

Between Security and Rights: The Policy Dilemma of Internet Shutdowns

On the evening of 4 August 2019, the Indian government imposed what would become the longest internet shutdown in any democracy. Lasting 18 months, the internet shutdown was enforced across the former state of Jammu and Kashmir, suspending mobile and fixed broadband connectivity, voice calls and messaging services, and isolating 12.5 million people from one another and the rest of the world.¹

The government deemed the shutdown a necessary security measure to maintain public order following the constitutional restructuring of Jammu and Kashmir – historically a volatile, conflict-affected region with persistent cross-border terrorism threats. But for the 2.8 million students in the erstwhile state, the blockade represented a complete educational paralysis.^{2,3} Households reliant on remittances from relatives working overseas faced severe financial hardship. Patients living far away from public health facilities lost the option to consult with doctors online. For the region's economy, it meant more than US\$2.4 billion⁴ in lost revenue and 500,000⁵ job losses – all within the first five months of the shutdown.

The blockade highlighted a fundamental policy dilemma: how should governments strike a balance between the economic, social and human costs of limiting internet connection and national security imperatives? In an increasingly digitalised world where internet access enables everything from education and healthcare to business and free expression, communication blackouts are a potent but controversial policy instrument.

This case study examines the circumstances that made the 2019 shutdown possible, protracted and difficult to challenge. It begins by situating the shutdown within the global rise of internet shutdowns as a policy instrument, as well as India's unique trajectory as the most frequent user, before delving into the specific political and historical background of the Kashmir conflict. At its core, the case study investigates the legal and administrative architecture that allowed a temporary emergency measure to persist for more than a year. It explores the shutdown's impact across economic, educational and social aspects, evaluates its effectiveness against the government's stated objectives, and highlights the perspectives of the stakeholders concerned. Finally, it discusses the policy alternatives available to countries with similar security challenges.

The Rise of Internet Shutdowns as a Policy Instrument

An internet shutdown refers to the intentional limitation of internet access, generally imposed by governments or relevant authorities as a means of control. These restrictions can take several forms, including

¹ Niha Masih et al., "India's Internet Shutdown in Kashmir Is the Longest Ever in a Democracy," *The Washington Post*, December 16, 2019, https://www.washingtonpost.com/world/asia_pacific/indias-internet-shutdown-in-kashmir-is-now-the-longest-ever-in-a-democracy/2019/12/15/bb0693ea-1dfc-11ea-977a-15a6710ed6da_story.html.

² Government of India's Ministry of Education, "Unified District Information System for Education Plus (UDISE+) 2019-20," 2021, https://www.medianama.com/wp-content/uploads/2021/07/UDISE2019_20_Booklet-2.pdf

³ Government of India's Ministry of Education, "All India Survey on Higher Education 2019-20," 2020, https://www.education.gov.in/sites/upload_files/mhrd/files/statistics-new/aishe_eng.pdf.

⁴ Fayaz Bukhari, "Indian Kashmir Sees More than \$2.4 Billion Losses since Lockdown," *Reuters*, December 18, 2019, <https://www.reuters.com/article/world/indian-kashmir-sees-more-than-24-billion-losses-since-lockdown-group-idUSKBN1YM0SJ/>.

⁵ Jammu Kashmir Coalition of Civil Society, "Kashmir's Internet Siege: An Ongoing Assault on Digital Rights," August 2020, <https://kashmir-scholars.org/wp-content/uploads/2020/08/kashmirs-internet-siege-jkccs-report-august-2020.pdf>

This case study was written by Sadaf Gani and edited by John Emmanuel Villanueva, Lee Kuan Yew School of Public Policy (LKYSPP), National University of Singapore. The case study does not reflect the views of the sponsoring organisation nor is it intended to suggest correct or incorrect handling of the situation depicted. It is not intended to serve as a primary source of data and is meant solely for class discussion.

Copyright © 2026 by the Lee Kuan Yew School of Public Policy at the National University of Singapore. All rights reserved. This publication can only be used for teaching purposes.

complete network outages commonly known as blanket bans, bandwidth limiting, otherwise known as throttling, and blocking services and platforms.

Internet shutdowns are becoming an increasingly prevalent feature of global digital life. As internet connectivity and access expand, more governments rely on internet shutdowns to restrict civic space and political liberties in the digital world. Recent evidence from the Cloudflare Q1 2026 Internet Disruption Report showed that state-imposed restrictions are on the rise – in terms of frequency, duration and severity. This is evidenced by countries such as Iran and Uganda implementing prolonged nationwide shutdowns during periods of unrest. At the same time, a parallel rise is seen in conflict-driven disruptions, in which military activity, including targeted strikes on digital infrastructure, has begun to have a direct impact on connection. These trends indicate how state control and geopolitical strife are shaping internet access globally.⁶

In 2025, Access Now and the #KeepItOn coalition documented 313 shutdowns in 52 countries, surpassing the records from 2024 (304) and 2023 (289). This represents a nearly three-fold increase from 2016 (80) across 28 countries, when Access Now first began tracking shutdowns. Among the worst-affected countries in 2025, Myanmar led with a record 95 shutdowns, followed by India (65), Pakistan (20) and Iran (11).⁷ The year 2025 also saw new countries enter the record for the first time, including Albania, Angola, Cambodia, Panama, Papua New Guinea, and the United States, using platform-level restrictions and temporary blackouts. With these countries joining the longlist, people in 100 countries have now experienced a shutdown since tracking began in 2016. This pattern indicates a broader diffusion effect: governments are increasingly viewing shutdowns as a feasible policy instrument and the practice becomes normalised as part of the modern state's policy toolkit.

State Motivations and the Logic of Shutdowns

Governments implement internet shutdowns for a variety of political, security and administrative reasons, which are frequently framed as necessary interventions during times of crises. According to Access Now statistics for 2025, the most prevalent triggers were conflict (125 incidents), protests and political instability (64) and information control (48), demonstrating the use of shutdowns as tools for managing dissent and shaping narratives. Shutdowns are also implemented in reaction to communal violence, elections and government officials' visits, with the goal of maintaining public order or limiting mobilisation. In certain circumstances, they are imposed to prevent cheating during examinations or to manage crowd safety at large religious gatherings. In sum, the rationale for internet shutdowns converges around national security, public safety, suppressing dissent and containing the spread of misinformation.

Architecture of State Internet Control

Governments implement internet shutdowns using a variety of methods, ranging from overt disruptions to more targeted and less visible controls (Table 1). On one end of the spectrum are complete or partial blackouts, which cut off connectivity at the national or regional level by altering routing information at key points in the network infrastructure. These measures are typically used during conflict or large-scale unrest. More commonly, however, authorities rely on targeted restrictions such as platform bans, Domain Name System (DNS) interference and Internet Protocol (IP)-based filtering to restrict access to certain services while maintaining broader connectivity.

