Gaps in the Record: On the Observability and Documentation of Internet Shutdowns

Simon Cheek
Georgia Institute of Technology
scheek6@gatech.edu

Zachary S. Bischof
Georgia Institute of Technology
bischof@gatech.edu

Amanda Meng
Georgia Institute of Technology
a.meng@gatech.edu

Alberto Dainotti
Georgia Institute of Technology
dainotti@gatech.edu

1 Introduction

Since the Arab Spring [8], government-ordered Internet shutdowns and censorship events have received sustained attention from researchers, civil society organizations, journalists, and policymakers. A growing ecosystem of measurement platforms and documentation efforts, including AccessNow's #KeepItOn [1], Open Observatory of Network Interference (OONI) [14], CensoredPlanet [4], and Cloudflare Radar [7], have emerged to detect, document, and publicize these events.

Among these efforts, the Internet Outage Detection and Analysis (IODA) project [12] has provided publicly accessible views of Internet connectivity at the national, regional, and Autonomous System (AS) level. In addition to publishing connectivity data, IODA maintains a curated list of large-scale outages and shutdowns [10]. This list has become an important reference for researchers and advocates seeking to characterize shutdown activity over time and to characterize government-ordered shutdowns in comparison to other forms of large-scale connectivity disruption, such as spontaneous outages [3] (e.g., natural disasters).

In practice, documentation within IODA follows an alert-driven workflow. IODA's automated alerts based on network-level signals serve as the primary starting point for investigation and curation, with some events added through targeted manual analysis in response to external reports or queries. However, this also means that shutdowns producing subtle or atypical signal changes may affect end users without being captured in the event list.

In this paper, we look for trends in the observability of documented shutdowns for each of IODA's signals and identify gaps in shutdown documentation by comparing IODA's event list with other shutdown records. Focusing on government-ordered, nationwide shutdowns, we examine 73 events since 2022 reported by Access Now's #KeepItOn (KIO) that did not appear in IODA's event list. Our analysis identifies three recurring characteristics associated with these documentation gaps: (i) disruption of communications infrastructure during prolonged armed conflict, (ii) shutdowns that target a small number of networks providing end-user connectivity while affecting only a limited share of national address space, and (iii) large-scale application-layer blocking that is not consistently visible in IODA's connectivity metrics. Together, these cases highlight challenges of event documentation. We conclude by discussing potential changes to IODA's systems that we believe would most improve event coverage.

Free and Open Communications on the Internet 2026(2), 42–46

2 Data and Methodology

IODA began manually curating an event dataset in 2018 based on its network-level connectivity signals: BGP, Active Probing, and Telescope, which are described in the work of Bischof et al. [3]. The dataset includes events that satisfy one of the two conditions: (i) a prolonged and significant drop is clearly visible in at least two of IODA's signals, or (ii) a prolonged and significant drop is visible in one of IODA's signals and corroborated by an external, independent source.

To examine the coverage of IODA's documented events, we compare this dataset with Access Now's #KeepItOn (KIO) dataset [1], which provides a list of government-ordered shutdowns and censorship events based on first-hand reports, news coverage, official government orders, and observations from monitoring platforms such as OONI, Cloudflare Radar, and IODA itself. Because the KIO dataset includes event types beyond IODA's design scope (such as application-specific blocking) we restrict our analysis to KIO-reported events classified as national, full-network shutdowns.

Following the methodology of Bischof et al. [3], we label a KIO-reported shutdown as "IODA-matched" when it overlaps in time and location with an IODA-documented event. We use matched events to characterize trends in shutdown observability across IODA's signals, and unmatched events to investigate shutdowns absent from IODA's documentation. The IODA event dataset records whether a signal shows a visible (to the reviewer) drop and whether an automated alert fired; we use visible signal drops to quantify observability.

