundeessaa. Official reports say 166 people were killed, although unofficial reports put the number much higher. According to police, some 2,000 people were arrested, including opposition leaders.[70] Authorities in Iraq blocked social media platforms and restricted messaging apps for 50 days, during two waves of mass protests that took place on October 2019. The restrictions were shortly followed by a near-total internet shutdown that cut off the entire country as protests escalated and evidence of targeted killings of protesters emerged.[71] The Islamic Republic of Iran imposed a nation-wide shutdown during mass protests against rising fuel prices between 15 and 19 November of 2019. Credible reports received by the Special Rapporteur claim at least 304 deaths occurred, including 12 children, at the hands of security forces. Unconfirmed estimates suggest the death toll included up to 1,500 deaths.[72] In Sudan, several shutdowns were imposed during the 8-month long prodemocracy movement to deter protesters from livestreaming police repression. A near total blackout was introduced for almost 5 weeks to prevent documentation of reported systematic killing and mass rape of protesters participating in a sit-in in Khartoum on 3 June 2019.[73] Most recently in Myanmar, where authorities have imposed regular internet shutdown, reports of mass killing of peaceful protesters continue to emerge.

36. Shutdowns also threaten sustainable development. Shutdowns directly impede the achievement of Universal access to information and communications technologies" (Target 9.C). Access to the internet is so fundamental to the achievement of the 2030 Agenda that governments committed to ensuring universal and affordable access to the internet in least developed countries in just 5 years (by 2020), when most targets were set for the year 2030. The linkages between access to digital technologies and sustainable development is further stressed under Goal 17 "Revitalize the Global Partnership for Sustainable Development", which calls for increased cooperation on access to technology and innovation as the basis for achieving the goals (Target 17.6).

37. The negative impacts of shutdowns also extend to the economy, with countries losing millions in revenue when both large-scale and targeted shutdowns are implemented,[74] directly hindering the 2030 Agenda's Goal 8 on the promotion of sustained, inclusive, sustainable economic growth.

38. Moreover, shutdowns contravene commitments to promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable, and inclusive institutions at all levels. Most directly, shutdowns threaten achievement of Target 16.10, which calls for ensuring "public access to information and

[68] BGD 2/2019.

[69] See www.thenewhumanitarian.org/2020/03/10/rohingya-refugees-internet-ban-bangladesh.

[70] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26115&LangID=E.

[71] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25222&LangID=E.

[72] IRN 17/2019. See also, ARTICLE19, "Tightening the Net 2020: After Blood and Shutdowns", (September 2020).

[73] SDN 1/2019. See also www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24689&LangID=E.

[74] Center for Technology and Innovation at Brookings Institute, Internet shutdowns cost countries $2.4 billion last year (October 2016); CIPESA, A Framework for Calculating the Economic Impact of Internet Disruptions in Sub-Saharan Africa (2017).

protect[ing] fundamental freedoms, in accordance with national legislation and international agreements." Shutdowns also risk a country's stability and peace, owing to heightened tensions from unaddressed grievances and demands from individuals and groups who are unable to channel them appropriately. This mandate has consistently maintained that systematic political repression of marginalized individuals, as well as of the organizations, movements and networks that represent them generates a considerable risk of violence. Suppressing opportunities for people to peacefully assemble and express their needs and aspirations "only opens up a less desirable avenue, one of violent resistance", an eventuality that would undermine sustainable development and directly affect achievement of Sustainable Development Goal 16.[75]

39. The COVID-19 pandemic has undeniably exacerbated these impacts and concerns. Despite several calls to States to end or refrain from imposing internet shutdowns during the pandemic, many shutdowns continued to take place, effectively impeding people's ability to access essential services necessary for education, work, health, and social connection, and thereby causing increased anxiety and fear. Shutdowns also heightened the risks of joining peaceful assemblies, as many countries respond to the pandemic with a national militaristic approach and enforce restrictions to movement and gatherings with excessive force and harsh penalties.

