Opening Up the Technical Aspects of Internet Shutdowns

Spotlight on South and Southeast Asia Cases

NOVEMBER 2022
EngageMedia is a nonprofit that promotes digital rights, open and secure technology, and social issue documentary. Combining video, technology, knowledge, and networks, we support Asia-Pacific and global changemakers advocating for human rights, democracy, and the environment. In collaboration with diverse networks and communities, we defend and advance digital rights.

Learn more at engagemedia.org.
Lead Writer
Ashraful Haque, Digital Security Specialist, EngageMedia

Advisory Team
Vino Lucero, Digital Rights Project Manager, EngageMedia
Red Tani, Program Director, EngageMedia
Egbert Wits, Program and Research Manager, EngageMedia

Report Editor
Katerina Francisco, Editorial Coordinator, EngageMedia

Published November 2022

This report has been produced by EngageMedia as part of the Greater Internet Freedom program work in South and Southeast Asia.

Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Understanding internet shutdowns</td>
<td>7</td>
</tr>
<tr>
<td>- Vital infrastructure or hardware failure/damage</td>
<td>8</td>
</tr>
<tr>
<td>- Routing</td>
<td>8</td>
</tr>
<tr>
<td>- Domain Name System (DNS) manipulation</td>
<td>9</td>
</tr>
<tr>
<td>- Filtering</td>
<td>9</td>
</tr>
<tr>
<td>- Throttling</td>
<td>10</td>
</tr>
<tr>
<td>Internet shutdown incidents in South and Southeast Asia</td>
<td>11</td>
</tr>
<tr>
<td>- Government justification for internet shutdowns</td>
<td>12</td>
</tr>
<tr>
<td>Civil society action on internet shutdowns</td>
<td>14</td>
</tr>
<tr>
<td>Conclusion</td>
<td>16</td>
</tr>
</tbody>
</table>
In August 2018, Bangladeshi students took to the streets of Dhaka to call for improvements in road safety after two teenagers were killed by a speeding bus. The peaceful protest turned violent as protesters clashed with police, injuring over 100 people. Photos and videos of police firing rubber bullets and tear gas at the crowd flooded social media. In an attempt to quell agitations and prevent more photos and videos from being uploaded online, the government ordered mobile phone operators to reduce internet speeds. Following the government order, internet monitoring organisation Netblocks confirmed that mobile networks were degraded to 2G speeds.

This is not the first time that the Bangladeshi government throttled the internet to restrict information sharing during controversial events and public disturbances. In 2015, the government temporarily blocked internet access and banned social media for a month after the Supreme Court upheld the death penalty for two opposition leaders convicted of war crimes.

Meanwhile in Southeast Asia, internet blackouts in West Papua have garnered international concern. In 2021, parts of the Indonesian province were cut off from the internet amid a long-standing dispute with the Indonesian government. Authorities claimed that broken undersea cables caused the disruption, but activists believe that it was intentionally done to hinder the pro-democracy movement. In previous years, similar unexplained internet outages have repeatedly occurred during critical moments such as protests or elections.

These incidents illustrate the different ways that governments can implement internet access restrictions to curtail people’s digital rights and weaponise these shutdowns to control dissent and movements on the ground. As these cases have shown, shutdowns can range from completely cutting internet access to partially disrupting connectivity, such as by reducing internet speeds.

Internet shutdowns have a significant impact on people's lives, especially considering the high degree of internet use in South and Southeast Asia combined. Network restrictions...
curtail people’s freedom of expression and access to critical information, forcing some to become “digital refugees” moving to other places for internet access. For businesses and public services such as schools and hospitals which rely on internet connectivity, internet shutdowns can severely disrupt normal operations.

Digital rights advocates and civil society actors need to understand how various types of internet shutdowns are technically implemented. By doing so, they will be better positioned to minimise the impact on affected populations and to gather evidence to hold perpetrators to account.

Drawing from and building on the existing literature on internet shutdowns and research efforts conducted by organisations such as Access Now and Jigsaw, this report breaks down the technical aspects behind several types of internet shutdowns and cites examples from cases reported in South and Southeast Asian countries. It also includes recommended actions that individuals and civil society members can take in the broader movement to safeguard and uphold freedom of internet access and digital rights.
Understanding internet shutdowns

#KeepItOn, a coalition of more than 200 organisations ranging from research institutions to advocacy groups, defines an internet shutdown as an “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”.