Dataset summary. Using the matched dataset, we first characterize shutdown documentation at the event level. We found that the fraction of KIO-reported shutdowns that are matched to IODA documentation increased from 13.3% to 33.9% between 2021 and 2024. This increase is driven largely by improved documentation of local and regional (i.e, subnational) shutdowns. Indeed, IODA's match rate for subnational KIO events increases from 3.4% in 2021 to 32.7% in 2024. However, these subnational matches are highly concentrated geographically: India and Iran together account for over 80% of matched local and regional events. As a result, improvements in event-level matching do not translate into comparable gains in country-level coverage, which declined over the same period.

Table 1: Overall number of countries per year with KIO-reported, nation-wide, full-network shutdowns and number of countries with at least one matching event documented by year (2018–2024).

Year	KIO Reported	IODA Matched	Match Rate
2018	21	8	38.1%
2019	25	15	60.0%
2020	25	14	56.0%
2021	30	18	60.0%
2022	23	6	26.1%
2023	26	5	19.2%
2024	34	7	20.6%

We next looked to identify countries that were under-documented. Table 1 summarizes, for each year between 2018 and 2024, the number of countries with at least one KIO-reported national shutdown and the subset of those countries with at least one matched IODA-documented event during the same year. While the total number of countries reporting shutdowns in KIO remains relatively stable over this period, the number of countries with at least one IODA-matched shutdown declines sharply, from 18 in 2021 to 7 in 2024. As a result, the country-level match rate drops from approximately 60% in 2021 to 20.6% in 2024.

To better understand the reason for these gaps in documentation, we compared both the KIO and IODA event datasets to all national-scale KIO shutdowns since 2022 that do not overlap with any documented IODA event, yielding 73 shutdowns absent from IODA's event list, which is the primary set of events we focus on for our analysis (see Appendix). In our analysis, we inspect IODA's connectivity signals for each of the 73 unmatched shutdowns. For each event, we examine IODA's publicly available dashboard [11] across the reported shutdown window, including BGP, Active Probing, and Telescope signals, as well as Google Search traffic where available. Additionally, we consulted Cloudflare Radar to provide complementary visibility into traffic patterns at both the national and network level.

3 IODA Observability Gaps

We begin by examining trends in how shutdowns documented by IODA manifest across its network-level signals, independent of alert triggering. For this, we replicate the signal-level observability analysis of [3], which examined, for each event, whether a significant drop was observable in each of IODA's three primary signals—BGP, Active Probing, and Telescope—distinguishing between government-ordered shutdowns and spontaneous outages.

We found that between 2018 and 2021 (years examined in [3]), shutdowns documented by IODA—defined as events matched to KIO-reported shutdowns in the same country and time window—almost always exhibit significant drops across all three signals. However, relative to this baseline, shutdowns in the 2022–2024 period are substantially less likely to produce observable drops in the Telescope signal. Table 2 outlines the proportion of each type of event in the corresponding time range that exhibits a visible drop in the given signal, with outages being defined as events observed by IODA but not KIO. We compare events in the 2018-2021 range (initially observed in [3]) with events occurring from 2022 through 2024 (the most recent well-documented time period). The fraction of shutdown events exhibiting observable drops across all three signals declines from over 94% in 2018–2021 to 51.8% in 2022–2024. While BGP and Active Probing each show a modest decrease in observability (approximately 4–5%), the decline in Telescope visibility is more pronounced, with only 54% of shutdown events exhibiting a detectable Telescope drop after 2022. We note that this change coincides with a transition in IODA's measurement infrastructure, including a migration of the network telescope from UCSD [5] to Merit [13], suggesting that the observed decline in Telescope observability may reflect changes in shutdown practices and measurement vantage points. Further analysis of the Telescope migration and its implications is left as future work.

Table 2: Percentage of shutdowns and outages with observed drops per signal, 2018–2021 vs. 2022–2024.