40. The harmful human rights and development impacts of internet shutdowns are further magnified whenever these measures are imposed on marginalized communities. The shutdown imposed on Rohingya living in refugee camps in Bangladesh, for example, added suffering to their already precarious refugee life. Without internet access and mobile phones, refugees lost the most important spaces and tools they had to access health, education and maintaining family and social connections. Children living in the camps suffered disproportionately. The shutdown deprived nearly 400,000 school-aged children in the camps of the only available tool for education.[76] The Special Rapporteur expressed alarm at the fact that the internet shutdown remained in place even as COVID-19 reached the refugee camps in Bangladesh, and strict lockdowns were imposed. This prevented Rohingya refugees from accessing and disseminating health information critical to protect themselves, their families, and their community against the coronavirus.

IV. Path Forward: Ending Shutdowns

41. The growing scale and intensity of internet shutdowns relating to peaceful assemblies emphasizes the need for strong action by all stakeholders. In this section, the Special Rapporteur proposes a set of actions to be taken by States, companies, international institutions, and other relevant actors to ensure that applicable international human rights norms and standards can be effectively implemented and provide greater protection for the right to peaceful assembly in the digital era. These actions have been developed with reference to existing challenges and promising practices.

A. States

1. Establish a legal prohibition against internet shutdowns

42. The Special Rapporteur has stressed that existing legal frameworks addressing the internet or digital communications either contradict international human rights standards or include weak protections for the right to peaceful assembly.[77] In particular, laws fail to deal adequately with the threat of internet shutdowns during peaceful assemblies or simply facilitate the use of shutdowns. The Special Rapporteur has found that in most States, internet shutdowns have no basis in law, but are nevertheless imposed. Other States argue that shutdowns are legitimately imposed under the ambit of vague and broadly drafted

[75] A/74/349, para 30 and A/HRC/32/36/Add.2, para. 10.

[76] See Athan, Kintha, Rohingya Youth Association, "Lockdown and Shutdown: Exposing the Impacts of Recent Network Disruptions in Myanmar and Bangladesh", (2020).

[77] A/HRC/41/41.

telecommunications legislation, which have been interpreted to grant unfettered power to authorities to impose shutdowns.[78] Many of the laws grant wide powers to employ shutdowns under vague and unspecified notions of "national security" or "national emergency,"[79] often giving national intelligence agencies the authority to order internet shutdowns. At the same time, new laws are being adopted, that would effectively provide government authorities with *carte blanche* to impose shutdowns, including during peaceful protests.

43. States should amend or repeal these laws and instead enact legislation prohibiting internet shutdowns and punishing the adoption of shutdowns. Any new legislation should fully incorporate international human rights norms and standards and to ensure the effective implementation of the prohibition against shutdowns. To this end, national laws should:

(a) Recognize access to the internet as a legal or constitutional right. Several countries have moved in this direction. For instance, the 2001 amendment to Greece's Constitution provides that "all persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as its production, exchange, and diffusion, constitute an obligation of the State" (Article 5A). The Constitutional Court of France and the Supreme Court of Costa Rica have ruled that access to internet is a fundamental right. In Finland, the 2010 Communications Market Act declares a legal right to broadband for all citizens, by including broadband as basic communications services along with telephone or postal services.

(b) Require that education and information programs regarding the prohibition against shutdowns are fully included in the training of public officials, including law enforcement and military personnel and other authorities who may be involved in the management of peaceful protests and the administration of the information and communications technology sector.

(c) Establish independent oversight mechanisms. Given the capacity of States to implement internet shutdowns without transparency or acknowledgement, national laws should establish monitoring and reporting mechanisms. As mentioned earlier, in most instances, State officials do not provide any rationale or public information about the blackouts, deny information when requested, or claim that the shutdown is the result of technical problems or caused by foreign intervention/attack without providing any evidence to support those claims. Any network disruption should be subject to detailed reports that are publicly accessible. These reports should detail the precise nature and causes of the disruptions and assess legal compliance. Civil society organizations should be granted access to data to independently verify the findings of these reports.

