August 2026

Shutdown Trends from 2019 to 2025

Where Do We Go from Here

Internet Society and Conexion Segura y Libre

Internet Society

Table of Contents

Executive Summary

Internet shutdowns have emerged as a prominent instrument for governments to impose sweeping digital censorship or manage perceived emergencies.[1] Ordered or carried out by governments, these deliberate disruptions of Internet access silence dissent, disrupt economies, and sever people from essential services, often without public justification or legal accountability.[2]

The Keep It On Coalition defines an Internet shutdown[3] 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. Internet shutdowns restrict freedom of expression, information, and association, as well as economic, social, and cultural rights. In many situations, the restricted communications and information flows can put people's health and safety at risk.

This reflects a broader human rights concern. In 2016, the UN Human Rights Council directly condemned "measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law," calling on countries to refrain from and cease them (Resolution A/HRC/RES/32/13).

Tracking shutdowns is therefore critical for improving Internet resiliency, documenting patterns of digital repression, and understanding a rapidly evolving threat to human rights online.

This report highlights Internet shutdown trends from 2019 to 2025, and was part of a larger effort to audit and update the Internet Society Pulse shutdown dataset. The work by the VEsinFiltro team at Conexion Segura y Libre supported data migration efforts, strengthened data consistency, and evaluated Internet shutdowns using a new scale of verification levels.

The analysis finds that Asia and Africa are the most severely impacted regions, accounting for the most Internet shutdown events and the longest cumulative durations across the dataset. Overall, the reviewed incidents span 61 countries across five continents, reflecting the global scale of the problem.

---

[1] OHCHR, Internet Shutdowns: Trends, Causes, Legal Implications and Impacts on a Range of Human Rights, UN Doc. A/HRC/50/55 (Geneva, 13 May 2022), https://www.ohchr.org/en/documents/thematic-reports/ahrc5055-Internet-shutdowns-trends-causes-legal-implications-and-impacts

[2] OHCHR, Internet Shutdowns: Trends, Causes, Legal Implications and Impacts on a Range of Human Rights, UN Doc. A/HRC/50/55 (Geneva, 13 May 2022), https://www.ohchr.org/en/documents/thematic-reports/ahrc5055-Internet-shutdowns-trends-causes-legal-implications-and-impacts

[3] KeepItOn https://www.accessnow.org/no-internet-shutdowns-lets-keepiton/ (1 April 2016)

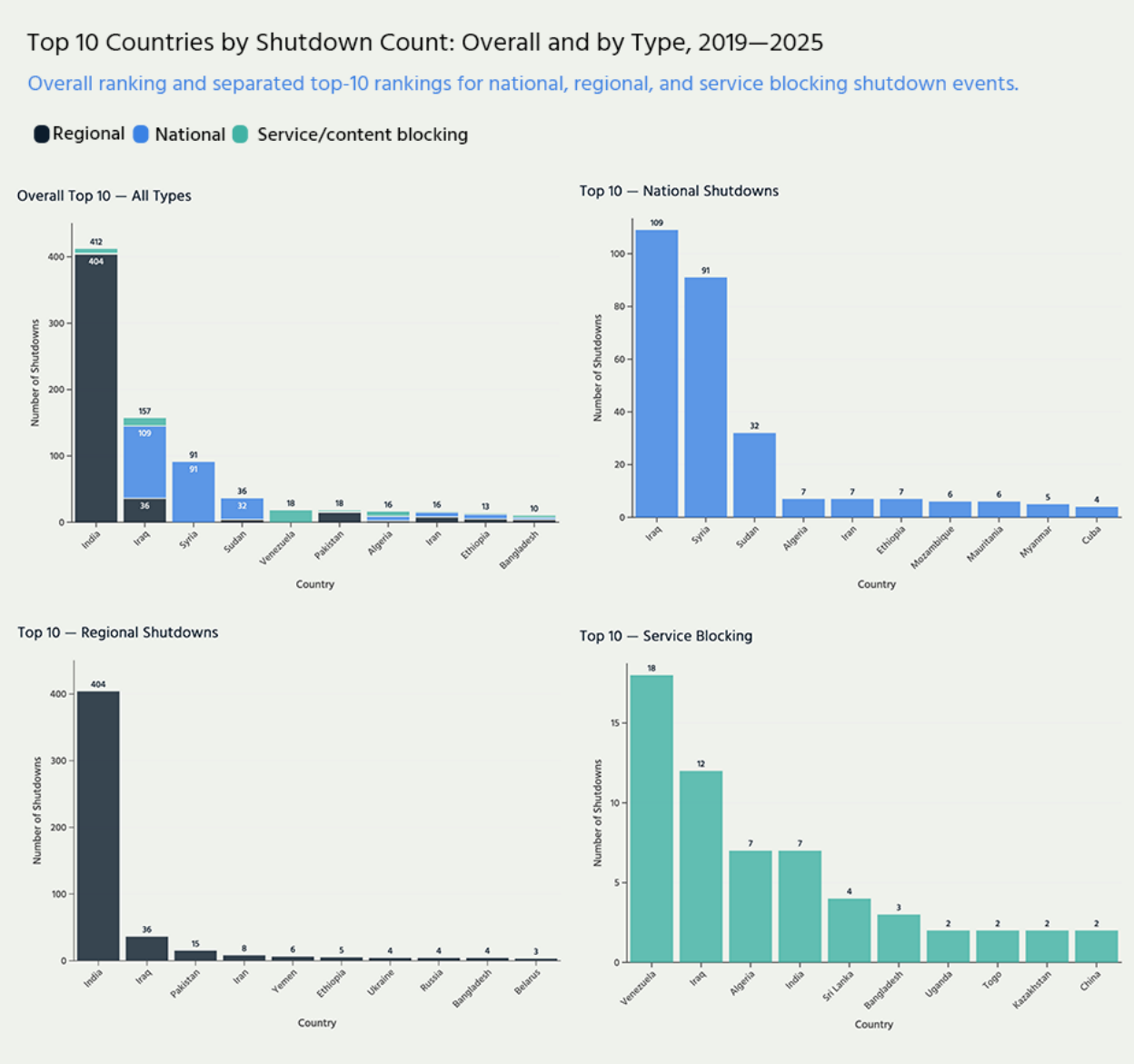

Figure 1: Top 10 countries by total shutdown count (2019–2025)

India is by far the country that has implemented the most Internet shutdowns, over twice as many as the next country, Iraq. India's shutdowns are almost exclusively regional, often affecting specific districts and local administrative areas below the state level.