	2018–2021		2022–2024	
Signal	**Shutdown**	**Outage**	**Shutdown**	**Outage**
Active Probing	98.4%	97.7%	94.3%	92.8%
BGP	99.5%	92.0%	92.9%	93.2%
Telescope	96.2%	65.4%	53.9%	15.6%
All (AP∩BGP∩T)	94.5%	55.3%	51.8%	15.2%

To better understand the nature of shutdowns absent from IODA's event list, we next examine the set of national, full-network KIO shutdowns between 2022 and 2024 that do not overlap with any documented IODA event. Table 3 displays a distribution of the top countries containing unmatched KIO events, showing that a majority (53.4%) of these events can be attributed to seven countries. In a small number of cases, such as Iran and Sierra Leone, manual inspection of IODA dashboards reveals false negatives in documentation: drops are visible in multiple IODA signals and alerts were triggered during the reported shutdown window, but no event was documented. These cases reflect constraints in manual documentation capacity rather than limitations of signal observability, and we treat them as distinct from the observability gaps that are the focus of the remainder of this section.

When examining the reported sources associated with unmatched KIO events, we find that Cloudflare is cited in 65.7% of cases, followed by sources including Kentik, Internet Society Pulse, and OONI. Notably, IODA itself appears as an attributed source for over 20% of unmatched events, indicating that signal-level evidence of disruption was available within IODA's measurements even when the events were not formally recorded.

Ultimately, our examination of the remaining unmatched events identifies three recurring characteristics: shutdowns occurring in conflict-affected settings where background connectivity disruption complicates shutdown observability; shutdowns that target a small number of networks providing end-user connectivity while affecting only a limited share of national address space; and large-scale application-layer blocking that is not consistently reflected in IODA's network-level measurements. We examine each of these characteristics in detail in the remainder of this section.

Table 3: Countries with the most missed IODA detections for national full-network KIO events, 2022–2024.

Country	Missed Events	% of Total
Palestine	12	16.4%
Ukraine	8	11.0%
Myanmar	6	8.2%
Sudan	5	6.8%
Cuba	4	5.5%
Senegal	4	5.5%
Mauritania	4	5.5%
Other (18 countries)	34	46.6%

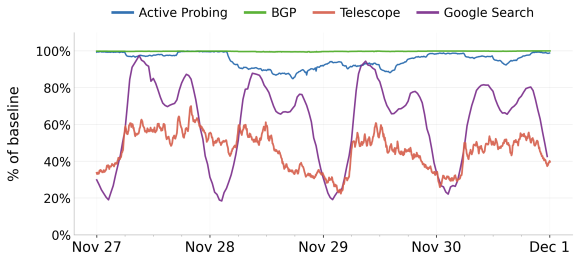

Figure 1: IODA signals for Ukraine, November 27-30, 2024

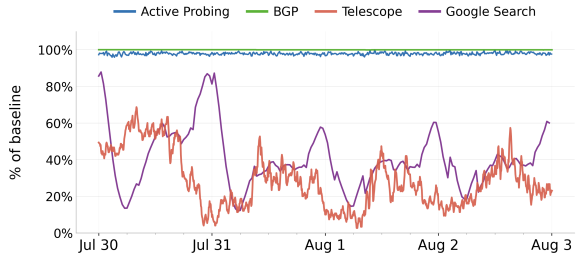

Figure 2: IODA signals for Senegal, July 29 - August 3, 2023

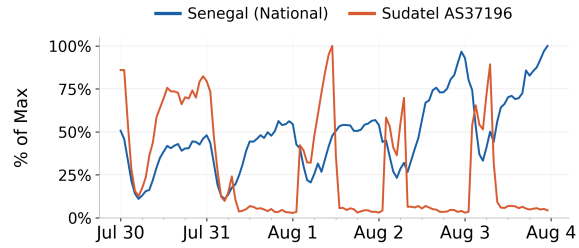

Figure 3: Cloudflare Radar for Senegal vs Senegal-Sudatel, July 30 - August 4, 2023. Reported shutdown begins on July 31st.

3.1 Armed Conflict

As shown in Table 3, the four countries with the greatest number of unmatched KIO events are Palestine, Ukraine, Myanmar, and Sudan. KIO attributes each to armed conflict: Palestine and Ukraine to destruction of energy and communications infrastructure, and Sudan and Myanmar to military seizure of ISP data centers and severed Internet lines, respectively [2].