(d) Require that the legal prohibition against shutdowns and human rights due diligence obligations are embedded in contracts or licensing agreements with digital technology companies, including telecommunications companies and internet service providers. This includes ensuring that companies operating in the country have an obligation to inform internet users of any unlawful disruptions and to seek remedy in courts. For State-run companies, the legal prohibition against shutdown should be clearly laid down in law and policy, with the expectation not only to refrain from implementing shutdowns but also to serve as role models in the sector.[80]

44. While many governments shut down the internet for manifestly illegitimate reasons, the Special Rapporteur recognizes that States may have disrupted networks under the misconception that the measure may help address a particular public order or public safety concern during assemblies. In particular, the Special Rapporteur recognizes that the existing challenges in tackling disinformation and hate speech online may lead some governments to consider drastic measures. Laws and policies addressing hate speech or online disinformation should be in place, including ensuring effective collaboration from social media and content platforms. However, these laws cannot justify internet shutdowns, which are disproportionate

[78] See, for instance, Sections 5(1) and 56 of the Uganda Communications Act of 2013 and Russia's Communications Act of 2003.

[79] See, for instance, Ecuador's 2015 Organic Law of Telecommunications and Bangladesh Telecommunications Act of 2001.

[80] A/HRC/32/45.

by default, and should strictly adhere to international human rights principles and standards, including those concerning the right to freedom of expression, as laid down by the mandate of the Special Rapporteur on the right to freedom of opinion and expression.

2. Provide effective remedies

45. In general, existing national legislation addressing digital technologies or telecommunications in most countries does not provide accountability for human rights violations or contain provisions on any forms of remedy for victims of internet shutdowns. To ensure effective implementation of the prohibition of shutdowns, the legal system must ensure that victims of shutdowns can obtain redress and exercise an enforceable right to a remedy.

46. In recent years, national judicial systems have been called upon to ensure accountability for network shutdowns and their human rights implications. There are many positive developments in this field. Some national courts have recognized that internet shutdowns constitute a human rights violation. The Indian Supreme Court, while addressing the months' long internet shutdown in Kashmir, for example, held that the indefinite imposition of internet shutdowns is unconstitutional and that internet shutdowns cannot be ordered to suppress dissent. In Indonesia, the Jakarta State Administrative Court declared that the internet shutdowns implemented in 2019 in Papua and West Papua was illegal. In Sudan, a court ordered telecommunication companies to end a shutdown imposed during peaceful protests in 2019 and restore internet access in the country.

47. The Special Rapporteur strongly believes that courts could play an important role in addressing the threat of shutdowns. However, many challenges remain. Civil society groups consulted in preparation for this report asserted that accountability for the implementation of internet shutdowns remains extremely difficult and that cases brought are often slow-moving and subject to delay. When courts do issue decisions, they do not fully incorporate international human rights law considerations, including those related to freedom of assembly. Most importantly, courts are failing to provide effective remedies to redress victims or prevent repetition. National laws should, for instance, ensure that courts can issue more timely injunctions against shutdowns in progress. They should also ensure that courts can access technical information about shutdowns from relevant authorities, including from national security or intelligence officers, and receive and evaluate as evidence the forensic analysis of technical experts.

48. In cases where internet shutdowns have facilitated large-scale violations in the context of peaceful assemblies, effective accountability mechanisms should be ensured. This includes the establishment of a comprehensive, independent commission of inquiry, including independent representatives of civil society, with a mandate to conduct fact-finding as well as to make recommendations for systemic reform.

3. Develop a national action plan to ensure human rights are respected in the context of peaceful protests

49. The Special Rapporteur has stressed that protecting national security, public order and public safety are not incompatible with the full exercise of the right to peaceful assembly. Where legitimate concerns are raised, States should identify best practices in addressing them, implementing measures that are compatible with their international human rights obligations. There are many alternative measures to internet shutdowns. Mediation or negotiation are key techniques to be employed to address tensions that arise in the course of assemblies, before resorting to any other option. The UN Human Rights Council has affirmed that "peaceful protests should not be viewed as a threat" and encouraged all States to engage in "an open, inclusive and meaningful dialogue when dealing with peaceful protests and their causes".[81]

50. In a joint report on the proper management of assemblies, this mandate and that on extrajudicial, summary, or arbitrary executions, insisted that States should develop, enact, and update a national action plan to guide the implementation of the international standards

[81] Human Rights Council resolution 25/38 of 11 April 2014.

relevant to the management of assemblies.[82] The Special Rapporteur reiterates this call and urges States to ensure these national action plans reflect the principles and standards set out by the Human Rights Committee in its newly adopted General Comment 37 on the right to peaceful assembly. This includes establishing an explicit prohibition against the use of shutdowns as a means to manage assemblies and requiring instead that authorities always attempt to engage with assembly organizers and/or participants of assemblies, address substantive demands and engage in genuine dialogue with peaceful protesters.