⁶ Steve Belson, "Shutdowns, power outages, and conflict: a review of Q1 2026 Internet disruptions," *Cloudflare Blog*, April 28, 2026, <https://blog.cloudflare.com/q1-2026-internet-disruption-summary/>.

⁷ Access Now and the #KeepItOn Coalition, "Rising Repression Meets Global Resistance: Internet Shutdowns in 2025", <https://www.accessnow.org/wp-content/uploads/2026/03/KeepItOn-Internet-Shutdowns-2025-Annual-Report.pdf>.

In recent years, governments have increasingly adopted more covert approaches such as throttling and Deep Packet Inspection (DPI). Throttling deliberately slows down data transmission, rendering platforms effectively unusable without formally blocking them, while DPI enables content-level monitoring and filtering. These sophisticated techniques are harder to detect and document, allowing authorities to manage information flows with reduced public scrutiny. In practice, modern internet shutdowns often take the form of layered interventions, combining multiple methods.^{8,9}

Table 1: Types of Internet Shutdowns¹⁰

Level of Restrictions	Type	Mechanism	Disruption
Network-level disruptions	Full/partial blackout	Entire internet access is cut off at national or regional level	Very High
	Routing manipulation	Internet traffic is misrouted or dropped at key infrastructure points, disrupting connectivity	High
Access-level restrictions	DNS interference	Domain name requests are blocked or redirected, preventing access to specific websites	Low–Medium
	IP Blocking	Traffic to specific IP addresses or ports is blocked	Medium
Content-level filtering	URL-based blocking	Specific webpages or URLs are restricted	Low–Medium
	DPI	Internet traffic is inspected and filtered based on content, keywords or application type	High
Service-level disruptions	Platform blocking	Specific apps or platforms (eg social media) are blocked	Medium
	Throttling	Internet speed is deliberately slowed, making services effectively unusable	Medium
Indirect/non-network controls	Non-technical restrictions	Legal, economic or administrative measures that limit access without direct technical blocking	Variable

India's Shutdown Landscape and Trajectory

India has become the world's most frequent user of shutdowns in recent years, with 920 documented shutdowns between 2016 and 2025.¹¹ This accounts for more than half of all shutdowns worldwide. Unlike most governments that shut down the internet, India does not impose a country-wide lockdown. Shutdowns are instead implemented at the state level, and are limited to a particular state, district or town. The duration and extent of these shutdowns vary significantly, ranging from brief suspensions of a few hours to long-term interruptions that extend over several months to more than a year.

India's approach to internet shutdowns has evolved from a broad emergency law to a more targeted legal framework based on the Temporary Suspension of Telecom Services Rules, 2017 and subsequently the Telecommunications Act, 2023. While subsequent amendments introduced procedural safeguards such as written orders, review panels, time limits and a necessity test, the core grounds for shutdowns – public order, national security and public safety – have remained vaguely defined.

Courts have played a key role in limiting state authority by recognising that freedom of speech and expression, as well as the right to carry on trade or profession through the internet, are protected under Articles 19(1)(a) and 19(1)(g) of the Constitution, respectively. In *Anuradha Bhasin v. Union of India*, the Court held that

⁸ Access Now and the #KeepItOn Coalition, "Rising Repression Meets Global Resistance."

⁹ Steve Feldstein, "Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?," *Carnegie Endowment for International Peace*, March 31, 2022, <https://carnegieendowment.org/research/2022/03/government-internet-shutdowns-are-changing-how-should-citizens-and-democracies-respond?lang=en>.

¹⁰ Author's compilation based on Feldstein, "Government Internet Shutdowns Are Changing."

¹¹ Access Now, "#KeepItOn Data Dashboard," accessed May 2, 2026, <https://www.accessnow.org/keepiton-data-dashboard/>

shutdowns must be proportionate, temporary, necessary and transparent, but declined to declare them a violation of fundamental rights.

While internet shutdowns are common across several states, Jammu and Kashmir has emerged as a recurrent target.¹² Between 2012 and 2025, the erstwhile state experienced a total of 445 shutdowns.¹³ Most of these shutdowns were categorised as preventive in nature, imposed in anticipation of potential unrest, rather than in response to actual violence.¹⁴ This frames communication blockades as a pre-emptive security tool used by the Indian administration. Officially, the administration justifies shutdowns as necessary to prevent militant coordination, reduce mobilisation that may lead to violence and protect public order. However, scholars argue that they also serve to regulate political dissent: by limiting communication, documentation and collective action, shutdowns reduce citizens' ability to challenge governmental choices.^{15,16}

Why Jammu and Kashmir? The Kashmir Conflict

Jammu and Kashmir, located in the northernmost part of the Indian subcontinent, has been the site of one of the world's longest-running territorial and political conflicts. Since the partition of India and Pakistan in 1947, both countries have laid claim to the region in its entirety while administering only parts of it. Decades of insurgency, violence, heavy militarisation and recurrent security operations have entrenched chronic instability. For the region's inhabitants, this prolonged conflict has meant persistent disruptions to daily life, with security operations, curfews, strikes and communication restrictions becoming routine features of existence.

The region has experienced several major uprisings, specifically in 2008, 2010 and 2016, each triggering prolonged unrest and corresponding government restrictions. Successive cycles of unrest were met with increasingly sophisticated control measures, including limits on movement and assembly, as well as sweeping communication blackouts.

Article 370 & 35A and the Longest Internet Shutdown in a Democracy

Adopted in 1949, Article 370 of the Indian Constitution granted special autonomous status to the erstwhile state of Jammu and Kashmir, allowing it to legislate on all matters except finance, defence, foreign affairs and communications. It served as the constitutional basis for the region's accession to the Indian Union at a time when former princely states had the choice of joining India or Pakistan following their independence from British control in 1947.¹⁷ In 1954, this autonomous status was further reinforced through Article 35A, introduced by presidential order, which retained the territorial regulatory requirements under Article 370. This allowed the state assembly to define "permanent residents" and confer on them exclusive rights to property ownership, public employment and other privileges.¹⁸

¹² Access Now, "Five Years in a Row: India Is 2022's Biggest Internet Shutdowns Offender," February 28, 2023, <https://www.accessnow.org/press-release/keepiton-internet-shutdowns-2022-india/>.