This definition widens the range of actions that can be considered an internet shutdown beyond the complete disconnection of internet access. Based on this definition, internet throttling and blocking social media and other online platforms are also considered internet shutdowns.

Internet shutdowns can be implemented at various points of the network. Understanding the execution point of an internet shutdown matters, since this informs the scope of affected populations. Depending on the aim of the network disruption, perpetrators zero in on particular execution points. Access Now, Jigsaw, and other organisations researching internet shutdowns have identified the following as some of the most common execution points:

- **Major international backbones** (submarine cables): The impact and scope of the network disruption are very high as this is one of the major internet structure backbones for most countries. Underwater optical fibre cable connections provide high-speed internet connectivity. If any damage or disruption occurs at this network point, all users and services hosted in the affected country will be impacted.
- **International Internet Gateways** (IIG): The impact of disruption is high to medium. IIG plays a very important role in internet connectivity in a country as it connects international internet traffic to the local network. A country can have multiple IIG providers. In Thailand, for example, there are 11 licensed IIG providers as of October 2022.
- Major national backbones (nationwide internet service providers): The impact of network disruption is medium to low. Internet service providers (ISPs) with
nationwide coverage act as the service provider for smaller local ISPs. As such, if disruptions occur at this point all the users connected to their network will be affected.

- Local ISP: The impact of disruption is low. Local ISPs provide internet connection to certain areas and there is typically more than one local ISP in operation. Network disruptions at the local ISP level will affect only the users connected to the network of the affected ISP.
- Single mobile phone tower: The impact of disruption is low. Network disruptions at this level result in a very targeted shutdown, as only the subscribers of the targeted cellphone tower will be affected.

As mentioned earlier, an internet shutdown can range from complete access restrictions to partial network disruptions. The following are some of the most common types of internet shutdowns, along with some examples from South and Southeast Asian countries:

**Vital infrastructure or hardware failure/damage**

This type of internet shutdown is caused by the failure of or damage to physical communications infrastructure or hardware necessary for communications and internet services. An example would be the physical destruction of a power grid or cellphone tower. In this type of infrastructure failure, it is often difficult to determine whether the shutdown was intentional.

In January 2022, Netblocks reported that several central Asian countries including Uzbekistan, Kazakhstan, and Kyrgyzstan suffered loss of connectivity for hours due to a widespread power outage.

**Routing**

On the internet, routing refers to the way that internet protocol (IP) packets of data travel from their origin to their destination. The routing paths are decided by network hardware called routers.
The manipulation of network routing is a simple but effective way to shut down the internet in a specific area or country-wide. This is done by altering the route information at key points (for example, international gateways) so that network traffic is blocked and does not pass beyond the controlled infrastructure. Instructions are sent to key routers, directing all requests to a null route (also known as a blackhole route) to and from a list of autonomous system numbers (ASNs), which are unique global identifiers for network IP ranges within a specific country. All traffic to or from the ASNs list will then be dropped along the blackhole route instead of being forwarded to the intended destination.

Domain Name System (DNS) manipulation

DNS is a naming system that translates human-readable domain names (like google.com) to machine-readable IP addresses (like 142.251.32.46). The internet's DNS system works much like a phone book by matching domain names to IP addresses. It also controls which server users will reach when they type a domain name into their web browser.

Manipulating DNS information can cause the shutdown of targeted services. This happens when DNS information is manipulated to direct users to either a non-existent server or a server controlled by the perpetrator. For example, if a user intends to visit twitter.com, the shutdown perpetrator would direct internet traffic away from Twitter's servers so the user is unable to access the website.

This can also be done through DNS hijacking, in which DNS servers return false mappings of domains to IP addresses. As a result, a user receives the IP address of a blocked page or a notice that the domain name is non-existent.

Filtering

In this type of shutdown, commercial filtering appliances and transparent proxy devices are used to block access to internet services. Based on recent cases, filtering has been more commonly used to block specific communications platforms.
These filtering devices work by analysing the metadata from network traffic and then allowing or blocking access based on that metadata. For purposes of censoring sensitive material, perpetrators typically set up filtering devices to look out for the following metadata attributes: source and destination IP address, destination domain name, source and destination port, full resource path, resource file extension, and keywords, among others.