4. Strengthen state leadership against shutdowns

51. Many States have shown a commitment to condemn internet shutdowns and explore ways to leverage diplomatic engagements to encourage other States to refrain from imposing internet shutdowns. Notably, the Freedom Online Coalition - a multilateral coalition of 30 governments that collaborate to advance Internet freedom worldwide – has issued several joint statements on state sponsored network disruptions and defending civic space online, including recommendations to States seeking to develop effective, human rights-respecting laws, legislation, and regulations designed to protect human rights online.

52. The Special Rapporteur echoes the calls made by the Freedom Online Coalition. States should strengthen efforts to raise issues of internet shutdowns, including their economic, social, and political impacts, in diplomatic activities, such as bilateral and multilateral engagements and negotiations. States should issue public statements when shutdowns in relation to peaceful protests are recorded and coordinate through embassies in the countries where such shutdowns are taking place to jointly urge governments to refrain from and cease such measures.[83]

53. Donor States should also strengthen their support to civil society so that they can continue and scale up efforts to track the impact of internet shutdowns. These efforts have played a key role in bringing visibility to internet shutdowns, including their scope, duration, and impact, as well as in advocating for more accountability and transparency around this issue, including by using litigation. More support to civil society to improve access and use of network measurement tools and other tracking skills is also needed.

B. Companies

1. Scale up good business practices in addressing internet shutdowns

54. On the path to ending shutdowns, actions by telecommunications companies and internet providers are essential. The Special Rapporteur recognizes that telecommunications companies and internet providers operate within a framework of laws and government practices that may limit their capacity to prevent shutdowns from taking place. These companies operate under considerable business pressure, and in some cases, laws or licensing agreements might prevent them from disclosing information about shutdowns. Moreover, workers of these companies are at risk of violence, arrest, and intimidation in the event of non-compliance with shutdown orders.[84] The military-ordered shutdown in Myanmar, for example, was reportedly executed by armed military forces who raided the data centers of internet providers.

55. Yet telecommunications providers' human rights responsibilities apply fully despite these constraints. These companies need to take internet shutdowns seriously push back against these measures, help mitigate their impacts and ensure accountability. A small number of telecommunications providers are showing evidence of moving in that direction. According to data collected by the organization Ranking Digital Rights, only a few companies disclose information about the circumstances under which they may shut down the network, the demands they receive, and actions to push back on or mitigate the effects of government orders.[85] A positive recent development is Africa's MTN, which carried out

[82] A/HRC/31/66, para. 17.
[83] Freedom Online Coalition, Joint Statement on State Sponsored Network Disruptions, 2017.
[84] HRC/35/21, para 31.
[85] See www.rankingdigitalrights.org/index2020/indicators/F10.

internet shutdowns in several countries in the region. The company committed to push back against such orders and notify users when carrying out shutdowns.[86] These efforts need to be replicated and scaled up.

56. The Special Rapporteur recognizes that as States increase the scale and intensity of shutdowns, the pressure on companies seeking transparency also increases. For example, foreign-based companies that operate in Myanmar- were reportedly barred from disclosing the military junta's directives they received ordering shutdowns.

57. The mandate of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has asserted that even if "companies are prohibited from disclosing the origin or basis of a shutdown request, they should nevertheless seek to provide regular updates about the services affected or restored, the steps they are taking to address the issue and explanations after the fact. Innovative transparency measures, such as the publication of aggregate data and the selective withholding of information."[87] Companies facing these difficult situations should also cooperate with civil society in challenging unlawful orders, using all available tools of law and policy, in procedure and practice, including litigation. These companies can also help preserve evidence of orders or threats to disrupt networks, and document the impacts of shutdowns, in order to inform efforts at accountability and redress. As a preventing measure, companies should engage regulators when initiating a business relationship and push back against licensing conditions (and laws governing the telecommunication sector) that allow for shutdowns.