Figure 1 depicts IODA signals for Ukraine in November of 2024, ranging from November 27th–30th. KIO reports a shutdown event beginning on the 28th: the Active Probing signal decreases from 100% to approximately 90% (still above IODA's alerting threshold), where it remains for the next few days. These shutdown events are visible, albeit difficult to detect algorithmically, as a subtle (even if stable) drop in Active Probing signal does not necessarily constitute an outage or shutdown. Each shutdown event we observed attributed to armed conflict exhibited distinctly different behavior overall. One example in Sudan contained an Active Probing signal that steadily dropped from 90% to 40% over the span of six days, presenting a challenge for algorithms to accurately identify since it was not a sudden drop. We also found that the recovery of shutdown events attributed to armed conflicts was more gradual in nature, lacking an immediate restoration of connectivity that other shutdowns typically exhibited.

3.2 AS-Targeted National Shutdowns

We examined 12 KIO events focused on blocking traffic from particular Autonomous Systems (ASes) within a country instead of all traffic within a country or region. For example, KIO reports a national, full-network shutdown in Senegal beginning on July 31st, 2023. IODA records no visible change in BGP or Active Probing signals, although it shows a drop in Google Search traffic. Figure 2 observes Google Search traffic for Senegal peaking at 30-40% lower daily than the days preceding the reported shutdown. Telescope signals hint at a similar decline, although in a much subtler manner.

We examined the Cloudflare Radar for Senegal in July of 2023, and found that both Senegal-Sudatel (AS37196) and Tigo (AS37649) saw traffic drop to near 0% during each outage window while national levels of traffic were largely unaffected, including traffic in Senegal's most populous AS, Sonatel (AS8346). Figure 3 displays the contrast between national Senegal traffic and Senegal-Sudatel during this time. This contrast in signal suggests the shutdown was scoped to specific providers, explaining why IODA's signals remained largely unaffected.

IODA's AS-level signals for Senegal-Sudatel showed little variation during the outage window, although IODA's coverage of Senegal-Sudatel is limited: Active Probing only observed 10-11 online /24 prefixes for Senegal-Sudatel during this window, compared to roughly 540 for Sonatel. The sustained drop in Google Search traffic nonetheless suggests a visible impact on national level traffic, despite no corresponding change in IODA's network signals.

3.3 Application Layer Blocking

In our investigation we also found patterns in unmatched KIO events that suggest targeted blocking of traffic. These are shown primarily in shutdown events resulting in significant drops in Google Search and Cloudflare Radar signals nationwide without affecting BGP, Active Probing, or Telescope signals.

Figure 4 shows IODA signals for Sudan during a KIO-reported shutdown occurring on a daily basis. Google Search traffic drops sharply for approximately two hours each day, but two distinct drops are visible per day. The first is a natural, smooth decline consistent with daily patterns in Sudan. The second is abrupt: before traffic can recover to its daily peak, it is suddenly cut off, then

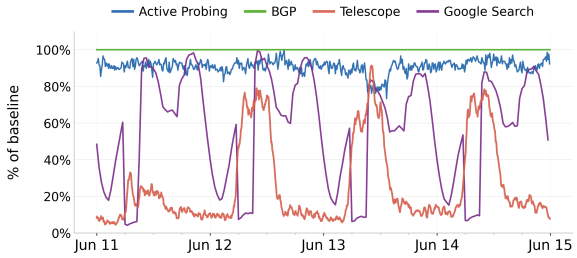

Figure 4: IODA signals for Sudan, June 11-14, 2022

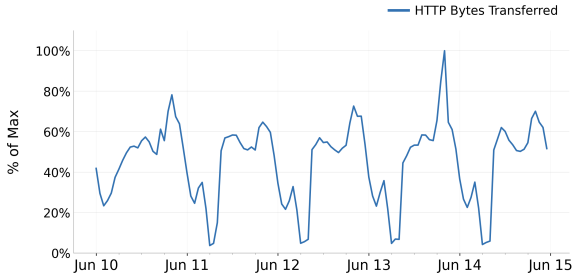

Figure 5: Cloudflare Radar for Sudan, June 10-14, 2022

restored just as quickly, a pattern consistent with a deliberate, time-bounded shutdown.