¹³ InternetShutdowns.in, "Jammu & Kashmir — Internet Shutdowns Tracker," accessed January 7, 2026, <https://internetshutdowns.in/static-page/jammu-kashmir>

¹⁴ Software Freedom Law Centre, "Let the Net Work 2.0: Internet Shutdowns in India," 2024, <https://sflc.in/let-net-work-20>

¹⁵ Raouf Ahmad Peerzada et al., "The Politics of Internet Shutdowns in Jammu and Kashmir," *Human Geography* 19, no. 1 (2026): 82–87, <https://doi.org/10.1177/19427786251324660>

¹⁶ Jayshree Bajoria, "No Internet Means No Work, No Pay, No Food": Internet Shutdowns Deny Access to Basic Rights in "Digital India", *Human Rights Watch*, June 14, 2023, <https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic>

¹⁷ Al Jazeera, "Kashmir Special Status Explained: What Are Articles 370 and 35A?," August 5, 2019, <https://www.aljazeera.com/news/2019/8/5/kashmir-special-status-explained-what-are-articles-370-and-35a>.

¹⁸ Safwat Zargar, "Between Rights and Risks: Life and Liberty in an Internet Dark Kashmir," October, 2020, <https://www.defindia.org/wp-content/uploads/2020/10/kashmir-longest-internet-shutdown.pdf>.

Article 370 could be amended either through a formal constitutional amendment requiring a two-thirds parliamentary majority, or through a presidential declaration under Article 370(3). In August 2019, the Government of India adopted the latter route. A presidential order issued under Article 370(1) amended the constitutional interpretation to allow the Parliament – acting in place of the state legislature under President's Rule – to recommend that Article 370 be rendered inoperative. Following resolutions passed in both Houses of Parliament, the president issued the formal declaration on 6 August 2019. Simultaneously, the Parliament enacted the Jammu and Kashmir Reorganisation Act, 2019, which bifurcated the region into two Union Territories, bringing them fully under the Indian Constitution without special status.

Anticipating strong public opposition to the revocation, the central government imposed extensive security measures. On the evening of 4 August 2019, a complete communication blackout was enforced, suspending all mobile phone, landline and internet services in the region. Additional measures included a ban on public assembly, the deployment of tens of thousands of security personnel and the preventive detention of political leaders and activists. Authorities justified these actions as necessary to maintain public order amid a critical political transition, citing concerns over the use of social media in disseminating anti-government sentiments and mobilising protests. The shutdown swiftly became unprecedented. Lasting 552 days – from 4 August 2019 to 5 February 2021 – it was the longest internet shutdown ever enforced in a democratic country.¹⁹

Legal and Administrative Architecture that Enabled the Shutdown

The proliferation and prolongation of the shutdown were a result of three interconnected systemic issues: ease of enforcement at both administrative and technical levels, legislative ambiguity that allowed for broad discretion while imposing minimal accountability, and a systematic lack of proportionality in practice.

Ease of Enforcement

The first issue lies in the ease with which shutdowns can be initiated and sustained. In India, internet shutdowns can be executed instantaneously through telecom providers, who are legally bound to comply with administrative orders.

From a technical standpoint, enforcing a blanket ban, such as the one implemented in 2019, necessitates telecommunications providers altering routing information at critical points in network architecture, preventing data from flowing through. Once the order is issued, this process can be completed within minutes. There are no technical barriers or implementation issues that might prompt officials to reconsider or delay the decision.

From an administrative standpoint, the threshold for ordering a shutdown is significantly low. Under the Temporary Suspension of Telecom Services Rules of 2017, a single designated official, such as the Union Home Secretary for central orders or a State Home Secretary for state-level orders, has the right to issue shutdown orders.²⁰

This ease of enforcement at both the technical and administrative level has two major repercussions. First, the absence of technical challenges, combined with the lack of pushback, allows for swift implementation with minimal scrutiny. When policy implementation is complex or resource-intensive, decision-makers are naturally motivated to consider alternatives or ensure that the measure is essential. Such restrictions do not apply to internet shutdowns in India. Second, low implementation barriers and a highly centralised decision-

¹⁹ Jayshree Bajoria, "No Internet Means No Work, No Pay, No Food": Internet Shutdowns Deny Access to Basic Rights in "Digital India", *Human Rights Watch*, June 14, 2023, <https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic>

²⁰ Government of India's Ministry of Communications, "Telecommunications (Temporary Suspension of Services) Rules," 2017, <https://dot.gov.in/sites/default/files/Suspension%20Rules.pdf>

making pattern leads to shutdowns being implemented as a routine security practice, contributing to their normalisation as a legitimate and justifiable policy response.

The 2019 shutdown exemplified both of these institutional dynamics. The decision to impose a region-wide communication suspension was made at the highest levels of government and implemented quickly and comprehensively. Once in place, the restrictions lasted over 500 days. Their persistence can be attributed in part to the low administrative and political costs of maintaining the shutdown: telecommunications providers implemented and enforced the restrictions on a continuous basis, absorbing associated financial losses, while the state bore no direct implementation burden after the initial order was issued.

This enforcement model is not unique to India. Several governments across the world rely on telecom companies to carry out shutdowns under legally enforceable directions. In more authoritarian regimes, this control is embedded in the network itself. In China, for example, content screening and blocking are incorporated into the infrastructure through state-dominated providers. In Russia, legislative and technological mechanisms, such as a national domain name system and surveillance architecture, allow the government to regulate traffic routing and access on a systemic level. Meanwhile, Myanmar's post-coup reform of the telecommunications industry has enabled authorities to directly compel providers to implement shutdowns and surveillance measures.²¹

India does not maintain a permanent, infrastructure-level censoring mechanism of this type. Shutdowns remain sporadic and technically reversible. However, the basic enforcement reasoning is the same: telecommunications providers have no significant ability to delay, resist or independently review shutdown orders before complying. The obligation is immediate and binding. This enables the state to combine the flexibility of temporary interventions with a level of enforcement ease often associated with more centralised methods of digital control.²²

Legislative Ambiguity

The absence of concrete laws regulating communication blockades, coupled with conjectural phrasing within the laws permitting these restrictions, has made it expedient to implement them. The Temporary Suspension of Telecom Services Rules, 2017 grant "competent government authorities" the right to suspend telecommunication services in specific regions during "public emergencies" or "safety concerns".²³ These two terms, however, have not been distinctly defined. In conjunction with this, a Review Committee consisting of officials from the state and the Union is responsible for the oversight of implemented restrictions. This effectively means that the authorities empowered to pass the restriction orders are mandated to review their decisions, leading to a conflict of interest that renders the committee inconsequential. This was observed during the 2019 shutdown when the Supreme Court ruled that the "blanket order" failed to provide any reasons to reflect that all the districts of the Union Territory of Jammu and Kashmir require the imposition of such restrictions; however, after considering the "compelling circumstances of cross-border terrorism", the Supreme Court refrained from calling it a constitutional violation, and mandated a special committee to review these restrictions periodically.²⁴

The United Nations Human Rights Committee has stated that restrictions on freedom of expression must be provided by law, and that laws must be formulated with sufficient precision to enable individuals to regulate

²¹ Irene Poetranto, "The Architecture of Digital Repression," *Carnegie Endowment for International Peace*, March 10, 2026, <https://carnegieendowment.org/middle-east/research/2026/03/the-architecture-of-digital-repression>

²² Irene Poetranto, "The Architecture of Digital Repression."