58. Social media platforms also have an important role to play to ensure respect for people's rights in the event of an internet shutdown. These companies, for example, should be more proactive in disclosing information about outages and disruptions they see in traffic flows, with or without attribution. These companies can also work with civil society groups and the technical community and take measures to help users circumvent blocking of their applications and be better prepared when shutdowns happen.

59. Another important business actor in preventing and addressing shutdowns are the companies that sell or provide governments with the hardware, software and services that support internet and telecommunications networks. The products and activities of these companies can facilitate internet shutdowns. For example, civil society organizations consulted in preparation for this report indicated that the Deep Packet Inspection (DPI) equipment used by Belarus to implement shutdowns during the 2020 election protests was provided by a company based in the United States. After advocacy by human rights groups and calls by members of Congress of the United States, the company ended its contract with the Belarusian government, explaining that actions by the Government of Belarus constituted a human rights violation and it has triggered the automatic termination of our end user license agreement.

2. Leverage investors' human rights due diligence to prevent and mitigate shutdowns

60. Investors, as business actors, have a responsibility to respect human rights in line with the UN Guiding Principles on Business in Human Rights. Investors need to know the human rights risks connected with their investment activities and understand how they can take action to manage those risks. Investors in digital technology companies, including telecommunications companies, are uniquely placed to facilitate and incentivize these companies to prevent, mitigate and address internet shutdowns. However, the involvement of investors in preventing and promoting due diligence on internet shutdowns remains exceptional. To address the rising threat of shutdowns, the exercise of human right due diligence by investors needs to become a new normal.

61. As first step, investors should publicly communicate their expectation that companies they invest in have in place policy commitments, due diligence processes, and effective transparency mechanisms addressing internet shutdowns, including measures to challenge internet shutdowns, as appropriate. To ensure this expectation is met, investors should closely

[86] See www.rankingdigitalrights.org/index2020/key-findings.

[87] A/HRC/35/22, para 71.

examine whether a company's current policies, financial disclosure and legal accountability mechanisms are sufficient to protect human rights, including the right to peaceful assembly, in the face of internet shutdowns. This involves requesting the company's transparency reports on shutdowns incidents and providing financial backing for large-scale lawsuits challenging shutdown requests or non-disclosure measures. Efforts to promote multistakeholder collaboration between investors, companies, academia, and civil society to identify better ways to respond to shutdowns should also be supported by investors.

C. The United Nations and international institutions

1. Address implementation gaps and ensure international human rights accountability

62. International and regional human rights mechanisms have unequivocally condemned internet shutdowns as a violation of international human rights law and called upon all States to refrain from and cease such measures. The Special Rapporteur believes international human rights institutions should continue to urge states that are deliberately denying people access to the internet and communications, particularly in the context of peaceful assemblies, to keep the internet on.

63. At the same time, there is an urgent need to move beyond condemnation and strengthen cooperation and implementation measures to end shutdowns. The Human Rights Council, for example, should ensure the Universal Periodic Review examines the use of shutdowns by all United Nations Member States and advocates more strategically against shutdowns in relation to peaceful protests. To ensure the legitimacy to this work, the Human Rights Council should promote and consider voluntary state pledges to fully respect, protect and fulfil digital rights as a positive factor when electing its member States. This is in line with state pledges to uphold the highest standards in the promotion and protection of human rights, already required by UN General Assembly (UNGA) resolution 60/251. States that impose internet shutdowns manifestly fail to fulfil the Council membership standards set forth in this resolution and should report to the Council any shutdowns occurring in their jurisdiction. Other bodies where such pledges should be affirmed include regional bodies, and multilateral entities like the Open Government Partnership and International Telecommunications Union, and thematic forums like the Internet Governance Forum and WSIS Forum. Entities such as the United Nations Office of the High Commissioner for Human Rights, and its regional and field offices, should identify best practices and build capacities among states to monitor, prevent, and mitigate internet shutdowns in their own territories and abroad.

64. International accountability should also be promoted. The ECOWAS ruling on the shutdown during peaceful protests in 2017 in Togo is an important example of how regional courts and treaty body mechanisms can ensure compliance with the human rights norms and standards outlined in this report and counter impunity. Ad hoc accountability mechanisms, such as United Nations mandated commissions of inquiry, fact-finding missions, and investigations, should be used to respond to situations where protest-related shutdowns have facilitated the commission of serious human rights violations.