Other ways to filter internet traffic include Deep Packet Inspection (DPI), in which network data is inspected and screened. If the data packet is found to be non-compliant with criteria set by the shutdown perpetrator, the data packet is blocked from passing through the inspection point.

Internet shutdowns through filtering are common, as seen in countries like Bangladesh. It has been used to block access to platforms such as Facebook, Twitter, or WhatsApp. This type of shutdown is very easy to implement, but also easy to bypass using a virtual private network (VPN).

Throttling

In this type of shutdown, the flow of data through the network is restricted, but not completely stopped. Access to the internet or particular services is slowed down so as to render the service or resource effectively unusable; for example, by downgrading mobile internet to 2G or capping data speeds.

Some ways to throttle internet connections include Quality of Service (QoS) throttling by a protocol and limiting bandwidth by source or destination IP addresses, IP subnets, VLANs or MAC addresses. This type of internet shutdown has been implemented multiple times across South and Southeast Asia, notably in West Papua.
Internet shutdown incidents in South and Southeast Asia

2021 saw an increase in internet shutdowns worldwide. Access Now and the #KeepItOn coalition documented at least 182 incidents in 34 countries, an increase of 23 incidents compared to the previous year.

Several countries from South and Southeast Asia comprised some of the top offenders among the surveyed countries. In 2021, 128 internet shutdowns were recorded in Afghanistan, Bangladesh, India, Indonesia, Myanmar, and Pakistan. Topping this list was India with at least 106 recorded incidents, followed by Myanmar with at least 15 incidents, although the true figure is likely higher.

The table below shows the recorded internet shutdown incidents in South and Southeast Asia over the last four years:

<table>
<thead>
<tr>
<th>Country</th>
<th>2021</th>
<th>2020</th>
<th>2019</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bangladesh</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>India</td>
<td>106</td>
<td>109</td>
<td>121</td>
<td>134</td>
</tr>
<tr>
<td>Indonesia</td>
<td>2</td>
<td>-</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Myanmar</td>
<td>15</td>
<td>1</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>Pakistan</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>12</td>
</tr>
<tr>
<td>Philippines</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>-</td>
</tr>
<tr>
<td>Vietnam</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Data collected from Access Now #KeepItOn reports

Although the number of incidents in these countries appears to be on the decline, the figures – especially for India and Myanmar – remain concerning. Additionally, this data represents only the incidents collected and recorded mostly by volunteer-run initiatives. Given the repressive political environments in some of the places where internet shutdowns have been recorded, the true figure of all shutdown events is likely to be higher.
Government justification for internet shutdowns

Based on recent cases, governments in South and Southeast Asia have typically resorted to internet shutdowns for national security reasons, to ease tensions during periods of social or political unrest, or to control information flow during elections or other high-stakes events.

In recent years, Bangladesh has restricted internet access several times for various reasons, including to quell protests, control instability over religious tensions, and prevent rumours and propaganda in the lead-up to the national elections. Thousands of websites have been blocked as part of an anti-pornography war, while news sites were shut down over national security concerns.

India has consistently ranked among the top offenders in cutting off the internet. In August 2019, authorities imposed an internet shutdown in Jammu and Kashmir after the Indian government stripped the region of its autonomy status. The shutdowns persisted until 2021 when at least 85 shutdowns were implemented, purportedly as a “counterterrorism measure”. The government also shut down the internet to suppress the Farmers’ Protests in 2021, a mass movement against controversial agricultural reforms.

Myanmar imposed at least 15 internet shutdowns in 2021, when the military staged a coup against the country’s democratically-elected government. Amid public protests, the junta ordered telecommunications companies to block social media and internet access. To circumvent restrictions, activists have turned to VPNs, but the junta has recently moved to reintroduce a draconian measure that would regulate the use of VPNs.

Citing security concerns, Pakistan has denied internet access in restive border regions, including imposing years-long internet shutdowns in Federally Administered Tribal Areas (FATA). Between 2016 and 2021, about 4.5 million people were unable to access the internet.