²³ Government of India's Ministry of Communications, "Telecommunications (Temporary Suspension of Services) Rules."

²⁴ Global Freedom of Expression, "Bhasin v. Union of India," accessed May 2, 2026, <https://globalfreedomofexpression.columbia.edu/cases/bhasin-v-union-of-india/>

their conduct.²⁵ In a landmark 2020 judgment in *Amnesty International Togo v. The Togolese Republic*, the Economic Community of West African States (ECOWAS) Court of Justice declared that Togo's 2017 internet shutdown was unconstitutional precisely because there was no clear legal basis. The Court ruled that internet connection is a "derivative right" necessary for the achievement of freedom of speech, and that any interference must be justified by a special regulation that fulfils the conditions of necessity and proportionality.²⁶ Similarly, in 2022, the ECOWAS Court ruled against Nigeria's suspension of Twitter, emphasising that national security claims cannot justify derogations from digital rights without a strict legal framework.²⁷

India's reliance on vague statutory language and compromised oversight mechanisms fail to meet these international standards. While courts in countries such as Indonesia have actively challenged government-mandated internet blackouts (such as the 2019 Papua shutdown)²⁸ for violating the legal parameters of emergency powers, Indian courts have frequently acknowledged legislative ambiguities without definitively invalidating the underlying executive actions.

In most developed democracies, any such restrictions would be subject to judicial review or scrutiny by an independent authority, ensuring that the executive is held accountable to an independent part of government. India's "self-review" model appears to be a departure from international standards that emphasise independent oversight.

Authorities began publicising shutdown orders and conducting periodic reviews through the same compromised committee structure. High-speed internet was suspended for another year following the decision. The legislative ambiguity was left unresolved, and the underlying issue of discretion without accountability persisted.

Blanket Bans and Absence of Proportionality in Practice

The third issue concerns the systematic inability to apply the principles of proportionality while executing shutdowns. Proportionality, a key concept in democratic administration, demands that constraints on rights serve a valid goal, employ the least restrictive means available, and strike a reasonable balance between public benefits and damages inflicted.

The 2019 shutdown is an exemplar of this problem. The blockade affected the entire population of Jammu and Kashmir – more than 12.5 million people. It drew no distinction between areas experiencing unrest and those that were peaceful. It made no exceptions for essential services such as education and healthcare. It provided no provision for persons with urgent communication requirements. A joint statement by the UN human rights experts noted that the shutdown was "inconsistent with the fundamental norms of necessity and proportionality and constitute(d) a form of collective punishment of the people of Jammu and Kashmir."²⁹

²⁵ United Nations Human Rights Committee, *General Comment No. 34: Article 19 — Freedoms of Opinion and Expression* (CCPR/C/GC/34), 12 September 2011, <https://www.ohchr.org/sites/default/files/english/bodies/hrc/docs/GC34.pdf>

²⁶ Access Now, "ECOWAS Togo Court Decision: Internet Access Is a Right That Requires Protection of the Law," Access Now, July 14, 2020, <https://www.accessnow.org/ecowas-togo-court-decision/>

²⁷ Access Now, "ECOWAS Court Victory: Nigeria Twitter Ban Declared Unlawful," Access Now, July 14, 2022, <https://www.accessnow.org/press-release/ecowas-court-nigeria-unlawful-twitter-ban/>

²⁸ Association for Progressive Communications (APC), "EngageMedia: Monitoring the ruling on 2019 internet shutdowns in Papua and West Papua," APC News, June 12, 2020, <https://www.apc.org/en/news/engagemedia-monitoring-ruling-2019-internet-shutdowns-papua-and-west-papua>.

²⁹ Office of the High Commissioner for Human Rights, "UN Rights Experts Urge India to End Communications Shutdown in Kashmir," accessed May 2, 2026, <https://www.ohchr.org/en/press-releases/2019/08/un-rights-experts-urge-india-end-communications-shutdown-kashmir>.

A Supreme Court decision noted the lack of proportionality of the ban – but refrained from issuing a verdict to enforce its application, demonstrating the absence of practical execution of these principles.³⁰

Courts across jurisdictions have upheld standards of proportionality when scrutinising internet shutdowns. In Indonesia, the Jakarta State Administrative Court, adjudicating the government's shutdown of internet services in Papua and West Papua in 2019, held that a blanket termination of network access was disproportionate insofar as it indiscriminately curtailed a wide range of constitutionally protected activities including access to education, healthcare information and economic participation. Critically, the Court indicated that proportionate responses must be targeted at specific unlawful content or actors, rather than suspending access for entire populations.³¹ Similarly, the European Court of Human Rights in *Cengiz and Others v. Turkey* (2015) ruled that the blanket blocking of YouTube was incompatible with Article 10 of the European Convention on Human Rights, which protects the freedom to receive and impart information.³²

Within India, *Anuradha Bhasin v. Union of India* (2020) aligned domestic jurisprudence with these international standards by prohibiting indefinite suspensions and anchoring the legality of shutdowns to the principles of necessity and proportionality. However, the gap between judicial decisions and administrative practice has remained significant and persistent. Subsequent shutdowns, including extended region-wide blackouts in Jammu and Kashmir, Rajasthan, and Manipur, have continued with limited review, implying that the Review Committee mechanism established by the 2017 Rules is more procedural than substantive.

When viewed from a comparative standpoint, India's internet shutdown structure occupies a middle ground. Its constitutional architecture and judicial discourse adhere to democratic norms: Article 19 protections include proportionality standards and transparency. However, its administrative reality, legal uncertainty and the recurrent deployment of blanket shutdowns is more akin to authoritarian administrations' digital control techniques. As the international community increasingly recognises internet access as an essential enabler of civil, political, economic and social rights, India's status as the world's most frequent user of internet shutdowns among democracies represents not only a policy concern, but also a structural democratic deficit.

