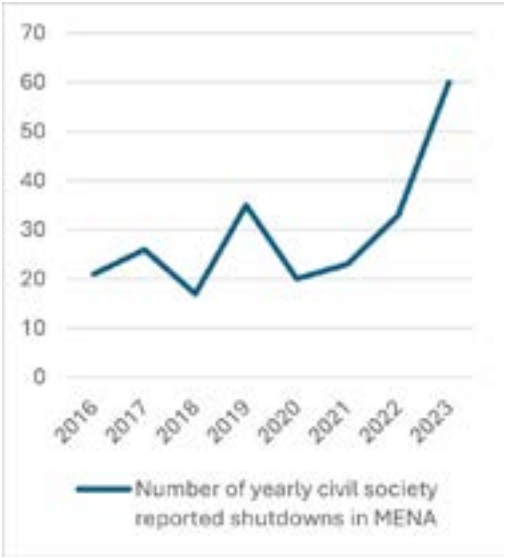
Civic Space Brief

TRENDS IN DIGITAL RIGHTS ACROSS THE MIDDLE EAST AND NORTH AFRICA (MENA) REGION: INTERNET SHUTDOWNS AND INTERFERENCES WITH NETWORK

Internet shutdowns – 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 – are becoming more frequent globally, including in the Middle East and North Africa (MENA) region. Since civil society began reporting data on shutdowns in 2016, the MENA region has experienced a steady increase (see graph). By May 2024, at least 235 shutdowns had been documented in the region for the period from January 2016 to December 2023, contributing to a global total of 1,458 shutdowns across 81 countries.



I. Trends of shutdowns

Shutdowns in the MENA region, much like global trends, have not only increased but also evolved in terms of tactics and complexity. Initially characterized by full network blackouts, they have evolved to increasingly include a mix of tactics, such as bandwidth throttling and targeted blockages of specific services, such as social media applications, Voice over Internet Protocol (VoIP), and phone calls and short messaging service (SMS). Attacks on network infrastructure to shut down connectivity have also been recorded in situations of conflict.

The ability of governments to impose shutdowns is closely linked to national internet infrastructure, where key factors include ownership or control over submarine optical cables, international gateways, national backbones, and telecommunications companies and Internet Service Providers (ISPs). In many countries in the region, governments maintain significant control and ownership over network operators and infrastructure. Governments can also control connectivity by imposing various limitations on telecommunications companies. For example, in Gaza companies have been restricted to coverage at 2G level, which offers far slower connection and poor encryption, as opposed to the modern and widespread use of 3G technology across the region.

II. Contexts of shutdowns

Shutdowns in the MENA region are often implemented during periods of political significance and armed conflict. According to civil society data, nearly half of the shutdowns recorded in the region between 2016 and 2023 coincided with armed conflict and periods of heightened political activity, including elections and protests — precisely when access to information is most critical for public safety and accountability. Shutdowns have far-reaching consequences on a host of human rights, isolating communities, disrupting communication, and exacerbating insecurity and violence while impeding humanitarian efforts.

A number of disruptions in MENA also took place during periods of school examinations, being justified as a measure to prevent cheating. However, evidence suggests that shutdowns have limited success in achieving that goal, and fail to tackle concurrent negative impacts on economic, social, and political activities, particularly where some shutdowns extend beyond examination periods.

III. Impacts of shutdowns

Shutdowns often result in widespread and disproportionate collateral rights violations, due to the blunt and blanket nature of imposition of such restrictions. In many cases governments impose shutdowns without an official announcement or reference to a legal basis. To the extent that governments do offer justification for interferences with access to the internet and mobile services they often point to the need to maintain national security and public order. Notwithstanding, shutdowns inevitably impact on a vast range of legitimate activities within an affected community, and is a disproportionate means to achieve what may otherwise be a legitimate objective.

Shutting down access to the internet and mobile communications most immediately impacts on the rights to freedom of expression, association and access to information of individuals – pertinently in situations of instability and conflict when people require connection with family, friends and networks the most. Also, shutdowns hinder – or even render impossible – communications of journalists, civil society actors, protection networks, human rights monitors and humanitarian service providers who exercise crucial functions in monitoring, reporting on and responding to human rights violations on the ground. In some instances, shutdowns may even be deliberately imposed to shroud and obscure violations and inhibit media freedoms.