In April 2022, Sri Lanka blocked social media platforms such as Facebook, Twitter, WhatsApp, YouTube, and Viber in an attempt to contain protests over a worsening economic

OPENING UP THE TECHNICAL ASPECTS OF INTERNET SHUTDOWNS
Anti-government hashtags had been trending on social media platforms as the country battled public anger over severe shortages in essential resources and soaring prices of goods.

As these cases have shown, cutting or slowing down internet access and limiting access points to information enable authorities to assert control or maintain power during restive periods. However, sweeping measures like internet shutdowns have become more of a collective punishment rather than a tactical response for ensuring public order and safety, and are violative of fundamental rights that people should be able to freely enjoy.
Civil society action on internet shutdowns

Internet shutdowns significantly impact people’s lives: intentional network disruptions bar people from exercising freedom of expression and peaceful assembly, and from accessing and sharing information, especially during times of crisis. Shutdowns disrupt productivity and economic opportunities, as well as educational opportunities for thousands of students. Internet shutdowns also put lives at stake during an unprecedented health crisis, and keep rights violations hidden from view, such as during the Myanmar coup when at least 38 protesters were killed during a nationwide blackout. In countries with authoritarian governments, internet shutdowns can act as a veil obscuring the true extent of the situation on the ground.

Tracking, monitoring, and reporting on internet shutdowns is important to raise public awareness, direct international attention, and hold perpetrators accountable for rights violations. To this end, several organisations and coalitions have released reports and resources to record shutdown incidents:

- Access Now’s Shutdown Tracker Optimization Project (STOP), in collaboration with the KeepItOn coalition, tracks and records internet shutdowns and publishes annual public reports.
- The Open Observatory of Network Interference (OONI) is an open-source system run by a global volunteer community documenting internet censorship worldwide. The project currently includes an easy-to-use mobile app that measures the blocking of websites and apps. Test results are published as publicly-available data on the OONI Explorer, enabling the real-time tracking of censorship events around the world. OONI also partners with several organisations to publish research reports, including a 2017 study on the state of internet censorship in Thailand produced in collaboration with Sinar Project and the Thai Netizen Network.
- The Internet Outage Detection and Analysis (IODA) project monitors the internet to identify macroscopic internet outages affecting the edge of the network. The project originally began at the CAIDA at the University of California San Diego, and is currently continued by the Internet Intelligence Research Lab at the Georgia Institute of Technology.
• **Censored Planet** collects data using multiple remote measurement techniques in more than 200 countries to determine the presence or absence of censorship.

• Through its Transparency Reports, **Google** publishes data on traffic to its products, documenting real-time access disruptions that indicate shutdowns.

• The **Sinar Project**, **East-West Management Institute**, **EngageMedia**, and **OONI** are supporting the **Internet Monitoring Program** (iMAP), which measures network interference and restrictions of freedom of expression online in several Asia-Pacific countries.

Beyond monitoring and reporting on shutdown incidents, activists can respond to network disruptions in real-time by using a variety of apps and tools. During an ongoing shutdown, using VPNs can bypass internet access restrictions implemented through routing, DNS manipulation, and filtering. To communicate with others when messaging apps have been blocked, offline messaging apps such as **Briar**, **Bridgefy**, **Meshenger**, or **Serval Mesh** are useful tools. It is also important to gather evidence on the ongoing shutdown by running the **OONI Probe** on a mobile phone or on a computer. The data will be recorded as publicly-available data and can be useful in supporting advocacy initiatives for restoring internet access.
Conclusion

The increasing prevalence of internet shutdowns across South and Southeast Asia indicates the deteriorating state of digital rights in the two regions. While state perpetrators often invoke national security as justifications for restricting or blocking internet access, shutdowns tend to have the opposite effect, worsening confusion and stoking conflict.

By restricting communication channels and the free flow of information, network disruptions further shrink online civic spaces and undermine people’s rights to exercise freedom of expression. Civil society organisations play a critical role in raising awareness of these issues, working together to counter internet restrictions, and putting pressure on authorities to hold perpetrators accountable for these rights violations.

By documenting internet shutdowns and increasing public knowledge and awareness on circumventing and reporting access restrictions, digital rights advocates and civil society can more effectively strengthen ongoing efforts to resist this form of digital authoritarianism.
EngageMedia.org/
Greater-Internet-Freedom