Timeline: How the Longest Internet Shutdown Unfolded

The 2019 shutdown unfolded in stages that reflected the administration's shifting attitude on the level of control. From an initial blanket suspension of all telecommunications to increasingly calibrated restrictions, such as speed throttling, selective whitelisting and targeted localised shutdowns, each phase preserved the substantive effects of digital isolation while presenting incremental restoration as evidence of normalisation.

Phase One: Complete Communication Blackout

The initial 158 days of the shutdown were defined by a near-absolute absence of internet connectivity. Beginning on 4 August 2019, all communication services, including broadband internet, mobile data, mobile phone calls and SMS, landline telephones, and cable television networks were suspended. For 72 days, the region experienced near-total communication isolation.³³ Television access was partially restored in certain areas after a week, although overall isolation was severe. The blockade created an information vacuum with far-reaching implications. Journalists struggled to report on ground conditions while working under strict restraints that prompted worldwide condemnation. Businesses could not process digital transactions or

³⁰ Global Freedom of Expression, "Bhasin v. Union of India."

³¹ Alliance of Independent Journalists and SAFEnet v. Minister of Communication and Information Technology and President of the Republic of Indonesia (Decision No. 230/G/TF/2019/PTUN-JKT), Jakarta State Administrative Court, June 3, 2020, <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2022/02/Indonesian-Case-Indonesian-Language-1.pdf>.

³² European Court of Human Rights, *Cengiz and Others v. Turkey* (Applications nos. 48226/10 and 14027/11), Judgment, 1 December 2015, HUDOC, <https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-5241080-6502267&filename=Judgment+Cengiz+and+Others+v.+Turkey+-+blocking+of+access+to+YouTube.pdf>.

³³ Ashraf Wani, "Postpaid Mobile Phone Services Restored in Kashmir 72 Days after Lockdown, Internet Still Off," *India Today*, October 14, 2019, <https://www.indiatoday.in/india/story/post-paid-mobile-services-restored-in-kashmir-valley-1609122-2019-10-14>

communicate with suppliers. Students could not access educational platforms and online learning materials. Healthcare providers were unable to contact specialists, access medical databases or manage patient referrals.

On 14 October 2019, postpaid mobile phone service was restored for voice calls. Prepaid mobile services, SMS messaging and all types of internet access remained suspended.³⁴ Consumers on postpaid subscriptions could make phone calls but not use data, text messaging or the internet on any device. The region continued to remain digitally isolated. During this time, the Supreme Court of India began hearing petitions questioning the constitutionality and proportionality of the shutdowns. The phase highlighted the authorities' continued priority on limiting internet access in order to prevent potential demonstrations and the circulation of inflammatory content.

Phase Two: The 2G Era & Whitelisting

This phase marked a critical, albeit limited, shift in the digital control policy, initiated by a landmark Supreme Court judgment. On 10 January 2020, India's Supreme Court issued a judgment in *Anuradha Bhasin v. Union of India*, directing the government to review all limitations within one week, recognising that the extended suspension of basic rights constituted an abuse of authority. However, the Court declined to declare the suspension illegal, citing the government's assertion of compelling circumstances of cross-border terrorism.³⁵

Four days later, on 14 January 2020, the administration began easing restrictions. 2G mobile internet services were restored in five of Jammu's ten districts. Broadband services were offered to hospitals, banks and government agencies. However, access was limited to 150 government-approved whitelisted websites. Mainstream news sources and social media platforms were absent from the whitelist. On 24 January 2020, the whitelist increased to 301 websites, including educational services, banking, travel and food delivery platforms. However, Facebook, WhatsApp, Instagram, Twitter and other social media platforms remained inaccessible.³⁶

On 25 January 2020, 174 days after the shutdown began, officials lifted the restriction on 2G mobile internet services in the Kashmir region. Access was confined to the 301 whitelisted websites, with social media platforms still prohibited. However, services were terminated the following day, claiming "security concerns," until being restored on 26 January.³⁷ The return of the 2G connection was largely symbolic. Modern internet applications, such as video conferencing, file downloads, streaming services and many educational platforms, require broadband speeds to work well. At 2G speeds (usually 50-100 kbps), loading a webpage takes several minutes. Despite notional restoration, the region remained largely disconnected from the world.

Phase Three: Gradual Restoration

On 4 March 2020, authorities lifted the whitelist limitation, granting access to all websites, including social media. However, internet speed remained throttled to 2G. The complete shutdown of fixed-line internet and mobile networks thus lasted 213 days. However, the ban on mobile high-speed 4G internet access would last far longer. Following continuous domestic and international pressure and repeated judicial interventions, authorities restored 4G mobile internet services on 5 February 2021. The restoration occurred 18 months after the initial blockade and about a year after the COVID-19 pandemic began, a period during which high-speed internet was crucial for remote work, education and healthcare.

The restoration did not mark the end of the internet shutdown policy in the region. Authorities maintained the ability to enforce localised shutdowns, and specific websites remained restricted. From 2021 to 2023,

³⁴ Wani, "Postpaid Mobile Phone Services Restored in Kashmir."

³⁵ Global Freedom of Expression, "Bhasin v. Union of India."

³⁶ Jammu Kashmir Coalition of Civil Society, "Kashmir's Internet Siege."

³⁷ Jammu Kashmir Coalition of Civil Society, "Kashmir's Internet Siege."

Kashmir continued to experience periodic internet shutdowns, shorter in duration and geographically targeted compared to the 2019 blanket ban, suggesting that the underlying policy approach remained unchanged.³⁸

Multidimensional Impacts: The Human and Economic Costs

The 2019 shutdown imposed significant costs across economic, educational and social dimensions, raising questions about whether the scale and ambit of restrictions were proportionate to the costs on civilians.

Economic Devastation

The shutdown led to significant economic devastation in the region. The Kashmir Chamber of Commerce and Industry projected losses of more than US\$ 2.4 billion in the first five months,³⁹ with roughly 500,000 jobs lost as firms were unable to operate without internet access.⁴⁰ The tourism industry, a major employer, collapsed almost immediately. Hotels that relied on online booking platforms shut down, travel agencies were unable to interact with clients and tour operators lost all bookings entirely.⁴¹ The prime tourist season, which ran from August to October, was effectively lost, with many businesses never recovering.