2. Ensure coherence between ITU norms and practices and human rights norms and principles

65. Some States have invoked the Constitution of the International Telecommunication Union (ITU), the United Nations specialized agency for information and communication technologies, to provide legal authority for shutdowns. The Special Rapporteur observes that the ITU Constitution, adopted in 1992, has been interpreted by some actors so as to provide States with authority to cut off the internet. Article 34, for example, provides that States can cut off telecommunications services when it "may appear dangerous to the security of the State or contrary to its laws, to public order or to decency." Article 35 further indicates that "Each Member State reserves the right to suspend the international telecommunication service, either generally or only for certain relations and/or for certain kinds of correspondence, outgoing, incoming or in transit, provided that it immediately notifies such action to each of the other Member States through the Secretary-General."

66. Such an interpretation contravenes the human rights norms and standards outlined in section II of this report and the ITU's own values and commitments. The United Nations Secretary General recognized in his Roadmap to Digital Cooperation the need for greater coherence throughout the United Nations system, including by recognizing that "human rights exist online as they do offline and have to be respected in full."[88]

67. The ITU legal regime on suspension of telecommunications, which predates the digital era, is ill-suited to prevent misuse by Governments and address the threats that internet shutdowns pose to human rights, including the rights to freedom of expression and peaceful assembly. ITU norms and processes lack guidelines or enforcement measures that would help prevent the human rights violations caused by these extreme measures. Even if notification to ITU is required per article 35 of the ITU Constitution, this cannot be equated with effective oversight. Article 34 of the ITU Constitution is particularly troubling as it could be interpreted to authorize internet shutdowns, including on a broad and indiscriminate basis. To prevent this undesirable outcome, the ITU should issue guidance clarifying that these provisions should never be understood as authorizing internet shutdowns and foster collaboration between States, Internet service providers (ISPs), mobile telephony operators and civil society groups to promote policies and practices to prevent network disruptions, in line with human rights norms and principles, including the United Nations Guiding Principles on Business and Human Rights (UNGPs).

V. Conclusions and Recommendations

68. States have obligations under international human rights law to ensure that everyone within their jurisdiction is able to access and use the internet to exercise his or her right to peaceful assembly. Those obligations include refraining from imposing internet shutdowns and ensuring that the internet remains open, accessible, and secure at all times.

69. Yet States continue to ignore these obligations and impose internet shutdowns to impede peaceful protests and punish collective action, while facilitating other human rights abuses. Ending shutdowns has become a human rights imperative both to allow people to exercise their rights online and offline and to safeguard democratic governance in the digital era. To this end, the Special Rapporteur calls upon States, international institutions, businesses, and other stakeholders to commit themselves to end internet shutdowns including in relation to peaceful protests and, in the context of elections. The Special Rapporteur proposes the following recommendations as steps towards realizing this goal.

70. The Special Rapporteur recommends States to:

- Recognize the right to access and use the internet as a constitutional and legal right and as an essential condition for the exercise of the right to freedom of peaceful assembly.
- Expand initiatives to provide universal and affordable internet access.
- Refrain from shutting down, throttling, or blocking the internet, and make a state pledge to refrain from imposing any unlawful restrictions on internet access and telecommunication in the future, particularly in upcoming elections and protests, and amid the COVID-19 pandemic.
- Repeal and amend any laws and policies that allow for internet shutdowns and enact legislation prohibiting and punishing these measures.
- Fulfil international obligation to guarantee the right to equality and non-discrimination and refrain from restricting freedom of peaceful assembly online and offline that specifically targets vulnerable groups.
- Ensure that the internet, including social media and other digital communication platforms, remains open, accessible, and secure. States should specifically: (i) order internet service providers operating in their country to provide

[88] A/74/821, para 38.

everyone with universal, affordable, high-quality, secure, and unrestricted internet access throughout election periods, protests and thereafter; (ii) refrain from pressuring technology companies, internet service providers or other telecommunications companies to moderate content online in contravention of human rights norms and standards and ensure their compliance with their responsibilities to respect and protect human rights in line with the UN Guiding Principles on Business and Human Rights; (iii) guarantee the safety of technical workers building and maintaining critical infrastructure networks, while ensuring sites are protected, and iv) promote and protect strong encryption, including by adopting laws, regulations and policies in line with international human rights norms and standards.

