Main Submitter: South Africa
Co-submitters: Ecuador
Signatories: Spain, Ecuador, Egypt, USA, Pol, and Bangladesh, Indonesia, Saudi Arabia, Haiti, Philippines
Topic: Examining the use of internet shutdowns as tools of political repression in authoritarian regimes

The Republic of South Africa,

Deeply concerned by the increasing use of government-imposed internet shutdowns to suppress political opposition, restrict freedom of expression, and interfere with democratic processes,

Recalling Articles 19, 21, and 25 of the International Covenant on Civil and Political Rights (ICCPR), which protect freedom of expression, peaceful assembly, and participation in public affairs,

Recognizing the importance of maintaining internet connectivity during elections, peaceful demonstrations, and periods of political instability to ensure transparency and democratic participation,

Alarmed by the humanitarian consequences of widespread internet restrictions, particularly their impact on access to healthcare, emergency services, education, and essential communication systems,

Emphasizing the responsibility of Member States to protect national security while ensuring that any restrictions on internet connectivity comply with the principles of legality, necessity, and proportionality,

Acknowledging the importance of international cooperation between governments, telecommunications providers, and human rights organizations in preventing politically motivated internet disruptions,

Bearing in mind the fundamental principle of national sovereignty while recognizing that national security concerns must not be used to justify violations of internationally recognized human rights,

Convinced that strengthening independent judicial oversight, government transparency, and international monitoring mechanisms is essential to preventing the misuse of internet shutdowns and protecting civilian populations,

1. *Calls upon* all Member States to adopt and enforce comprehensive national legal frameworks regulating government-ordered internet shutdowns, ensuring that any restriction on digital connectivity is consistent with international human rights obligations, particularly Articles 19, 21 and 25 of the International Covenant on Civil and Political Rights (ICCPR), through:

a. Requiring all proposed internet restrictions to satisfy the internationally recognised principles of legality, necessity and proportionality, including, i. Establishing a clearly defined legal basis identifying the specific circumstances under which connectivity may be restricted, and
ii. Demonstrating an immediate and legitimate threat to public safety or national security rather than relying on vague claims of political instability, and
iii. Ensuring that restrictions are limited to the minimum geographical area, population and duration strictly necessary to address the identified threat,

b. Introducing independent judicial oversight of government shutdown orders, including:
i. Requiring prior authorisation from a competent judicial authority wherever reasonably practicable, and
ii. Mandating prompt judicial review of emergency restrictions and their continued necessity, and
iii. Providing affected individuals and organisations with accessible procedures to challenge restrictions they believe to be unlawful,

c. Requiring governments to publish publicly accessible explanations of imposed restrictions, including their legal justification, expected duration and geographical scope, while protecting genuinely sensitive security information;

2. *Recommends* the strengthening of international monitoring of internet shutdowns through an OHCHR-coordinated Digital Connectivity and Human Rights Monitoring Initiative, operating in cooperation with existing UN human rights mechanisms and independent civil society organisations, with the mandate to:

a. Establish a centralised reporting framework documenting government-imposed internet disruptions, including:
i. The date, duration, geographical coverage and technical nature of each reported restriction, and
ii. The governmental authority responsible and the publicly stated justification for the measure, and
iii. The documented consequences for freedom of expression, peaceful assembly, access to information and essential civilian services,

b. Encourage Member States to submit voluntary periodic reports concerning national internet restrictions, including:
i. The domestic legislation governing shutdown authorisations, and
ii. The judicial and administrative oversight procedures applied, and
iii. The measures undertaken to prevent politically motivated or discriminatory restrictions,

c. Present findings to the Human Rights Council through periodic assessments that:
i. Identify recurring patterns of restrictions coinciding with elections, demonstrations or periods of political instability, and
ii. Highlight states demonstrating effective safeguards and transparent

governance, and
iii. Recommend specific legal and institutional reforms to address identified violations;

3. *Urges* Member States to strengthen the protection of journalists, independent media organisations, human rights defenders and civil society representatives against digital censorship and restrictions intended to obstruct the documentation of human rights violations, through:
    a. Establishing national safeguards protecting lawful journalistic activity during periods of political instability, including:
        i. Prohibiting restrictions specifically intended to prevent the reporting of government misconduct or peaceful political opposition, and
        ii. Protecting journalists from intimidation, arbitrary detention and retaliation for publishing information of legitimate public interest,
        iii. Ensuring that restrictions on digital platforms are subject to independent legal review,
    b. Supporting independent journalism and public access to reliable information through:
        i. Voluntary funding and professional training programmes for independent media organisations, and
        ii. Cooperation with UNESCO to strengthen journalist safety and media freedom, and
        iii. The development of accessible channels through which journalists can report censorship and threats to their professional independence,
    c. Encouraging Member States to cooperate with relevant UN mechanisms when credible allegations arise that internet restrictions have been used to conceal human rights abuses;