The handicraft industry, which had relied on digital marketplaces to reach worldwide buyers, was cut off from supply chains. Artisans were unable to fill orders, contact purchasers or organise shipping. Small and medium-sized businesses in all industries faced existential threats. Digital payments, which have become a standard practice, were impossible. Businesses with small margins barely survived for a few months without revenue, exacerbating the region's economic fragility.⁴²

Educational Crisis

Around 2.8 million students were affected by school and university closures. Schools lost 150 days of instruction in 2019 alone.⁴³ When the COVID-19 pandemic hit the region in March 2020, students experienced a double lockdown⁴⁴ — unable to attend physical schools or access online education while the rest of the world went online. Educational administrators decreased syllabi by 30% to allow for grade advancement, resulting in cascading learning losses as pupils proceeded without understanding core concepts.⁴⁵ Secondary level dropout rates grew drastically, from 3.4% (2017–18) to 18.5% (2019–20), a fivefold rise in two years. Primary dropout rates increased from 2.9% to 6.7%.⁴⁶ At the same time, instructors saw an increase in behavioural problems, anxiety and depressive symptoms among students. The combination of social isolation and academic uncertainty resulted in a mental health crisis.⁴⁷

³⁸ InternetShutdowns.in, "Jammu & Kashmir — Internet Shutdowns Tracker."

³⁹ Bukhari, "Indian Kashmir Sees More than \$2.4 Billion Losses."

⁴⁰ Jammu Kashmir Coalition of Civil Society, "Kashmir's Internet Siege."

⁴¹ Regina Mihindukulasuriya, "Kashmir Internet Shutdown Hit Valley Industries Hard," *ThePrint*, October 29, 2019, <https://theprint.in/india/kashmir-internet-shutdown-hit-valley-industries-hard/312659/>.

⁴² Niha Dagia, "Perpetual Silence: Kashmir's Economy Slumps Under Lockdown," *The Diplomat*, August 14, 2020, <https://thediplomat.com/2020/08/perpetual-silence-kashmirs-economy-slumps-under-lockdown/>.

⁴³ Bisma Bhat, "Academic Calendar: 150 Days of Classwork Lost," *The Kashmir Monitor*, November 2, 2019, <https://www.thekashmirmonitor.net/academic-calendar-150-days-of-classwork-lost/>.

⁴⁴ Leoni Connah, "Double Lockdown in Kashmir during the Covid-19 Pandemic," *Peace Review: A Journal of Social Justice* 33, no. 1 (2021): 33–38, <https://doi.org/10.1080/10402659.2021.1956128>.

⁴⁵ Bishal Kalita, "Jammu and Kashmir Reduces School Syllabus by 30%," *NDTV*, August 14, 2020, <https://www.ndtv.com/education/jammu-and-kashmir-reduces-school-syllabus-30-2279639>.

⁴⁶ Government of India, *State/UT-wise Details of Dropout Rate by Level of Education as per Unified District Information System for Education Plus (UDISE+)*, Open Government Data Platform India (data.gov.in), published July 17, 2025, <https://www.data.gov.in/resource/stateut-wise-details-dropout-rate-level-education-unified-district-information-system>.

⁴⁷ Majid Maqbool, "A Year with No School: Mental Health Fears Rise for Kashmir's Children," *The New Humanitarian*, July 21, 2020, <https://www.thenewhumanitarian.org/news/2020/07/21/Kashmir-lockdown-schools-children-mental-health>.

Social and Healthcare Consequences

Healthcare services were severely impacted. Patients could not consult with specialists. Doctors could not use medical databases or coordinate patient care. Emergency communication proved difficult, resulting in life-threatening scenarios.⁴⁸ Banking and financial services became inaccessible; households were unable to receive remittances from relatives working overseas, resulting in financial difficulty.⁴⁹ The information vacuum had a significant psychological impact. Families separated by restrictions were unable to communicate for weeks or months, leading to widespread feelings of abandonment and collective punishment, which further eroded trust in governance.

Stakeholder Perspectives

The 2019 internet shutdown produced sharply divergent stakeholder responses, demonstrating a clear difference between those who enabled and implemented the policy and those who suffered the effects. While the state justified the shutdown as a necessary preventive measure to maintain public order and security, other actors including the judiciary, service providers, businesses, civil society and the affected population either facilitated its implementation, were forced to comply, or suffered significant legal, economic and social consequences. Their diverse responses, which ranged from justification and deference to adaptation and legal challenge, demonstrate how the consequences of the shutdown and the exercise of authority were distributed asymmetrically across these groups.

Central Administration and Security Establishment

The Central Administration justified the shutdown through several arguments revolving around national security and public safety concerns. First, preventing mass mobilisation: social media had historically been used to organise large-scale protests. Second, combatting misinformation: digital platforms had previously been used to circulate inflammatory content that was linked to instances of violence. Third, security: digital platforms were utilised by militants to coordinate and carry out operations. Fourth, public safety: temporary inconvenience was justified in order to avert loss of life.

Government statements consistently framed the restrictions as temporary, preventive, and essential to maintain public order and security during a politically delicate situation. However, the persistence of restrictions, especially during crises such as COVID-19, demonstrated a policy stance of maintaining widespread preventive controls rather than considering targeted or time-bound measures.

Judiciary

The judiciary emerged as a prominent actor after the shutdown had been in place for a while. Multiple petitions questioned both the legality of the communication limits and their prolonged duration. In January 2020, the Supreme Court determined that access to the internet was essential to constitutionally guaranteed freedoms and that the extended suspension of services was illegal. However, the Court declined to mandate quick reinstatement, instead asking the government to conduct periodic evaluations and consider proportionality. Subsequent action centred on the continuous limitation of 2G services, with the Court consistently deferring to the executive's assessment of security conditions. While the judiciary's involvement helped establish legal principles and boundaries, it did not affect executive decision-making.

⁴⁸ Meenakshi Ganguly, "Kashmir Shutdown Raises Healthcare Concerns," *Human Rights Watch*, August 30, 2019, <https://www.hrw.org/news/2019/08/30/kashmir-shutdown-raises-healthcare-concerns>.

⁴⁹ Human Rights Watch, "India: Restore Kashmir's Internet, Phones," August 28, 2019, <https://www.hrw.org/news/2019/08/28/india-restore-kashmirs-internet-phones>.

Telecommunications and Internet Service Providers

Telecommunications operators executed and enforced the shutdown and throttling directives. Service suspensions were carried out swiftly and at scale, affecting both mobile and fixed-line networks. Providers had no formal participation in decision-making and had minimal knowledge of the restoration criteria. Even though revenue-generating activities were suspended throughout the closure, operators continued to incur infrastructure and maintenance expenditures. Restoration stages necessitated technical reconfigurations as services were selectively activated, blocked or restricted to whitelisted websites and user groups. Providers suffered reputational and financial losses as a result of instituting shutdowns; however, they had no choice but to comply with the directives.

Businesses

The business community reported huge economic losses. The closure directly impacted businesses that relied on digital payments, online procurement and contact with markets beyond the region. Small firms, merchants, and service providers experienced challenges in closing deals, maintaining inventories and coordinating logistics. Export-oriented industries, such as handicrafts and horticulture, were impacted by the inability to contact buyers and platforms.