When compared with Cloudflare Radar in Figure 5, we observe a sudden drop in HTTP traffic, affecting the entirety of Sudan (not just AS-scoped). Despite these sudden and significant drops on a daily basis, almost no change in BGP or Active Probing signal is exhibited. Telescope signals rise during this time of day as is typical for Sudan, showing little to no reaction to the shutdown.

We observed several events matching this pattern, with nationwide impact visible in Google Search and Cloudflare Radar but no corresponding drops in IODA's BGP, Active Probing, or Telescope signals. The absence of changes in these network layer measurements raises uncertainty about whether these events involved full-network shutdowns (e.g., implemented through transport-layer filtering) or large-scale censorship operating at the application layer. Resolving this ambiguity would require further investigation with additional network-level measurements, which we plan to explore in future work.

4 Discussion

Many of the undocumented national shutdowns exhibit signal behaviors that challenge documentation initiated by alerts despite observable disruption. Figure 6 illustrates one such case, in which Active Probing, Telescope, and Google Search signals all exhibit sustained decreases that remain below IODA's alerting thresholds. Although these drops persist for multiple hours, their limited magnitude prevents the event from being surfaced through automated alerts, highlighting how shutdowns characterized by subtle or distributed signal degradation can evade documentation.

The diurnal nature of Telescope signals also contributes to the difficulty of shutdown detections. As shown in Figure 6, Telescope signals continue to increase during the likely shutdown window

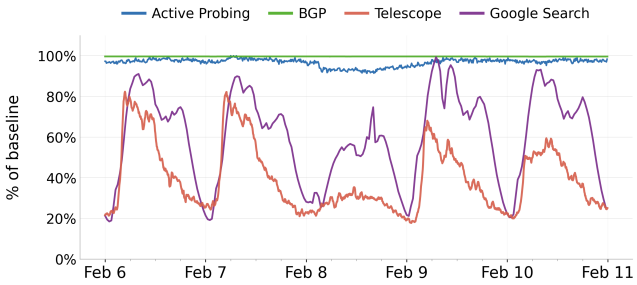

Figure 6: IODA signals for Pakistan, February 6-10, 2024

(February 8th). Visually, we can observe the discrepancy as a reduced peak in daily Telescope signal. Algorithmically, these situations require more nuance. Guillot et al. [9] propose Chocolatine, a refined Telescope detection method that uses seasonal data to predict Telescope signals and alert when current signals deviate from this predicted value. A similar approach could enhance Google Search's ability to complement IODA's current alerting methodology. More generally, accounting for daily and weekly oscillations in Telescope and Google Search signals would likely enhance IODA's overall observability.

Additional considerations are required for the implementation of such enhancements. Similar to [3], we confirmed two trends that persist through 2024. First, approximately 50% of national shutdowns occur between 4:00-8:00am local time, when signals such as Google Search and Telescope are not at their peak. Second, approximately 40% of national shutdowns cluster at approximately 24-hour intervals. Figure 4 visualizes shutdowns that occur precisely every 24 hours for 4 days in a row. Enhancements to detection algorithms must be able to consider whether signals from a previous time period (such as 24 hours ago) were part of an outage or not. Otherwise, a recurring outage may accidentally be interpreted as normal traffic patterns despite each occurrence being part of one continuous outage event.

5 Conclusion

This paper characterizes reported national shutdowns that were undocumented by the IODA team. We observe that IODA Telescope signals have alerted with lesser frequency since 2022, and that the number of countries with KIO-reported full-network shutdowns matched by IODA per year declined from 18 to 7 between 2021 and 2024. In our investigation we found that undocumented events are typically associated with armed conflict, shutdowns targeting specific ASes, and large-scale application layer blocking.