Due to the central role of communications in facilitating one's life and accessing basic needs, shutdowns also indiscriminately undermine many other rights. These include for example: the right to health, when individuals cannot reach healthcare services or access life-saving information; the right to education, when people are unable to access educational institutions or materials; the right to security of person, where victims of physical attacks cannot call for help; the rights to work and an adequate standard of living, where office communications, banking services and, particularly for gig workers, service provider apps and mobile services are inaccessible; and the right to social and economic development, when these daily, personal incumbrances are extrapolated to the societal level.

These violations are exacerbated in situations of armed conflict – impeding connection with family, friends and networks when it is needed the most to receive news on attacks and orders impacting people's movement, and to check on loved ones, coordinate escape or request for help, but also limiting access to health care, which is critical during conflict. In conflict situations, reports have revealed intentional targeting of telecommunications infrastructure, resources and staff as a method of warfare to limit movement, obscure violations and accentuate confusion within communities.

IV. Moving forward

Key asks:

1) States Should Refrain from Implementing Shutdowns

Given their well-documented significant negative impact on human rights, economic activity, and security, questions are raised about why shutdowns remain frequent and how societies can better prevent and respond to these events. To address this, States should prioritize internet access and connectivity as a fundamental human right, refrain from imposing shutdowns, and remove the multiple obstacles that limit communication. States should also repeal any laws or policies that allow for ordering of blanket shutdowns and review laws or policies enabling interferences with internet access and connectivity, including cybercrime laws, to ensure they adhere strictly to the principles of legality, necessity, proportionality and legitimate aim.

2) All Actors Should Prevent and Respond to Shutdowns

Multiple stakeholders can contribute towards increased internet access and connectivity by preventing and responding to shutdowns, e.g. through proactive engagement with authorities before disruptions are likely to occur (for example, in the run up to elections and protests) and by collaborating with internet/ telecommunications service providers, local civil society and protection networks to develop strategies for effective responses if shutdowns are implemented.
Focusing on enhancing the capacity of national actors and institutions to challenge the legality of these shutdowns and on improving digital literacy and providing access to circumvention tools, such as virtual private networks (VPNs) and mesh networks, which help people to stay connected during disruptions, would lead to improved responses. Additionally documenting, reporting and litigating these disruptions are vital to ensure accountability.

Civil society organizations are key players in responding to shutdowns, while international organizations should ensure that all development cooperation aimed at expanding connectivity includes safeguards against shutdowns and support access to circumvention tools.
Despite these efforts, scaling and sustaining these initiatives amid increasing shutdowns in the region remains a challenge, with the need to explore how cooperation between civil society, international organizations, and private sector actors can be expanded to prevent shutdowns and build more resilient digital systems that enable communities to withstand and circumvent these disruptions.

3) Companies' Responsibility to Respect Human Rights

Telecommunications companies and internet service providers, under the UN Guiding Principles on Business and Human Rights (UNGPs), have a responsibility to respect human rights. This includes conducting due diligence to assess the impact of shutdowns and providing grievance mechanisms that are accessible, equitable, and rights-compatible.

Furthermore, companies should take all lawful measures to challenge government requests, inform the public about disruptions, and provide regular updates on efforts to restore communications. They should also conduct human rights assessments when entering or renewing license agreements. Yet, there is limited transparency from companies regarding shutdown requests and how or if they challenge them, raising important questions regarding how to ensure increased adherence to their human rights responsibilities in the region.

4) Building More Resilient Systems

International and local organizations, researchers, and companies have forged alliances aimed at mapping risk factors, identifying early warning signs, and devising mitigation strategies against shutdowns. These efforts promote circumvention tools like VPNs and mesh networks, and support decentralized communication models, and enhance resilience. Continued support for these initiatives is essential, along with improved coordination among communities, civil society organizations, lawyers, and companies during periods of heightened risks of shutdowns. This collaboration fosters timely information exchange and effective mitigation measures.

Building resilient systems also requires a re-evaluation of how internet access is measured. Traditional metrics often overlook the quality and openness of connections do not capture the lived experiences of users. New measurement initiatives aim to fill these gaps by expanding data collection and refining our understanding of the digital divide.

Development cooperation can bolster resilience by fostering partnerships between financing agencies, States, and the telecommunications industry to reform telecommunication systems and legal and institutional frameworks. Prioritizing human rights safeguards in these projects will help ensure that initiatives benefit users and address human rights risks related to the digital space. Constructive coalitions focused on the Sustainable Development Goals can further support this effort, promoting data collection methods that protect users and enhance our understanding of digital rights and connectivity.