Media and Civil Society

Journalistic activity was constrained by the lack of digital communication channels. Reporters depended on physical travel and a government-facilitated media centre that provided limited shared internet access. Civil society organisations produced material on the economic, educational and legal consequences of the shutdown and backed lawsuits against it. Given the limitations of real-time communication, engagement with international bodies took the form of secondary reporting and retroactive documentation.

General population

Residents were significantly affected by the blockade, which disrupted everyday communication, service access, and participation in commercial and educational activities. The lack of mobile connectivity and internet access hampered households' ability to contact family members, access banking services and receive information, especially in the context of the COVID-19 pandemic. These consequences were felt generally across the community, as restrictions were imposed uniformly. This contradiction, in which the state depended on digital infrastructure to control the pandemic elsewhere while restricting it in Kashmir, demonstrates the extent to which security reasoning overrode all other policy considerations.

International Observers

International organisations and foreign governments monitored the developments and progress using publicly available material, communication with the Central Administration, judicial procedures and post-restoration reporting. Statements and publications were focused on the duration and extent of the limitations, rather than the immediate security context. While these actors did not have a direct effect on policy decisions, their statements and assessments sustained international attention and imposed reputational pressures on the Indian administration.

Did the Shutdown Achieve its Stated Objectives?

The government justified the shutdown on three grounds: preventing mass mobilisation, countering disinformation and disrupting insurgent operations. However, available evidence offers limited clarity on the extent to which prolonged, region-wide restrictions fulfilled these objectives.

Repressing Mass Mobilisation

The administration contended that social media facilitates rapid protest coordination. However, mass mobilisation may still occur in the absence of digital platforms, especially in closely-knit communities.⁵⁰ According to estimates cited in press reporting, approximately 20 protests per day took place between August 2019 and August 2020, with thousands of protesters coordinating and defying curfew despite the internet blackout.⁵¹ Banning these platforms may also fuel uncertainty and panic — restricting the free flow of information can inadvertently lead to a counterproductive outcome and further proliferate misinformation.⁵²

Countering Disinformation

The second argument focuses on preventing the spread of inflammatory information, fake news and propaganda via digital media. However, research on information restrictions indicates that limiting communication channels does not eliminate disinformation but frequently exacerbates it by creating information vacuums in which misinformation can propagate.⁵³

In 2021, a Parliamentary Standing Committee investigated whether internet shutdowns effectively handled public emergencies or safeguarded public safety. The Committee received testimonies from diverse stakeholders and examined the available evidence and found no evidence to support shutdown efficacy for these aims. The Committee condemned the dependence on shutdowns, noting that it reflects badly on the state's law and order machinery, and proposed that more sophisticated ways of information management ought to be explored.⁵⁴

Counterterrorism

The third justification has centred on counterterrorism efforts. Security authorities stated that militant organisations utilise internet communication to organise and maintain contact with handlers. Militant activity remained continuously high during the protracted internet shutdowns, with 255 in 2019 and 244 in 2020. After high-speed mobile internet connections were restored in February 2021, occurrences slightly decreased to 229 in 2021⁵⁵ and further to 123 in 2022,⁵⁶ indicating a declining trend following the relaxation of connectivity limitations. These statistics reveal that patterns of violence remained largely consistent, and in fact followed a declining trend in response to easing connectivity constraints. This raises questions about whether protracted, region-wide shutdowns contribute to achieving stated security aims.

⁵⁰ Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India" (working paper, Stanford Global Digital Policy Incubator, February 7, 2019), <https://ssrn.com/abstract=3330413>

⁵¹ AFP, "India-Held Kashmir's Internet Shutdown Continues amid Restrictions," *Dawn*, October 5, 2019, <https://www.dawn.com/news/151465>

⁵² Rydzak, "Of Blackouts and Bandhs."

⁵³ UNESCO, "UNESCO Statement on Internet Shutdowns," January 20, 2026, <https://www.unesco.org/en/articles/unesco-statement-internet-shutdowns>

⁵⁴ *Suspension of Telecom Services/Internet and Its Impact*, Twenty-sixth Report of the Standing Committee on Communications and Information Technology, 17th Lok Sabha. December 1, 2021. https://eparlib.nic.in/bitstream/123456789/820699/1/17_Communications_and_Information_Technology_26.pdf

⁵⁵ Government of India, *Year-wise Details of Terrorist Incidents in Jammu and Kashmir (2018–2021)*, Open Government Data Platform India (data.gov.in), February 24, 2023. <https://www.data.gov.in/resource/year-wise-details-terrorist-incidents-jammu-and-kashmir-2018-2021>

⁵⁶ Government of India, *State/UTs-wise Details of the Number of Terrorist Incidents, Security Force Personnel Martyred, and Civilians Killed in These Attacks in the Hinterland of the Country and in Jammu and Kashmir during 2022*, Open Government Data Platform India (data.gov.in), April 3, 2023. <https://www.data.gov.in/resource/stateuts-wise-details-number-terrorist-incidents-security-force-personnel-martyred-and>

Policy Options

During the constitutional reorganisation, the Indian government did not exercise a binary choice between shutdown and no shutdown. It implemented a variety of security measures concurrently: curfews, preventive detentions, military deployment and communication restrictions, while making sequential judgments regarding the extent, length and severity of digital controls. The administration relied on a combination of policy options across different phases of the shutdown.

Path Taken: Region-Wide Communication Shutdown with Gradual Restoration

To eliminate any digital channel that could be used to coordinate protests, disseminate information about the revocation of Article 370, or enable organised resistance to the security operation accompanying the constitutional transition, the Central Administration ordered a blanket shutdown in addition to substantial security measures, including Section 144 restrictions, preventive detentions, and large-scale force deployment. Authorities gradually restored post-paid mobile voice services, limited broadband for institutions, and later 2G mobile internet with whitelisted websites, while repeatedly extending restrictions via executive orders and periodic reviews, including following Supreme Court scrutiny. This option maximised administrative control, but also resulted in long-term, population-wide limitations based on internal security evaluations that were not publicly disclosed.

The shutdown stifled any dissent organised through digital means in the immediate aftermath of the revocation. No large-scale unrest comparable to the 2016 demonstrations took place. However, there were severe economic and social implications. This approach maximised administrative control and minimised the risk of coordinated unrest. It accomplished this by imposing the entire cost on the civilian population rather than on the state. The costs were not incidental, they were structural: a blanket shutdown, by definition, cannot discriminate between a person coordinating violence and a student studying for an exam, a doctor conducting a consultation, or a company processing a payment. The approach, therefore, set a precedent for normalised use: the same institutional infrastructure that allowed for the shutdown remained in place thereafter, and periodic shutdowns continued throughout 2021, 2022 and 2023.