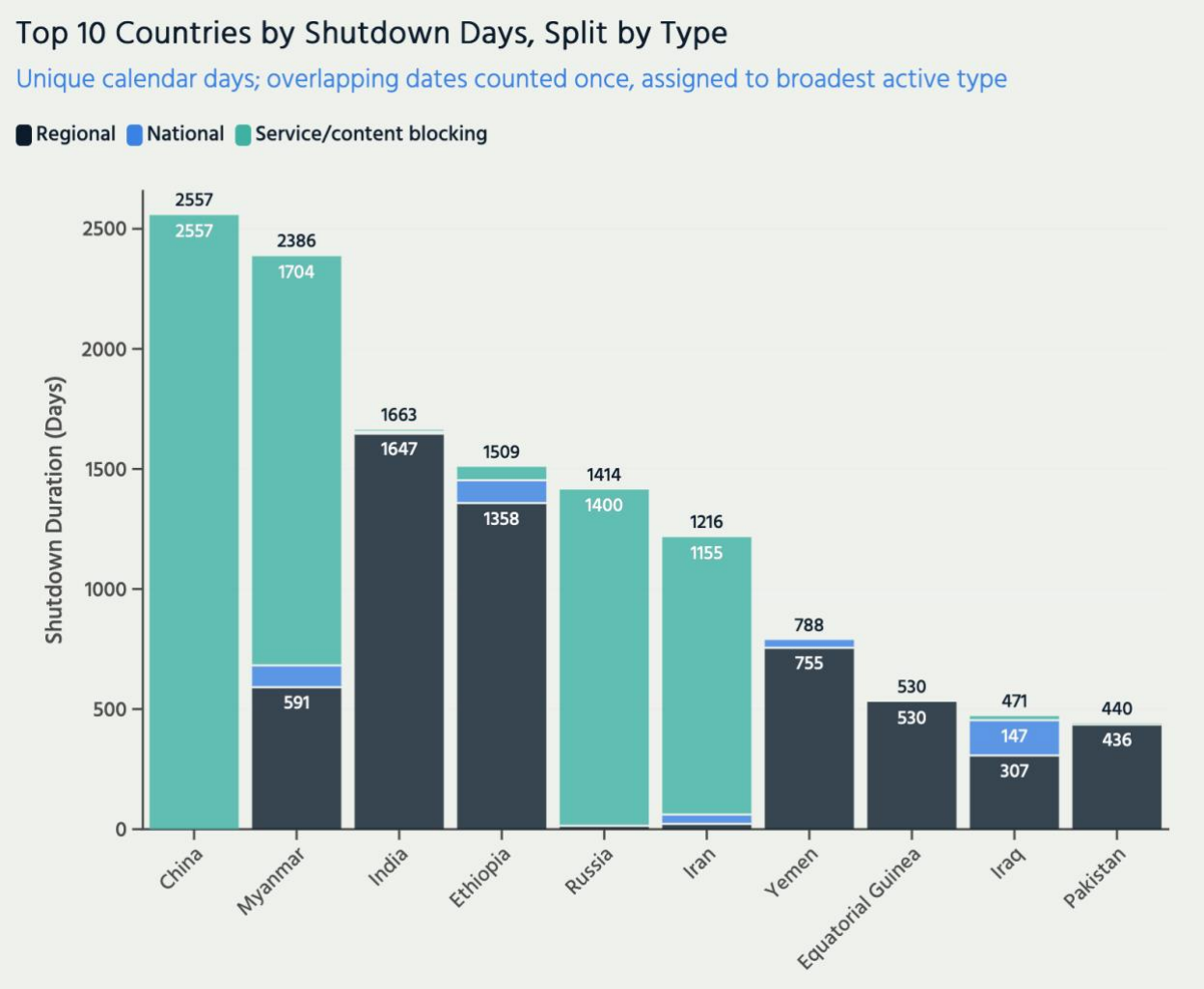

Figure 2: Top 10 countries by total time implementing a shutdown (2019–2025)

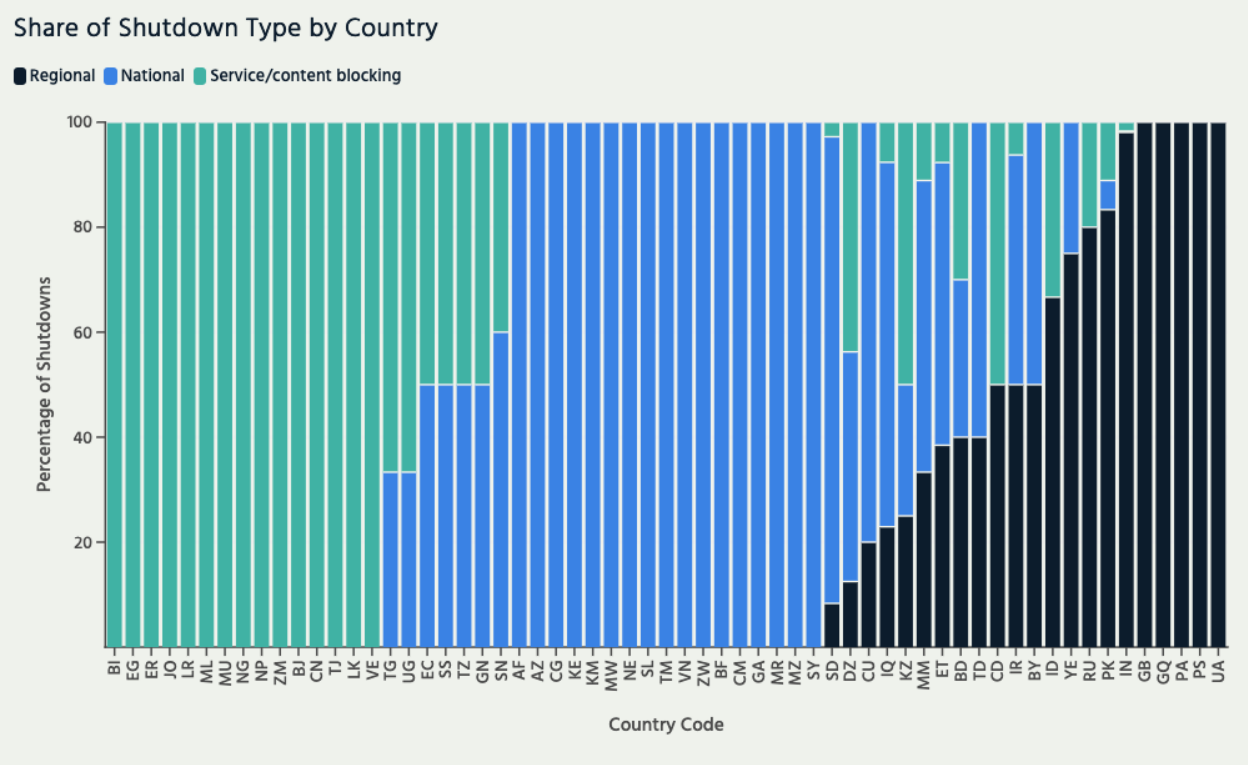

Figure 3: Share of shutdown type by country

The countries that spent the most time under shutdown conditions are not necessarily the same as those with the highest count. Using calendar days,[4] counting overlapping shutdowns only once, the country with the most days under an Internet shutdown is China, from the longest-running case in the dataset.

The analysis in this report highlights the growing challenge of distinguishing deliberate disruptions from unintentional outages caused by critical infrastructure failures.

The report also identifies a concerning normalization of Internet shutdowns and related restrictions. This includes long-running blocks, such as those documented in China, Myanmar, and Iran, as well as the emergence of increasingly routine justifications, notably the use of shutdowns during public exams in countries like Algeria, India, Iraq, and Syria.

Brief by Design, Permanent by Choice

Internet shutdown durations exhibit a highly asymmetrical distribution (Figure 4). Across the dataset, 70.8% of incidents lasted one day or less, and 95.4% of all shutdowns ended within 30 days. This trend is consistent across various shutdown types, suggesting that most shutdowns are designed as temporary

[4] This report uses elapsed time, instead of calendar days affected by a shutdown unless otherwise noted like in this instance when ranking total days of Internet shutdown.

interventions: tools deployed at specific events, such as national school exams, or at moments of heightened political sensitivity.