- Improve foreign policy alignment by issuing specific guidance against shutdowns to embassies, systematically integrating the issue into diplomatic training and senior leadership briefings, designating a senior official to spearhead interagency coordination on this issue.

- Increase financial and political support to civil society groups and human rights defenders working to monitor and advocate against internet shutdowns, as well as those civil society organizations developing legal and technological solutions to shutdowns.

71. The Special Rapporteur recommends digital technology companies, including telecommunication providers and digital communications platforms, to:

- Develop and make publicly available policies that specifically state their position against internet shutdowns and how they address any shutdown orders from governments, in compliance with the Guiding Principles.

- Prepare for a range of threats to the rights of users, particularly where bandwidth is overwhelmed and congested as a result of large demonstrations and ensure that the company deploys extra capacity throughout the events.

- Challenge censorship and service limitation requests from states, using all available tools of law and policy, in procedure and practice. Notify affected users and the public of any such requests and any orders implemented, early and often, both in real time and in regular transparency reports.

- Reach out to peer companies and other stakeholders in advance of potential censorship events and demonstrations and protests. Establish response plans and channels of communication with government actors and civil society.

- Preserve evidence of orders or threats to disrupt networks, and document the impacts of shutdowns, in order to inform later efforts at accountability and redress.

- Require regulators (or Government officials and bodies who issue shutdown orders, such as ministers or security agencies) to provide a formal, written, justification for the shutdown, including citing the specific laws and provisions under which they are issued and the situation that warranted invoking the disruption.

- Improve transparency reporting, including documenting government directives for internet disruptions. Companies should insist on written instructions and orders from authorities, and promptly make these orders public.

- Provide timely and transparent guidance to users to identify disruptions likely to impact the quality of service they receive.

- Expand their partnerships and engagement with civil society and join key platforms that aim to collaboratively advance a free and open internet.

- Engage regulators and push back against licensing conditions (and laws governing the telecommunications sectors) that allow for shutdowns.

- Challenge shutdowns before national, regional, and international mechanisms for accountability and compensation of losses incurred.

72. The Special Rapporteur recommends investors to:

- Request a company's transparency reports that include statistics and information on i) government and private party demands for access to user data; ii) takedown or restriction of content or accounts, including information on internet shutdowns; and iii) clear explanation of corporate processes and policies responding to these requests and incidents.

- Encourage companies to appoint a member or committee from the Board of Directors to be responsible for policies and related risk management on internet shutdowns (including but not limited to policies and practices developed when entering a national market, and a clear understanding of the laws in those markets that might lead to a shutdown request).

- Ensure companies have a clear policy development process for operational decision making relating to entering and operating in countries where governments may request the disruption of services. This policy should make clear the conditions in which a company will operate in a country, demonstrate an understanding of the risks in that country, and outline how it will respond to a request by the government to suspend services, including disclosure to customers.

- Encourage companies to publish transparency reports, to the extent legally possible, that list the countries in which they operate, and clarify in which countries they have received requests for service shutdown or monitoring.

- Support a company's efforts to use litigation to challenge shutdown requests or non-disclosure measures.

73. The Special Rapporteur recommends the United Nations and international institutions to:

- Urge states that are deliberately denying people access to the internet and communications, particularly in the context of assemblies, to keep the internet on.

- Foster multi-stakeholder engagement to systematically monitor, document, and report on network disruptions, in line with human rights norms and principles, including the United Nations Guiding Principles on Business and Human Rights (UNGPs).

- Identify best practices and build capacities among states to monitor, prevent, and mitigate internet shutdowns in their own territories and abroad.

- Hold states accountable when they impose internet shutdowns in relation to peaceful protests, and provide for effective remedies including non-repetition measures.

- Ensure coherence between norms and practices adopted United Nations agencies and entities, such as the International Telecommunications Union, with human rights norms and principles.

- Enhance the role of the Office of the United Nations Secretary General's Envoy on Technology, to guide and measure progress of these recommendations.