Alternative 1: Time-Bound Shutdown with Strict Conditions for Extension

Instead of an indefinitely renewable blanket order, each extension could have been conditioned on documented security assessments establishing necessity and proportionality, requiring the state to demonstrate persistent security risks.

This approach would preserve the state's ability to impose internet restrictions during genuine security emergencies while imposing a procedural requirement that prevents open-ended renewal by making continuation contingent on demonstrated and documented reasons. The issuing authority (Union or State Home Secretary) would maintain the ability to impose and extend shutdowns. The shift is in what the authority must produce: a reasoned, proven and documented justification rather than a rolling administrative order. Judicial scrutiny would be increased by giving courts explicit grounds for evaluating extension requests, rather than the existing practice of deference to executive security judgments.

In terms of security efficacy, this would not materially weaken the state's ability to prevent coordinated violence and at the same time, prevent infringement of rights and reduce the impact on the general population. In addition to this, it would lend the administration a degree of credibility that unreasoned blanket orders structurally cannot.

Institutional feasibility would be a concern since the present Telecom Rules lack such conditionalities. This alternative, therefore, would require either legislative modification or a judicially imposed norm, neither of which is easily accomplished in a militarised region.

Alternative 2: Functional Exemptions for Essential Services

Rather than imposing population-wide restrictions, authorities could have expanded functional exemptions earlier and more systematically, such as restoring full broadband access to educational institutions, healthcare providers, businesses and media, while maintaining tighter controls on mass-access mobile data and social media platforms.

This approach separates the security function of a shutdown from its collateral damage. The security objective would be partially preserved. Channels utilised for protest coordination would remain suspended. This approach would have potentially reduced the economic losses, educational disruptions, and healthcare failures documented in 2019.

The principal drawback is administrative complexity. Implementation would require active collaboration between the issuing authority, telecommunications providers and the sector-specific departments in charge of identifying and certifying exempted platforms and institutions. These exemptions necessitate layers of verification procedures to avoid circumvention. In a conflict-affected state with limited administrative capacity and security pressures, it would be difficult to implement.

While this approach mitigates harm, it does not fundamentally alter the unilateral nature of decision-making. The government has complete discretion over which services are considered essential, which institutions are eligible for exemption, and what evidence is sufficient to justify curtailing an exempted function. Affected communities, companies and civil society organisations have no official participation in selecting those categories, no way to challenge an exclusion from exemption in real time and no assurance that the criteria would be applied consistently or openly.

Alternative 3: Finer Geographic and Risk-Based Targeting

Restrictions could have been tailored to localised threats rather than treating the entire region as a uniform security zone. Districts without ongoing disturbance may have had partial restoration, with stricter controls for known hotspots.

Geographic targeting is technically feasible: telecom companies can impose district-level routing limitations using the same technology as blanket shutdowns. The implementation challenge is institutional, not technological. It calls for high-quality, timely and granular intelligence that appropriately differentiates across districts based on actual threat levels rather than administrative convenience. It necessitates a decision-making procedure that can update restrictions within days as conditions change.

In terms of security efficacy, this is the most contentious option: it necessitates high-quality, real-time intelligence and interagency collaboration, which may not have been feasible in 2019. However, this approach would have resulted in substantially less harm, particularly for communities living in areas without active conflict. A blanket closure imposed costs on communities who were not involved in active conflict. Targeting would have avoided unnecessary disruptions to livelihoods, education and access to essential services.

This alternative is the most operationally demanding of the three, and its legitimacy is dependent on the integrity of its implementation, as unequal levels of unrest may not always justify targeting. Without clear criteria, transparency and accountability in how “high-risk” areas are designated, geographic targeting risks becoming a tool for selective punishment.

Conclusion

The 2019 shutdown represented an unprecedented measure of digital disconnection in a democratic society. High-speed internet was restored after 18 months of limitations, several judicial proceedings, significant economic and social consequences, and sustained local and international pressure. The aftermath revealed long-lasting socio-economic devastation. Educational gaps remained, and students who missed critical learning years continued to suffer. Businesses that had closed did not instantly reopen. Mental health professionals and educators have raised concerns about the long-term psychological effects on students who experienced prolonged periods of educational disruption and social isolation. The shutdown also highlighted the limitations of digital disconnection as a security measure. Despite the limits, the region continued to encounter security issues.

The policy alternatives examined here – time-bound orders with documented justifications, exemptions for essential services and geographic targeting based on actual threat levels – are not exhaustive solutions, but each addresses a distinct failure highlighted by the 2019 case. Importantly, they are not necessarily mutually exclusive. A more defensible policy framework would most likely integrate components of all three, layering their core principles rather than presenting them as competing options.

The 2019 shutdown has since become a reference point in global debates on digital rights and security governance. The fundamental questions it raises persist: under what conditions, if any, are communication shutdowns justifiable? What principles of necessity, proportionality and accountability should govern such decisions? And how can states facing genuine security threats avoid putting the entire cost of those threats onto the civilian populations they are nominally acting to protect?

Discussion Questions

1. The case identified three institutional enablers of the internet shutdown: ease of enforcement, legislative ambiguity and a compromised review mechanism. Which factor played the most important role in extending the shutdown beyond the initial security emergency? Do you think the shutdown could have continued if any one of these factors had been absent?
2. The shutdown affected all 12.5 million residents — students, patients, businesses and suspected militants alike — and was described by the UN as a form of collective punishment. In a conflict-affected region, can such broad restrictions ever be considered proportionate? What principle should guide where the line is drawn?
3. The government justified the shutdown on three grounds: suppressing mass mobilisation, countering disinformation and disrupting militant operations. Protest continued at an average of 20 incidents per day; misinformation arguably worsened in the information vacuum; and militant activity followed a declining trend only after internet restoration. What does this evidence tell us about the effectiveness of communication blackouts as a counterterrorism tool?
4. The case presents three alternatives: time-bound orders with documented justifications, functional exemptions for essential services and geographic risk-based targeting. Which combination best balances the government's security objectives against the rights and welfare of the civilian population? What institutional changes would be required to implement your preferred approach?
5. In 2025, 313 internet shutdowns were recorded across 52 countries, including several first-time users such as the United States. As more governments adopt shutdowns, the measure is being normalised as part of the modern state's policy toolkit. What governance mechanisms — domestic, regional or international — are most likely to slow this spread? Drawing on the Kashmir experience, what lessons should be taken into account by governments considering shutdowns?