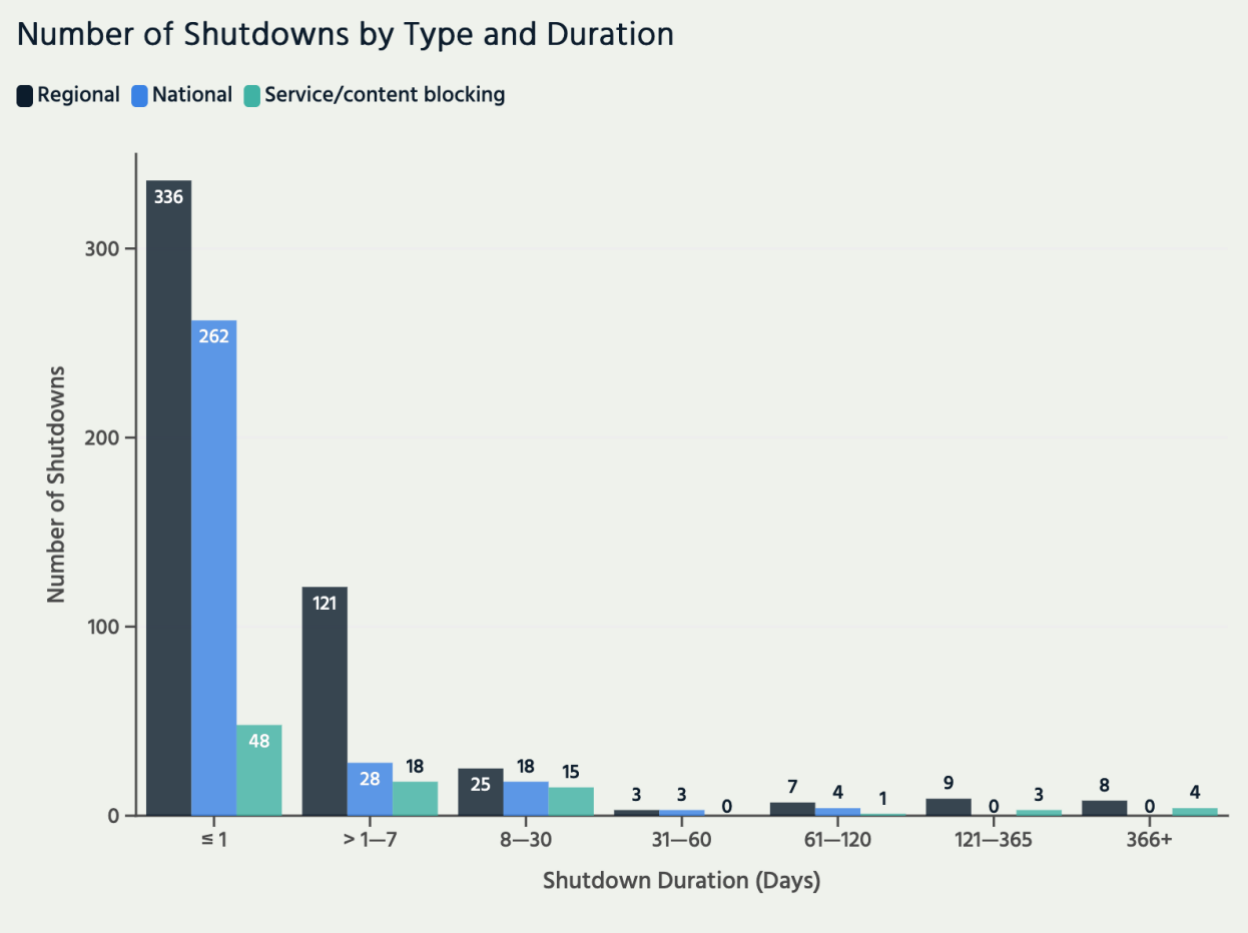

Figure 4: Distribution of shutdown durations by type

Broken down by type, the pattern is similar. Regional shutdowns, the most frequent type (55.8% of recorded shutdowns), tend to be brief: 89.78% lasted less than a week and 94.70% less than 30 days. National shutdowns are even more concentrated at the short end—83.1% lasted a single day or less, and the longest reached 102 days—reflecting their use as a targeted, time-limited instrument of control. Note: this doesn't include the 2026 national Internet shutdown in Syria.

Content and service blocking present a different profile. While many blocking incidents are also short-lived, the cases that persist tend to last for years: active blocking incidents have a median duration exceeding 900 days. The longest case in the dataset reached 2,556 days by the end of 2025 and is still ongoing.

This contrast underscores a structural difference in how governments use each shutdown type. They tend to deploy national shutdowns as acute interventions. Regional shutdowns last longer on average, as they limit the practical, economic, and reputational impact of the restrictions. And service blocking shutdowns are more likely to become long-term censorship.

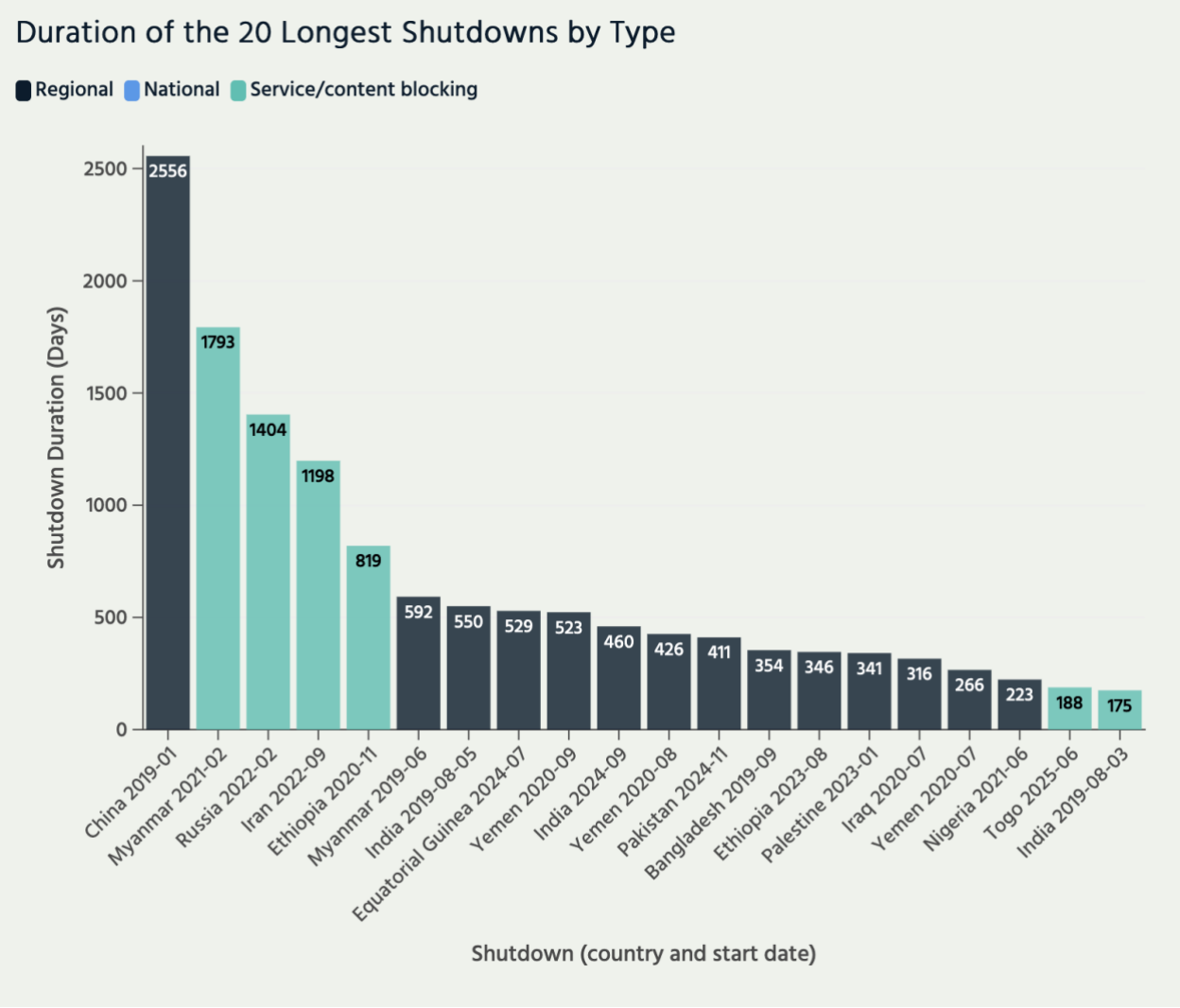

Figure 5: Top 20 longest Internet shutdowns by duration (2019–2025)

An analysis of the 20 longest incidents reveals two key patterns. The first involves service blockades with national reach and structural political motivations, in countries such as China, Iran, Myanmar, and Russia. These four cases share common characteristics: all were triggered by government action, all affected social media and communication services, and three of them remain active at the time of this analysis. The second corresponds to prolonged regional shutdowns that occur more frequently, accounting for 14 of the 20 cases, linked to armed conflicts or internal tensions.

The Longest Service Blocking Shutdowns

The four longest shutdowns in the period we analyzed are long-term blocks of essential communication tools that severely impact the rights of Internet users and keep them isolated from the global community. Even the fourth-longest case, Iran, lasted 1.5 times as long as the fifth case in the list, setting this group apart from the rest of the dataset.

China's Blocking of International Social Media and Many Internet Services

The longest shutdown recorded is the ongoing block of major Internet services in China, including Google, Facebook, YouTube, Instagram, and WhatsApp. Pulse has tracked the block from 1 January 2019, but it started well before then.

The government implements these long-standing blocks on major platforms, as well as many other websites and services, through a combination of sophisticated systems commonly known as the “Great Firewall” of China.

Local search and social media products often offer experiences similar to their global counterparts while complying with local government censorship and surveillance requirements. In addition to restrictions on social media, the blocking of search engines severely limits the content accessible on the Internet in China. Freedom House rates China's Internet as “Not Free” in its Freedom on the Net report.

Internet blocks and other restrictions limit and isolate Chinese Internet users within what the Internet Society has described as a national intranet.

Russian Block of Social Media Since 26 February 2022

Two days after Russia's full-scale invasion of Ukraine, on 26 February 2022, the Russian government began issuing orders to block social media and news outlets providing critical war coverage. X (formerly Twitter) was throttled first, then fully blocked on 4 March. Facebook followed on 3 March, Instagram on 13 March. Independent Russian news outlets, including Dozhd and New Times, and foreign media, including the BBC, Deutsche Welle, and Voice of America, were blocked in parallel. The incident has lasted 1,404 days as of the end of 2025 and remains ongoing.

Open Observatory of Network Interference (OONI) data shows that blocking is implemented in a decentralized manner, with each Internet service provider (ISP) responsible for executing government-mandated blocks independently, resulting in variation across networks. In 2024, YouTube throttling was additionally reported. Freedom House classifies Russia as "Not Free" in its Freedom on the Net report.

Block of Social Media in Myanmar Starting 2 February 2021

Myanmar's military junta blocked social media platforms, including Facebook, X (formerly Twitter), and Instagram, starting on 2 February 2021, the day after the coup d'état that deposed the elected government. After more than 1,700 days, this shutdown remains ongoing.

An analysis of OONI data by OONI, the Cooperative Association for Internet Data Analysis (CAIDA), and Myanmar ICT for Development Organization (MIDO) highlights a large number of TCP/IP anomalies, indicating that blocking of Internet Protocol (IP) addresses is the predominant blocking method. At the same time, some ISPs used Domain Name System (DNS) tampering to display block pages, suggesting that the implementation is decentralized.