In future research into shutdown observability, we plan to examine in greater detail the technical attributes of shutdowns that coincide with armed conflict. In our investigation, we found that they make up a significant portion of unmatched shutdowns and exhibit traits that IODA's current automated alerts miss. In addition, other undocumented shutdowns resulting from application layer blocking and AS-specific shutdowns present opportunities to improve detection methods by incorporating alerts based on Google Search and Cloudflare Radar data.

References

[1] Access Now. 2026. #KeepItOn: Fighting Internet Shutdowns Around the World. https://www.accessnow.org/keepiton/ Accessed: April 2026.

[2] Access Now. 2026. #KeepItOn Shutdown Tracker Optimization Project (STOP) Dataset. https://docs.google.com/spreadsheets/d/1DvPAuHNLp5BXGb0nnZDGNoiIwEeu2ogdXEIDvT4Hyfk/edit?gid=1986365878#gid=1986365878 Accessed: April 2026.

[3] Zachary S. Bischof, Kennedy Pitcher, Esteban Carisimo, Amanda Meng, Rafael Bezerra Nunes, Ramakrishna Padmanabhan, Margaret E. Roberts, Alex C. Snoeren, and Alberto Dainotti. 2023. Destination Unreachable: Characterizing Internet Outages and Shutdowns. In *Proceedings of the ACM SIGCOMM 2023 Conference (ACM SIGCOMM '23)*. ACM, New York, NY, USA, 608–621. https://doi.org/10.1145/3603269.3604883

[4] Censored Planet. 2026. Censored Planet. https://censoredplanet.org/#/

[5] Center for Applied Internet Data Analysis (CAIDA). 2026. UCSD Network Telescope. https://www.caida.org/projects/network_telescope/

[6] Simon Cheek, Zachary Bischof, Amanda Meng, and Alberto Dainotti. 2026. Gaps in the Record – Notebooks and Analysis Dataset. https://doi.org/10.5281/zenodo.20965948

[7] Inc. Cloudflare. 2026. Cloudflare Radar. https://radar.cloudflare.com Cloudflare Radar.

[8] Alberto Dainotti, Claudio Squarcella, Emile Aben, Kimberly C. Claffy, Marco Chiesa, Michele Russo, and Antonio Pescapé. 2011. Analysis of country-wide internet outages caused by censorship. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* (Berlin, Germany) *(IMC '11)*. Association for Computing Machinery, New York, NY, USA, 1–18. https://doi.org/10.1145/2068816.2068818

[9] Andreas Guillot, Romain Fontugne, Philipp Winter, Pascal Mérindol, Alistair King, Alberto Dainotti, and Cristel Pelsser. 2019. Chocolatine: Outage Detection for Internet Background Radiation. In *Proceedings of the Network Traffic Measurement and Analysis Conference (TMA)*. https://arxiv.org/abs/1906.04426

[10] Internet Intelligence Lab, Georgia Tech. 2026. Investigated IODA Outages. Accessed: April 2026.

[11] Internet Intelligence Lab, Georgia Tech. 2026. IODA Dashboard for Monitoring Internet Outages. https://ioda.inetintel.cc.gatech.edu/dashboard Accessed: April 2026.

[12] Internet Intelligence Lab, Georgia Tech. 2026. IODA: Internet Outage Detection and Analysis. https://ioda.inetintel.cc.gatech.edu/project Accessed: April 2026.

[13] Merit. 2026. National Distributed Network Telescope. https://www.merit.edu/research/national-distributed-network-telescope/

[14] Ram Sundara Raman, Prerana Shenoy, Katharina Kohls, and Roya Ensafi. 2020. Censored Planet: An Internet-wide, Longitudinal Censorship Observatory. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (Virtual Event, USA) *(CCS '20)*. Association for Computing Machinery, New York, NY, USA, 49–66. https://doi.org/10.1145/3372297.3417883

Publicly Available Code and Dataset

The dataset and analysis notebooks supporting this paper are publicly available on Zenodo [6]. The repository includes the 73-event dataset of KIO events undocumented by IODA, as well as the code used in our analysis.