4. *Calls upon* Member States to ensure that any legally justified and strictly limited interruption of internet connectivity does not unnecessarily deprive civilian populations of essential public services, recognising the disproportionate humanitarian consequences of widespread digital restrictions, through:
    a. Establishing national emergency connectivity and service-continuity plans that preserve access to:
        i. Emergency response systems, including ambulance, fire and disaster management communications, and
        ii. Hospitals, healthcare providers and humanitarian coordination networks, and
    iii. Essential educational, financial and public-administration services, b. Requiring national telecommunications regulators to cooperate with service providers in developing technically feasible continuity arrangements, including: i. Maintaining dedicated emergency communication channels where technically possible, and
        ii. Establishing clearly defined exemptions for authorised humanitarian

and medical organisations, and
iii. Ensuring that emergency connectivity arrangements remain operational and accessible throughout any restriction,

c. Conducting periodic independent assessments of service-continuity arrangements to:
i. Identify disruptions affecting vulnerable and remote communities, and
ii. Evaluate the effectiveness of existing emergency exemptions, and
iii. Recommend improvements to national digital resilience and civilian protection policies;

5. *Encourages* stronger cooperation between Member States, telecommunications providers and independent regulatory institutions to prevent the misuse of private digital infrastructure for political repression, while recognising the importance of transparent corporate governance and lawful business operations, through:
a. Developing voluntary international transparency standards for telecommunications companies, requiring participating providers to:
i. Publish periodic reports detailing government requests for internet restrictions, and
ii. Disclose the legal basis and general scope of restrictions legally, and
iii. Explain the procedures followed when assessing the legality of government-issued shutdown orders,
b. Encouraging telecommunications providers to establish internal human rights due diligence procedures that:
i. Assess the potential civilian impact of government requests, and
ii. Seek independent legal guidance when the legitimacy of a restriction is disputed, and
iii. Maintain appropriate records of decisions concerning government directed disruptions;
c. Promoting cooperation between national telecommunications regulators and international organisations to:
i. Develop consistent standards for corporate transparency, and
ii. Share non-confidential information concerning patterns of unlawful restrictions, and
iii. Identify opportunities for technical assistance and improved corporate accountability;

6. *Calls* for strengthened international cooperation to prevent internet shutdowns from being used to obstruct the documentation, investigation and reporting of alleged human rights violations, particularly during elections, demonstrations and armed conflicts, through:
a. Supporting independent and impartial documentation initiatives conducted by recognised human rights organisations, including:
i. Recording publicly available information concerning the timing and circumstances of internet restrictions , and
ii. Collecting independently verifiable reports of abuses allegedly occurring

during periods of disrupted connectivity , and
iii. Cooperating with relevant UN investigative mechanisms where credible evidence of violations emerges,

b. Encouraging the preservation of relevant digital evidence in accordance with applicable law and international standards, ensuring:
i. The authenticity and integrity of collected material, and
ii. The confidentiality and protection of witnesses and individuals providing information, and
iii. Secure retention procedures that prevent unauthorised alteration or disclosure of sensitive evidence,

c. Encouraging competent national judicial authorities to investigate credible allegations that internet shutdowns were deliberately used to conceal or facilitate human rights violations, including:
i. Examining the decisions and conduct of officials responsible for authorising restrictions, and
ii. Assessing whether restrictions obstructed lawful investigations or humanitarian reporting, and
iii. Pursuing appropriate legal remedies where individual responsibility is established;

7. *Urges* all Member States to prohibit the deliberate use of internet shutdowns as a means of suppressing political opposition, restricting freedom of expression, or interfering with democratic processes through measures including, but not limited to:

a. Establishing national legislation to prevent governments from restricting internet access in response to peaceful protests, elections, or political criticism,

b. Requiring any proposed internet restriction to be justified under international human rights law and subject to independent judicial oversight in partnership with the UNHRC, c. Ensuring that any lawful restrictions are necessary, temporary, and limited in geographical scope;

8. *Calls upon* the United Nations Human Rights Council (UNHRC), in cooperation with the International Telecommunication Union (ITU), to strengthen international monitoring and documentation of politically motivated internet shutdowns through:

a. Developing a voluntary international reporting framework encouraging Member States to disclose:
i. The reason behind any government-authorized internet restrictions, and
ii. The geographical areas and populations affected, and
iii. The expected duration of the restrictions,

b. Encouraging cooperation between governments, telecommunications providers, and independent human rights organizations to identify and document unjustified internet disruptions,

c. Partnering with private companies to ensure internet coverage and bandwidth priority during critical moments such as, but not limited to:
    i. Elections, and
    ii. Moments of civil unrest,
d. Creating early warning systems for planned internet shutdowns for civilians.