Iran's History of Blocking Social Media, Communication Platforms, and More

The service-blocking shutdown in Iran, which started in 2022, is representative of a longer-standing pattern of selective service blocking that predates this dataset and periodically intensifies during moments of civil unrest. Shorter regional shutdowns also took place during the same period.

Censorship increased noticeably in September 2022, during the Women, Life, Freedom movement. OONI, Internet Outage Detection and Analysis (IODA), and FilterBaan have documented the blocking of WhatsApp, Instagram, Skype, LinkedIn, and search engines. Iran also blocked DNS over HTTPS (DoH) endpoints, as well as both the Apple App Store and Google Play Store.

On 8 January 2026, Iran fully shut down the Internet nationwide. The shutdown was initially motivated by protests and later appeared to be linked to the U.S.–Israel airstrikes. It remains ongoing.

Prolonged Regional Cases

Of the 20 longest shutdowns, 14 are regional shutdowns. These cases are concentrated in Sub-Saharan Africa, South Asia, the Middle East, North Africa, Afghanistan, Pakistan, and Myanmar. Nearly all are linked to armed conflict, military operations, prolonged internal disputes, or severe political instability.

Ethiopia alone accounts for multiple events, including the Tigray shutdown, which lasted approximately 819 days during the region's devastating civil war. India's Jammu and Kashmir appears in the dataset with a shutdown exceeding 550 days—the longest recorded in a democracy—which the government imposed after revoking the region's autonomous status in August 2019.

Sudan and Yemen provide examples related to ongoing conflicts. In these two cases, armed conflict motivated Internet shutdowns, but the outages persisted long after the armed incidents that triggered them. For example, in Al Hudaydah, Yemen, a regional Internet shutdown began in September 2020 and lasted for 523 days.[5] The shutdown was triggered by Houthi insurgents sabotaging fiber optic cables during local offensives, cutting off communications to isolate liberated areas from the world.[6]

Motivations for Shutting Down the Internet

While Internet shutdowns are a disproportionate response that harms the integrity of the Internet and the societies that endure them, it is often possible to identify the motivations behind them.

The most general "trigger" for an Internet shutdown is "government action": an intentional government order that can't be confidently attributed to more specific government motivations. Government

[5] Internet Society, Regional shutdown: Districts of Hays and Al-Khokha, Yemen. Internet Soceity Pulse (24 September 2020). https://pulse.Internetsociety.org/en/shutdowns/yemen-3/

[6] Newsyemen. The Houthis isolate the liberated areas of Hodeidah from the world cut off communications and Internet services. https://newsyemen.net/new/61675

action accounts for the majority of incidents, with 389 cases. However, its prevalence has steadily declined since 2019, when it peaked at 119 cases, falling to 22 cases in 2025.

Several factors may account for this downward trajectory. It likely reflects an evolution in the underlying incentives for state-ordered disruptions, as well as changes in how governments publicly disclose or justify them. The trend may also partially result from the growing difficulty of retrospectively identifying specific triggers when reviewing and standardizing older shutdown records.

Conversely, exam-related shutdowns have increased significantly, becoming the most prominent factor in recent years. From 17 cases in 2019, exam-related disruptions rose dramatically to 85 in 2024 and remained high in 2025, at 59. This pattern indicates a normalization of preventive restrictions as a tool to mitigate cheating.

Shutdowns linked to protests follow a different trend. After peaking in 2019 with 49 cases, incidents dropped sharply, but have seen a moderate resurgence in 2024, with 23 cases. This suggests that, while large-scale restrictions linked to protests have become less frequent, they remain a persistent response to periods of political instability.

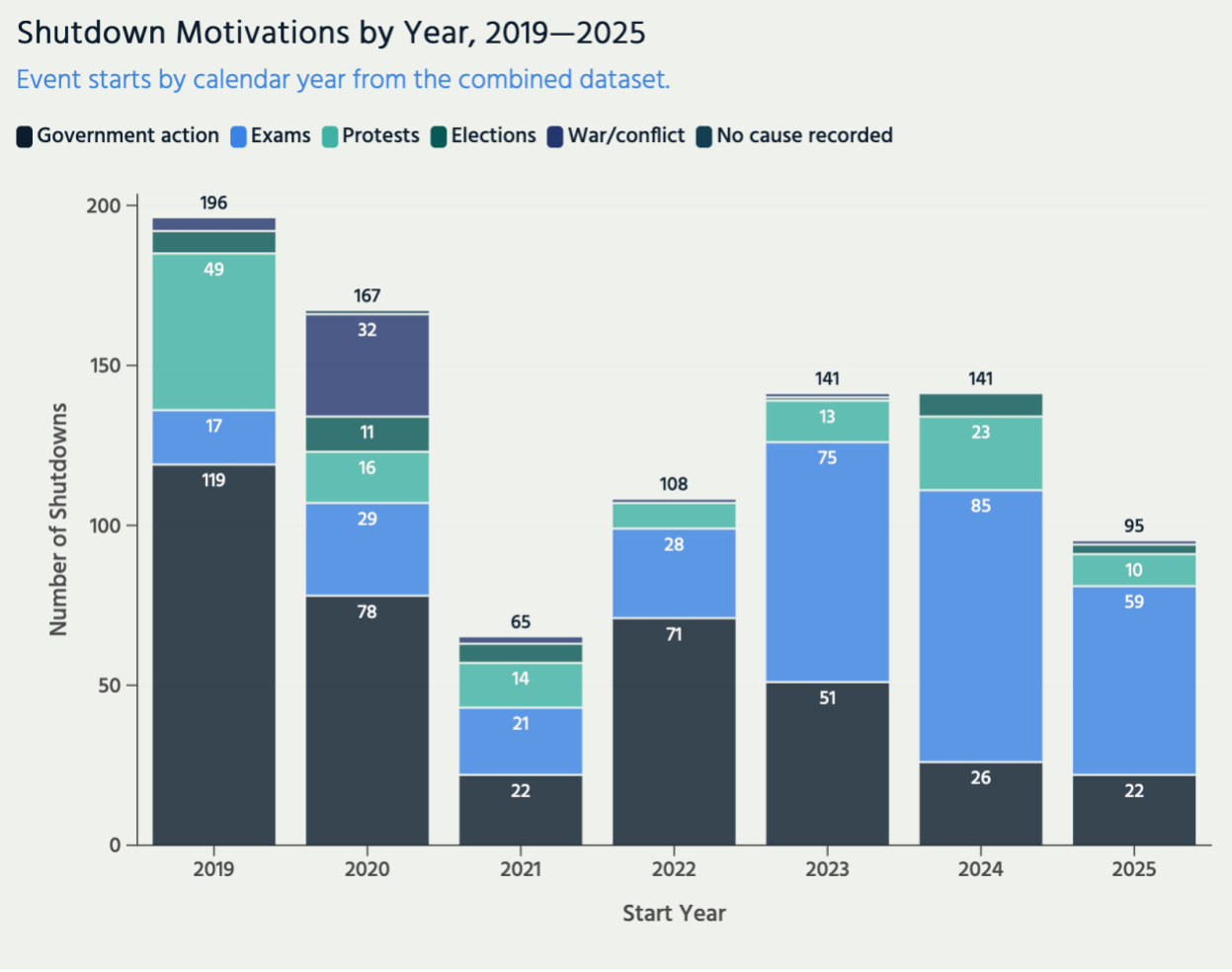

Figure 6: Internet shutdowns by trigger (2019–2025), showing a shift from government-driven disruptions toward exam-related shutdowns

A Failing Grade on Exam-Related Shutdowns

Between 2023 and 2025, the largest increase in stated justifications for Internet shutdowns was related to exams. These restrictions, which seek to minimize cheating during public exams, are most notable in Algeria, India, Iraq, and Syria.

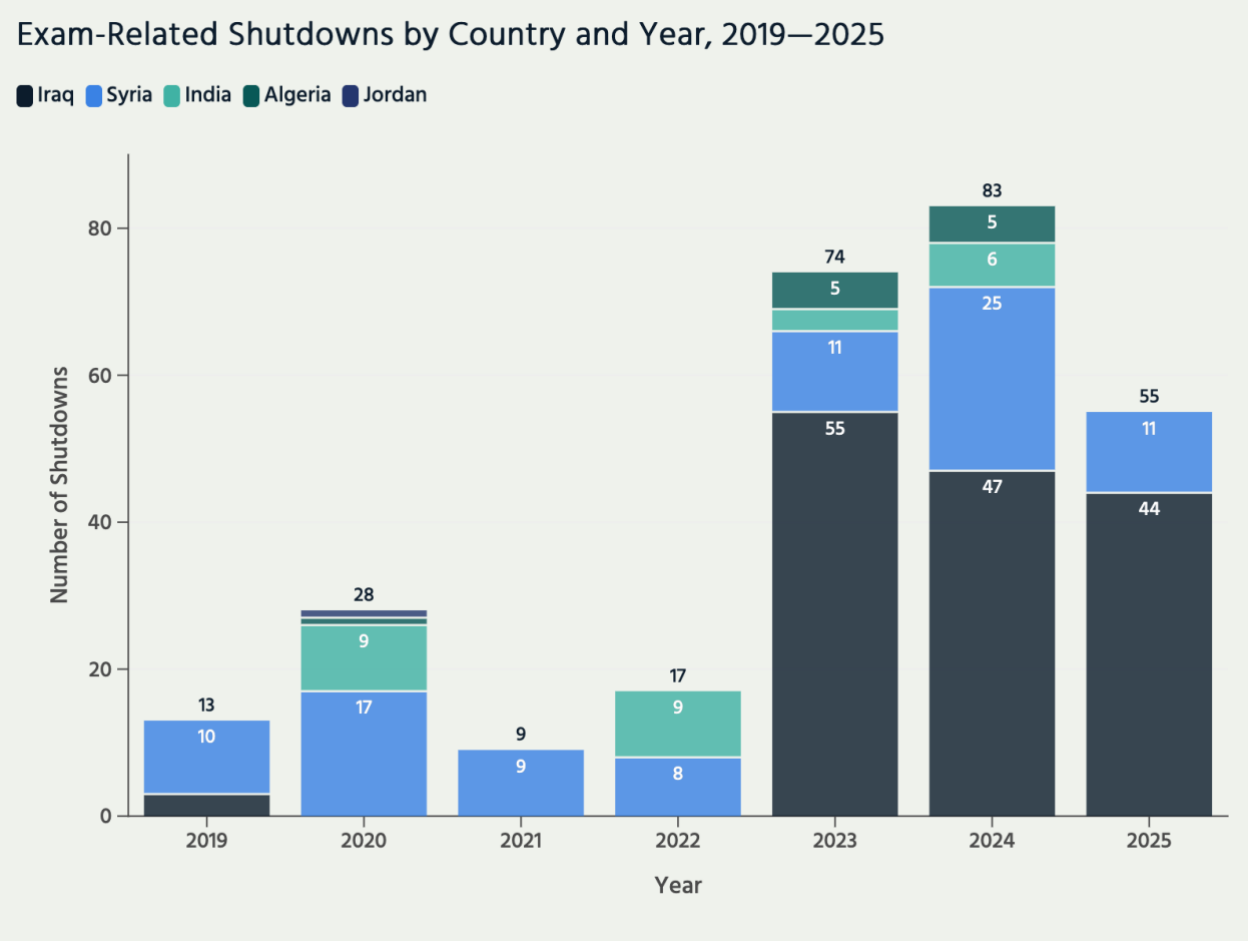

Figure 7: Exam-related shutdowns by year: Algeria, India, Iraq, and Syria (2019–2025)

Shutting down the Internet is a disproportionate action with wider implications. It affects Internet-dependent services and activities far beyond the exam context, including essential communications, economic activity, and government services. It also limits learning opportunities for other students who may be studying for unrelated courses or relying on online resources independently.

Authorities order these shutdowns during major exams to minimize cheating. However, the Internet is far from the only tool students can use, and it is not even the only communication method they can abuse for these purposes. Conventional cellphone calls using discrete earpieces and microphones have been documented, and in some instances, Bluetooth and Wi-Fi communication could remain effective even without Internet access. This casts doubt not only on the justification for these measures but also on their efficacy.

The Internet needs to be fully available to benefit users and societies. If residents of a country start to view the Internet as a resource that is only accessible sometimes, it can reduce trust and confidence in it, limiting the Internet's contribution to the country's social and economic development.

Geographic Trends

Internet shutdowns vary significantly by country and region, with overall trends in length, type, and the motivating factors that led governments to impose them.

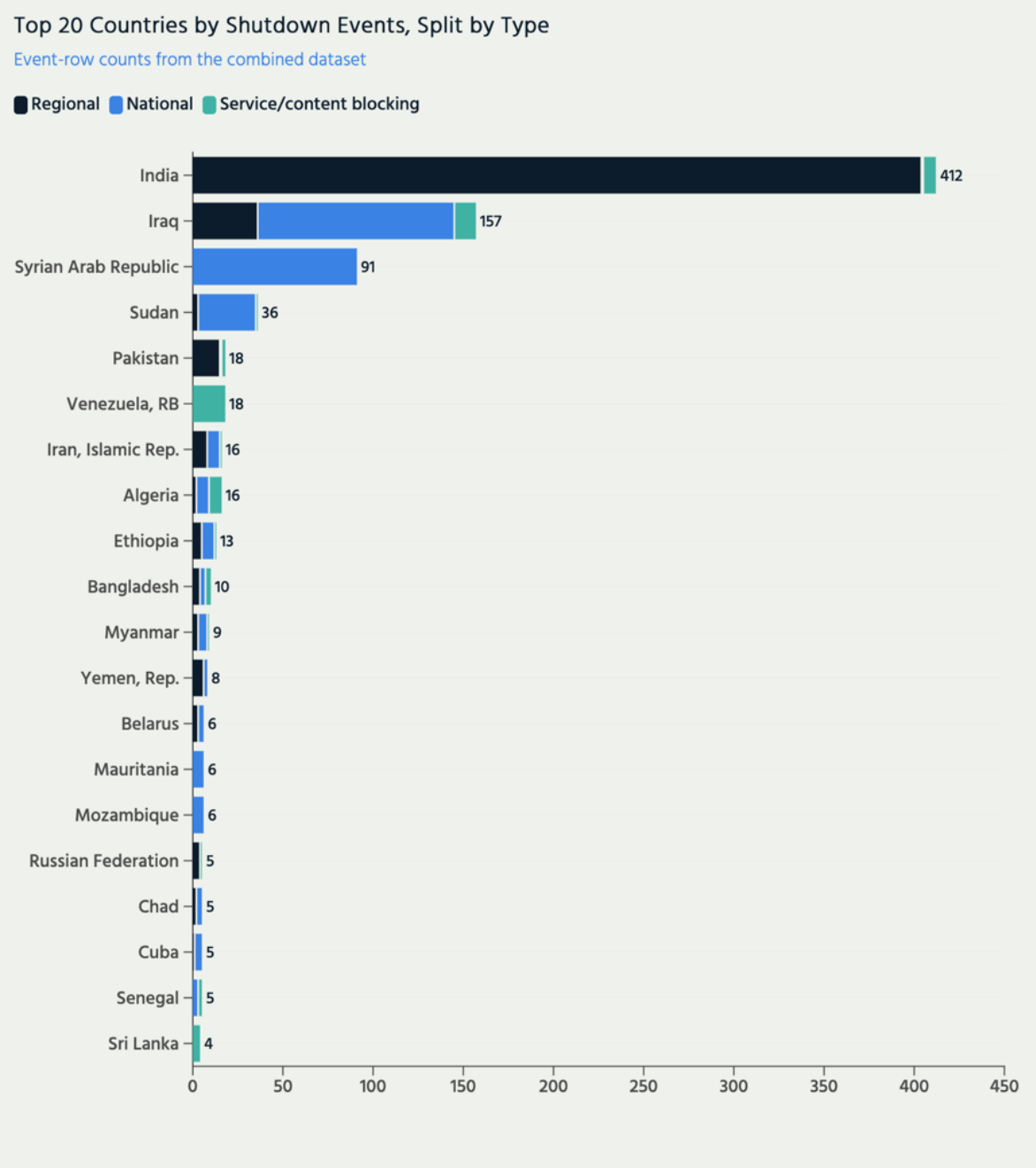

Figure 8: Top 20 countries by shutdown events and type

Figure 8 shows a marked preference for certain types of Internet shutdowns in some countries. Most notably, India, the country with the largest number of individual Internet shutdowns, mostly implements them regionally. Countries like Iraq, Syria, and Sudan mostly ordered nationwide shutdowns, while Venezuela, during the period of analysis, only implemented shutdowns by blocking communications and social media platforms.

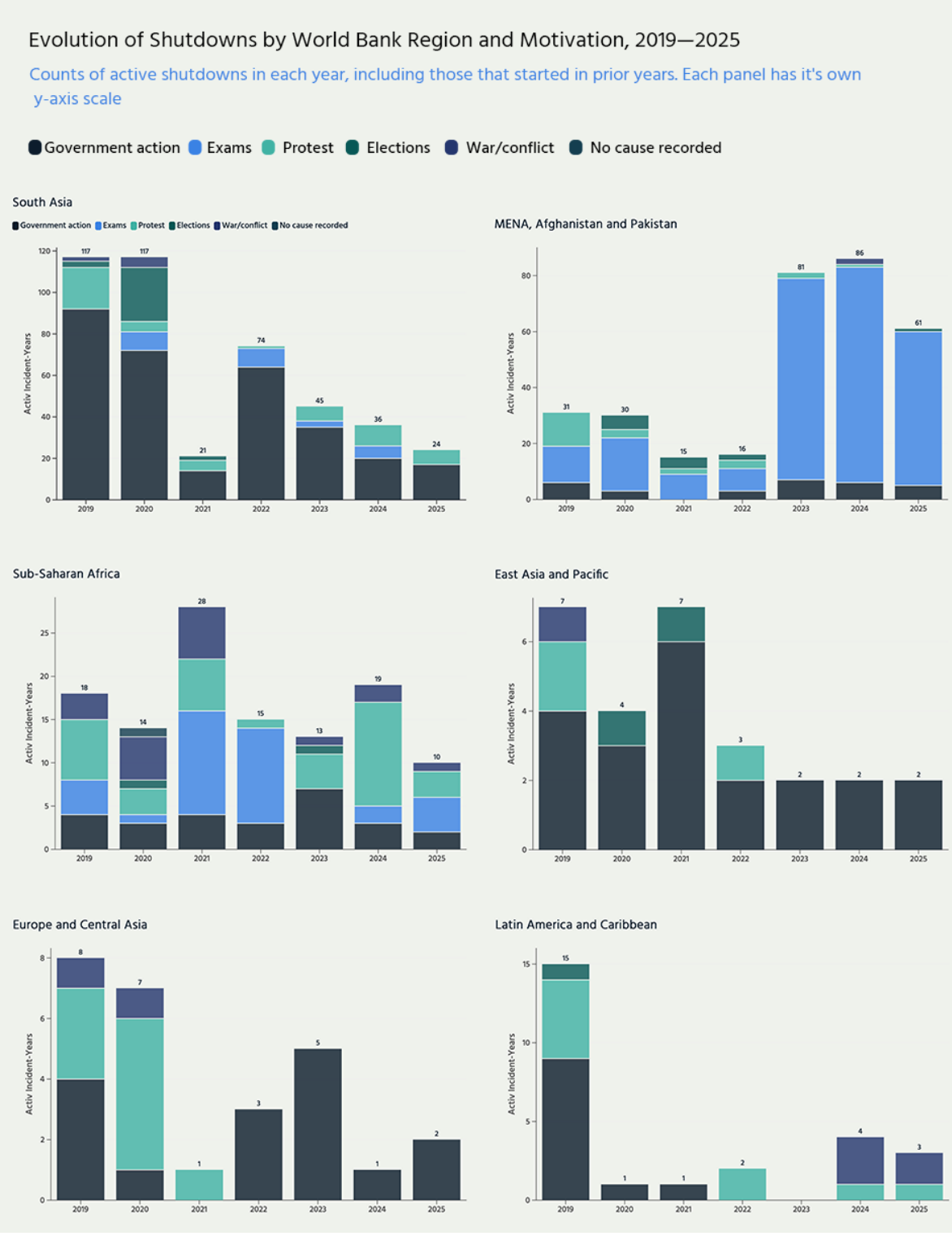

Figure 9: Evolution of active Internet shutdowns 2019-2025 by motivating factor, grouped by World Bank region. Counts represent active incident-years, meaning a shutdown is counted in each year during which it was active, including long-running or ongoing cases.

North America is the only region without recorded Internet shutdowns, while South Asia has the largest number of individual shutdowns, accounting for 48.8% of the dataset. East Asia and the Pacific have fewer shutdowns overall, but have several of the longest-running shutdowns.

Sub-Saharan Africa shows a declining trend of Internet shutdowns in the dataset, with a wide mix of motivating causes. The Middle East, North Africa, Afghanistan, and Pakistan, despite shutdowns with many motivations, had 81.1% of shutdowns related to public exams, a growing trend during the evaluation period. Latin America and the Caribbean had relatively few Internet shutdowns, concentrated primarily between Venezuela and Cuba.

While this is a topic for research on its own, it seems that in countries where shutdowns get normalized, they become a recurring response by authorities. And in some instances, the use of shutdowns by other countries in the region seems to reinforce their use in others.

This is the case of Internet shutdowns motivated by attempts to protect the integrity of public exams, which are especially prevalent in the Middle East and North Africa, as well as in Afghanistan and Pakistan. They have not only increased in number, but also in the number of countries implementing them over time.

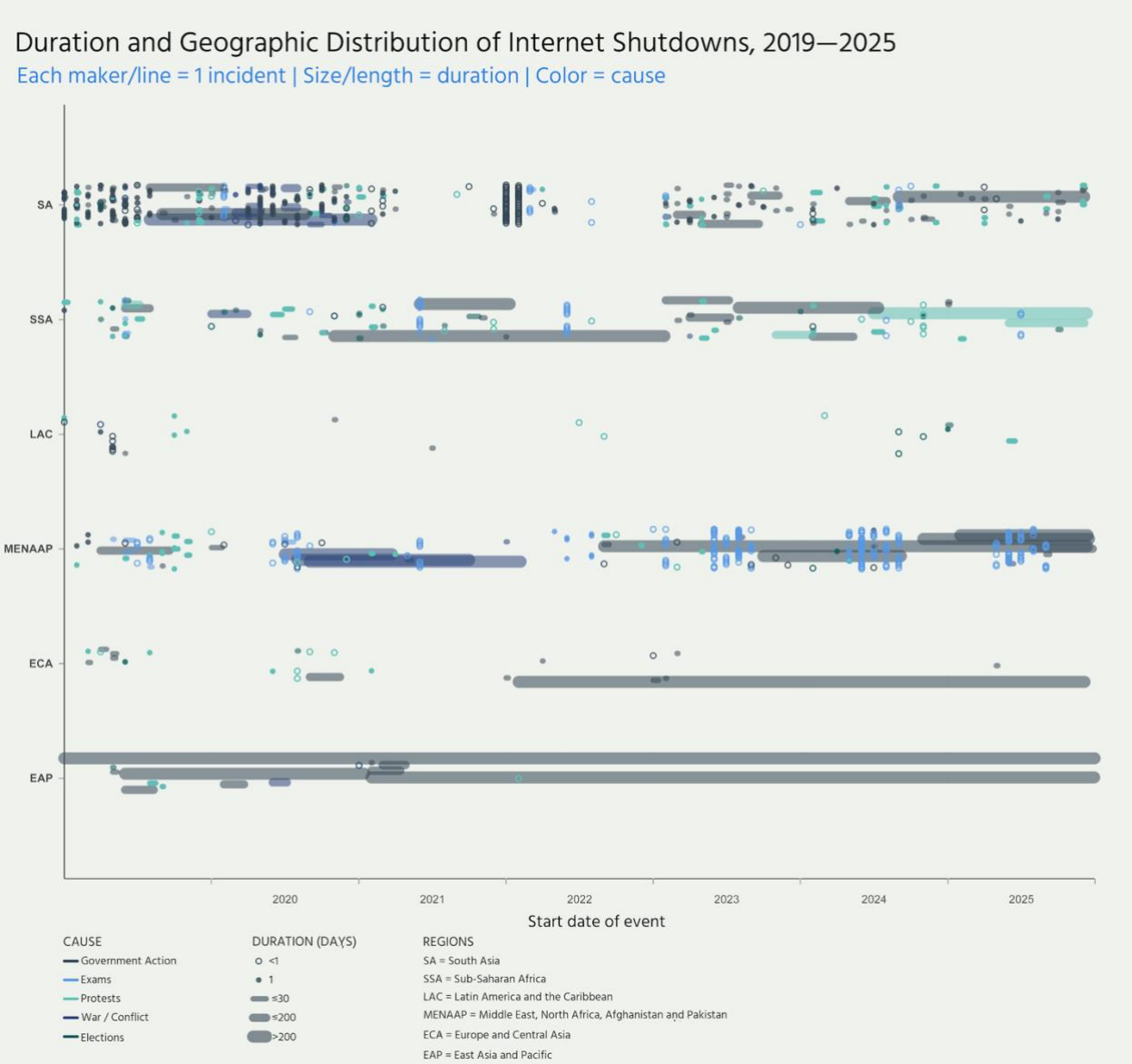

Figure 10: Shutdowns from 2019 to 2025 and the time they were active, by region and motivation

The temporal overlap of multi-month shutdowns within specific regions (Figure 10) suggests shared patterns of regional security pressure, political instability, and crisis response. It may also point to a possible peer-influence effect, in which authorities observe or adopt restrictive practices used by neighboring states.

To test this, we asked: among countries that had not previously implemented an Internet shutdown in the dataset, were they more likely to implement one for the first time if a bordering country had a shutdown in the previous year?

The strongest association appeared among countries sharing a land border. Among countries that had not previously used an Internet shutdown, the probability of adopting their first recorded shutdown

was 9.5% when at least one bordering country had an active shutdown in the previous year. By comparison, the probability was ~1.0% among countries with years without such border exposure.

The analysis used country-year combinations from 2020 to 2025. A country-year was considered eligible to be its first shutdown if the country had not recorded a shutdown before that year. The year of a country's first recorded shutdown remained eligible, while subsequent years were excluded. For each eligible country-year, we checked whether it was exposed to at least one land-border neighbor having an active shutdown in the preceding year (including exposure in 2019). The risk associated with this exposure was the ratio of exposed first-time country years and all exposed country-years eligible to be a first-time shutdown.

The ratio between the risk of a first-time shutdown when exposed vs unexposed is 9.14 (risk exposed ÷ risk unexposed). In practical terms, the observed probability of first-time adoption of a shutdown was about nine times higher in countries with prior-year border exposure than in countries without it. The absolute difference was 8.4 percentage points.

Border Prior-Use Association by Overall, Type, and Motivation

Exposure: A land-border neighbor had an active shutdown in the prior year. Type/motivation rows use-category prior shutdowns.

		Lower first-use probability	Higher first-use probability	Difference	Ratio
Overall	Any shutdown	Border		+8.4 pp	RR 9.14
Type	National	Border		+4.3 pp	RR 3.63
Type	Regional	Border		+1.9 pp	RR 3.52
Type	Service/content blocking	Border		+4.4 pp	RR 5.59
Motivation	Government action	Border		+3.1 pp	RR 4.71
Motivation	Exams	Border		+2.8 pp	RR 12.00
Motivation	Protests	Border		+4.8 pp	RR 4.93
Motivation	War/conflict	Border		+4.1 pp	RR 11.09
Motivation	Elections	Border		+4.6 pp	RR 6.28
Motivation	No cause recorded	Border		-0.1 pp	RR 0.00

Figure 11: Comparison of the likelihood of a first-time shutdown if a neighboring country shut down the Internet in the previous year. Overall, it shows whether any prior shutdown in a bordering country is associated with a country's first shutdown of any kind. Type and motivation: whether prior bordering use of the same shutdown type or with the same motivation is associated with first-time adoption of a shutdown of that specific type or motivation. RR: risk ratio compares the probability of a first Internet shutdown in exposed countries with that of unexposed countries (risk exposed ÷ risk unexposed).

This analysis does not account for all relevant political, security, legal, economic, or institutional variables. Bordering countries may face shared crises, regional instability, similar election cycles, cross-border conflict dynamics, or common policy pressures. The pattern does not establish causation, but suggests that future research and threat models should consider both shared regional political and security trends and the possibility of policy influence across countries.

Blurred Lines

Recent years, especially 2025, saw a worrying trend of large-scale outages at major content delivery networks (CDNs) and hosting providers, two markets that have seen dramatic centralization.

Large Internet service outages have a significant and growing impact on overall Internet resilience and can have consequences similar to Internet shutdowns, despite their different causes and nature. In places where conflicts or shutdowns are expected, they can easily be confused with one another.

This increasingly important phenomenon should be tracked to provide clarity to Internet users and to identify trends, both on their own and in relation to shutdowns and other related phenomena. Doing so would help stakeholders, including policymakers, understand their impact on Internet resilience.

Another important phenomenon to track is large-scale outages caused by damage to subsea and terrestrial fiber-optic cables, with an average of nearly 200 undersea cable faults per year. While many of these cable cuts are accidental, the alleged sabotage of backbone Internet infrastructure motivated by geopolitical tensions looms as a growing concern. It is hard to attribute and is part of a growing list of gray-zone tactics that affect Internet health and the rights of Internet users.

Outages from fiber-optic cable cuts have severe impacts on Internet resilience. Still, they can also be confused with Internet shutdowns, or, conversely, used as an excuse to deflect criticism of an intentional shutdown. This was the case in Kenya in 2024, when a likely Internet shutdown occurred during protests despite government denials of planned restrictions. ISPs blamed undersea cable issues, yet the disruption's intentionality remained suspect.

Other cases, such as the severe outage in Cameroon in 2025, also contribute to this confusion and help identify the need to track large outages. In this incident, both the state-owned CAMTEL and private ISPs attributed the disruption to a technical issue at a cable landing station. At the same time, some activists and social media users alleged that the government intentionally shut down the Internet in response to protests. Cameroon has shut down the Internet previously, including a 94-day Internet shutdown in 2017, before the start of the shutdown records in Pulse.

It is important to track large-scale outages caused by major hosting providers and CDNs, international fiber-optic cable failures, and suspected shutdowns caused by other countries. This would bring clarity

to affected Internet users, help identify trends for each of these phenomena, and also help identify their relation to intentional shutdowns. This way, all stakeholders, including policymakers, can see their trends and impact on Internet resilience.

Supporting Demands for Transparency and Accountability

This data audit introduced three categories representing a scale of verification. This structured approach is a significant improvement to the dataset, supporting the diverse needs of Internet users, digital rights activists, researchers, and policymakers working to address Internet access reliability and uphold human rights online.

Officially Acknowledged Shutdowns

Categorizing shutdowns officially acknowledged by governments, or in some instances by Internet service providers (ISPs), provides a more complete picture of documented events. By tracking whether shutdowns were acknowledged, we can better understand whether affected communities know why the Internet was unavailable, and which authorities tend to impose shutdowns without explanation.

The act of an institution publishing a restriction or publicly confirming an event is highly significant, as it allows for some public scrutiny and policy debate, even if the restriction itself is coercive.

This category is especially important as a reliable way to verify shutdowns, particularly those targeting smaller regions or specific networks where independent technical measurement might be ambiguous or difficult to conduct. In these cases, the official acknowledgment serves as evidence that the event occurred.

Confirmed Shutdowns

This category encompasses shutdowns that, although not officially acknowledged, have been robustly verified using data from independent, reputable network measurement organizations or documented by digital rights groups with in-house Internet measurement capabilities. In the case of Pulse, this primarily relies on a combination of Cloudflare Radar, IODA, OONI, and regional Internet exchange points.

Unconfirmed Shutdowns

The addition of unconfirmed shutdowns as a category supports the work of local organizations and Internet users by formally recognizing and documenting their reports of an Internet shutdown, even when full technical confirmation is not possible.

This category highlights on-the-ground reports and complaints. Local organizations and users are often the first to experience and report restrictions, sometimes providing initial technical evidence, such as screenshots of error messages or connection failures.

Inclusion in this category indicates that, for any reason, the event has been difficult to measure and independently confirm via technical means. This is often the case for:

- **Hyper-local Internet shutdowns:** restrictions affecting a very small geographical area or neighborhood.
- **Regions with low population density:** areas where the limited number of network probes makes statistically significant measurement challenging.
- **Sophisticated throttling:** restrictions implemented through highly targeted deep packet inspection or traffic shaping that is harder to detect than a complete network blackout.
- **Limited number of measurements:** for example, content restrictions blocking specific platforms that may require measurements from the vantage point of affected users, but there may be insufficient measurements available, and traffic data from the affected platform itself may not be public.

Other technical challenges often interact with the above. For example, shutdowns affecting mobile Internet tend to be more difficult to measure because they are often local, and traffic from mobile networks can be harder to geolocate than traffic from fixed ISPs.

By tracking these reports, even without full independent confirmation, this category empowers local activists. It acknowledges their experiences and serves as a vital indicator for future targeted research and technical monitoring, ensuring that no community's report of lost access is overlooked.

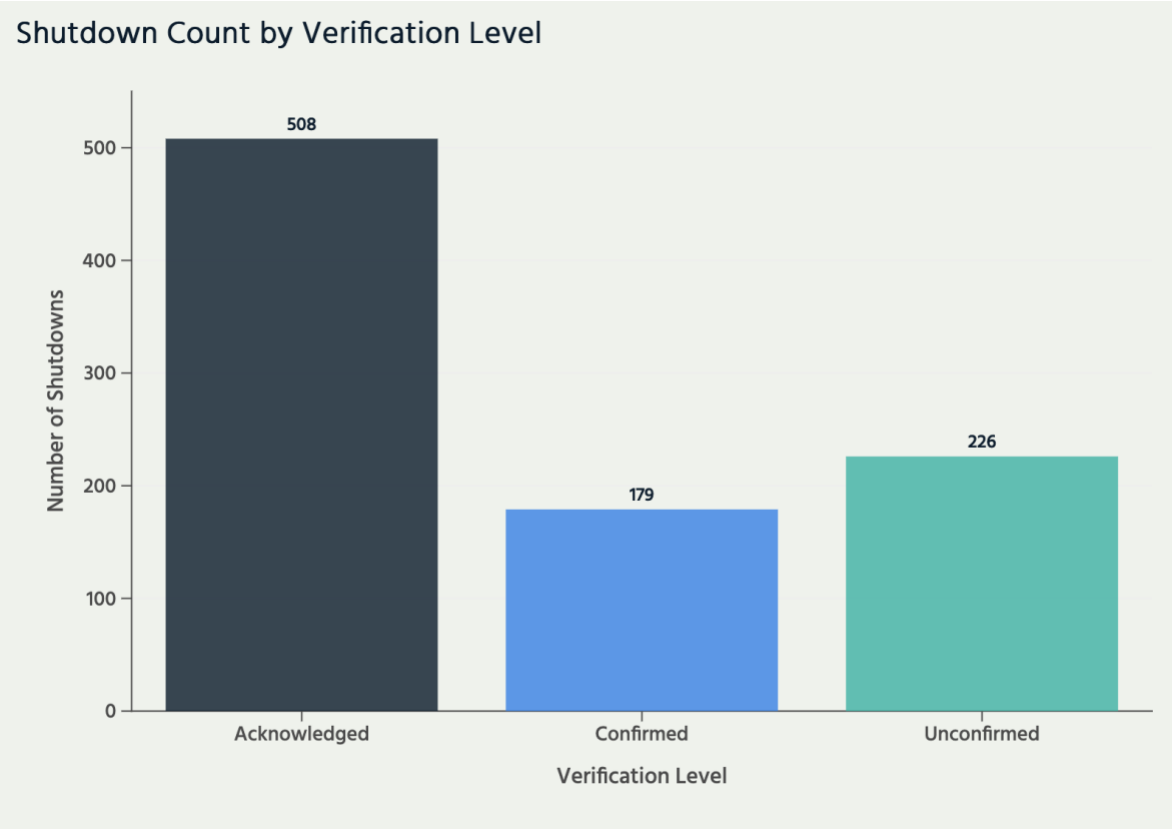

Figure 12: Shutdown count by verification level: acknowledged, confirmed, and unconfirmed (2019–2025)

It is currently unclear, and will require further research, whether there is a positive trend of increasing acknowledgment of Internet shutdowns. While this would be a hopeful sign, the goal remains a reduction in shutdowns and a more dependable, accessible, and human rights-empowering Internet overall.

On the Difficulties and Changes in Documentation and Measurement of Shutdowns

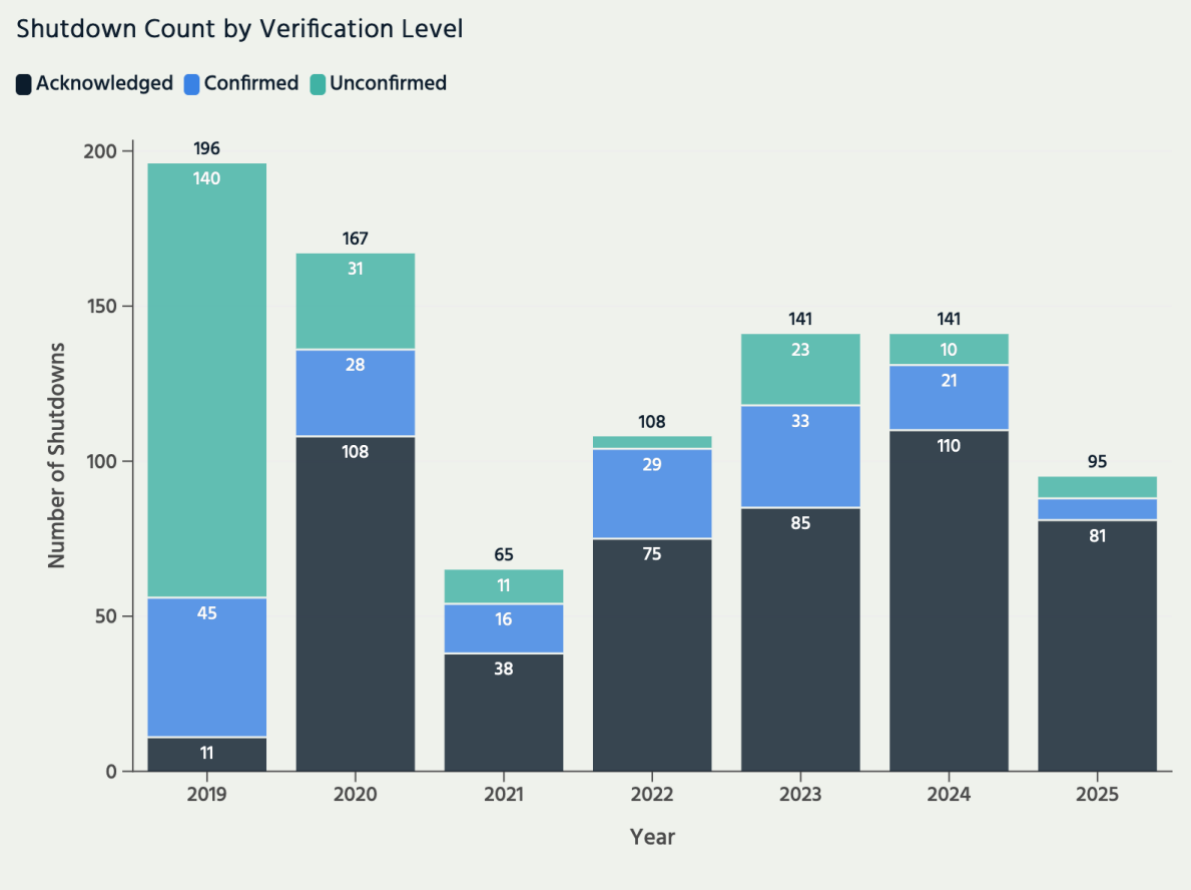

Figure 13: Number of shutdowns by verification level by year

Older shutdowns skew towards unconfirmed, as validating them is more challenging than verifying more recent shutdowns. This uncertainty comes from the availability of less technical evidence due to a less mature community, fewer network measurement tools at the time, and the loss of public access to older data.

Another possible contributing factor is that no reference to public acknowledgment of the shutdown was described in the dataset for these older cases, and finding evidence of the acknowledgment in late 2025 was much harder than for more recent events due to the greater time elapsed.

Some public tools that generate data have changed or disappeared over the years, leading to a loss of evidence, as old data from these platforms is no longer available. One example of a tool that was useful for analyzing outages and shutdowns but is no longer available is Oracle Internet Intelligence. Another example of data no longer being available is IODA data from before 2022.

Network measurement and shutdown-tracking initiatives need to ensure resilient access to their platforms and commit to long-term data access and availability, even after a project winds down or changes its scope, including national-level civil society projects.

It is also crucial to archive copies of official shutdown orders or other government communications to guarantee the future availability of these records, even when governmental entities remove original documentation from the public Internet or local news media coverage disappears.

The measurement community should make preservation efforts a top priority, making sure reports include backed-up datasets and static graphs for resilience. Embedded scripts that consult external APIs for dynamic graphs are excellent tools, but should include a more resilient static image as a fallback.

In the data audit of the Internet Society Pulse dataset, we leveraged new developments in IODA, specifically options for metrics at the sub-national administrative region level (such as state or province) by autonomous system number (ASN) and vice versa. This advancement facilitates the documentation and corroboration of local shutdowns, a task that has historically been very challenging to measure.

Large online platforms are often well-positioned to observe these local shutdowns, but typically do not provide public traffic or usage metrics, or if they do, the data is aggregated only at the national level. Greater access to this kind of granular data would significantly help to overcome the difficulty of measuring local shutdowns.

Conclusion

Internet shutdowns are broad, disproportionate actions that many governments resort to during times of crisis, political instability, or important events.

A small number of countries account for most recorded shutdown events, while a smaller set of long-running cases account for much of the cumulative time people spend under restrictions. Most shutdowns remain short, often lasting one day or less, but the dataset also shows the persistence of long-term service and content blocking that can isolate users for years.

The motivations behind shutdowns are also changing. Broad “government action” remains the largest category overall, but exam-related shutdowns have become increasingly prominent, especially in parts of the Middle East and North Africa. This normalization of shutdowns for routine administrative

purposes is particularly concerning because it treats access to the Internet as optional at a time when societies increasingly depend on it for education, work, services, and public life.

Reliable, transparent, and enduring shutdown documentation is vital. To ensure accountability, it's necessary to understand national and subnational shutdowns and to examine broader trends, including the influence of neighboring countries. Maintaining long-term preservation evidence, technical and otherwise, is fundamental to seeing trends and impact over time.

Deliberate shutdowns are not always distinguishable and are not the only phenomenon with a broad impact on Internet access and use. Their tracking can bring into sharper focus other ways connectivity fails, or even how the appearance of infrastructure failures can mask intentional disruptions.

Achieving this requires the persistent efforts of both global and local organizations that conduct network measurements, provide context for shutdowns, and document their various impacts.

The ongoing commitment of local groups, digital rights advocates, network measurement initiatives, and global Internet resilience projects remains fundamental to ensuring that shutdowns are properly recorded, analyzed, and contested.