A multi-perspective view of Internet censorship in Myanmar

Ramakrishna Padmanabhan
CAIDA, UC San Diego
ramapad@caida.org

Arturo Filastò
OONI
arturo@openobservatory.org

Maria Xynou
OONI
maria@openobservatory.org

Ram Sundara Raman
University of Michigan
ramaks@umich.edu

Kennedy Middleton
UC San Diego
kmiddlet@ucsd.edu

Mingwei Zhang
CAIDA, UC San Diego
mingwei@caida.org

Doug Madory
Kentik
dmadory@kentik.com

Molly Roberts
UC San Diego
meroberts@ucsd.edu

Alberto Dainotti
CAIDA, UC San Diego
alberto@caida.org

ABSTRACT

In the wake of a military coup in February 2021, Myanmar experienced unprecedented levels of Internet censorship. Beginning with haphazard blocking of social media and intermittent Internet connectivity outages, controls proceeded to stricter blocking of websites, the shutdown of cellular data in several networks, and nearly complete disconnection from the Internet every night. In this study, we use diverse datasets and measurement methods to offer a holistic view into the censorship events in Myanmar that occurred since the coup and show how Internet censorship *evolved* during this time.

CCS CONCEPTS

• **Networks** → Network measurement;

KEYWORDS

Internet censorship, Internet outages, Availability

ACM Reference Format:
Ramakrishna Padmanabhan, Arturo Filastò, Maria Xynou, Ram Sundara Raman, Kennedy Middleton, Mingwei Zhang, Doug Madory, Molly Roberts, and Alberto Dainotti. 2021. A multi-perspective view of Internet censorship in Myanmar. In *ACM SIGCOMM 2021 Workshop on Free and Open Communications on the Internet (FOCI'21), August 27, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3473604.3474562

1 INTRODUCTION

Since the first nationwide government-mandated Internet connectivity shutdown in 2005 in Nepal [77] the frequency of such events has been increasing worldwide [1, 2, 14, 61, 73, 79]. Today, Internet censorship takes several forms: from complete disconnection [16, 62], to blocking of specific websites [3, 4, 20]. Few censoring entities, however, have sought to exert control over the Internet in the manner employed by the Myanmar military in the wake of the recent coup.

FOCI'21, August 27, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8640-1/21/08.
https://doi.org/10.1145/3473604.3474562

On February 1, 2021, the Myanmar military seized power [50, 54, 55]. The same day—before "Internet curfews" became the norm in the country [84]—Internet connectivity was severely disrupted for several hours. Following the coup, the military also ordered the blocking of Facebook, Twitter, and Instagram [12, 22, 30]. The Internet censorship events that occurred in the aftermath of this coup are among the most disruptive, long-lasting, and widespread events in recent times.

While early studies of Internet censorship events had to be performed by analyzing news reports [34], or by using ad hoc datasets [16, 35–37], there exist several tools and datasets today whose purpose is to shed light on these types of events [7, 8, 10, 52, 56, 73]. As Internet censorship has evolved, so have the tools to observe them, enabling fine-grained analysis leading to valuable insights and lessons.

In this paper, we use publicly available datasets from IODA [10] and OONI [21, 61], and a proprietary dataset from a large network observability company—Kentik [40]—to dissect and analyze technical data about Internet censorship events in Myanmar following the coup. We use these complementary datasets to offer a holistic view (Figure 1). We present empirical data on large-scale Internet connectivity shutdowns including nightly Internet curfews and cellular outages, rampant censoring of websites, and even a route hijacking incident. We also extract political insights from this technical data. Specifically, we report upon:

- **Massive-scale censorship**: Nightly *country-wide* Internet connectivity shutdowns occurred continuously for more than two months, normalizing Internet curfews. Further, we show that access to cellular data has been restricted since March 15, 2021. We also reveal extensive blocking of social media and circumvention tool websites.
- **Evolution and consolidation of power**: The censorship events in Myanmar show signs of evolution over time. From the somewhat haphazard early Internet connectivity outages to the well-coordinated nightly outages, there has been increasing sophistication. The uncoordinated nature of the early outages are consistent with the potential limited authority and lack of access to the appropriate communication channels that the military may have had in the immediate aftermath of a coup. The subsequent evolution is consistent with the new regime's consolidation of power. Going forward, in countries with multiple Internet Service

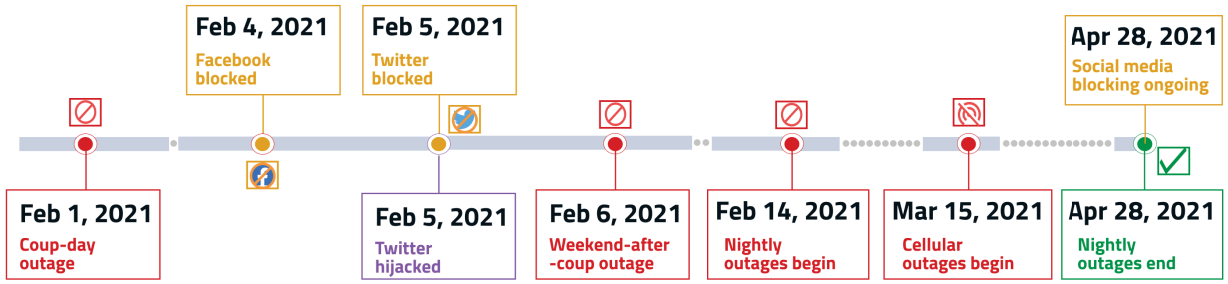

Figure 1: Timeline of censorship events in Myanmar.

Providers (ISPs), like Myanmar, the extent of government-control over the Internet could serve as one indicator of political control, which is difficult to observe in non-democracies [24].

- **Collateral damage:** Internet censorship in Myanmar showed signs of collateral damage not restricted solely to the country; a notable hijack of Twitter's address space led to users in other countries being unable to access Twitter as well. We also observe signs of IP address blocking, which has been known to be an aggressive blocking method that could possibly lead to collateral damage, since many domains may be hosted on the same IP address [11, 69, 85]. Indeed, we observe two cases of popular CDN IP addresses blocked that render several sites inaccessible.

2 BACKGROUND AND DATASETS

2.1 Political context and prior censorship

Myanmar was ruled by an autocratic military government for nearly 40 years, from 1962 to 2011. In 2007, it became the second country after Nepal to experience government-mandated country-wide Internet connectivity shutdowns [77]. At that time, only two ISPs offered Internet services in Myanmar, both state-controlled [77], facilitating the ability of the government to exert sweeping control.

Myanmar saw the end of formal military rule in March 2011, which coincided with decreased Internet censorship [67]. A report published by OONI in 2017 analyzed all OONI measurements collected from Myanmar between Oct. 2016 to Feb. 2017 and did not confirm any cases of Internet censorship, while confirming the accessibility of major social media platforms [81]. Democratic Myanmar experienced a marked increase in the number of ISPs, including international players, such as Telenor and Ooredoo [48].

In June 2019, censorship began to rise again. Internet connectivity was severed in several townships in the Rakhine and Chin states [29, 33, 74] for several months, although such measures have received push-back from service providers [29]. In 2020, an OONI report showed that the scale of Internet censorship had increased, as OONI data confirmed the DNS based blocking of 174 domains on Telenor Myanmar (AS133385). While most of these blocked domains contain adult content, several are ethnic media websites [45].

In Nov. 2020, Myanmar held general elections in which the incumbent National League for Democracy party won in a landslide [51]. On Feb. 1, 2021, a military junta led by Min Aung Hlaing seized control of the government, arresting members of Parliament, the President Win Myint, and State Counsellor Aung San Suu Kyi. The coup has been followed by widespread protests as well as violent repression. One might expect the diversity of ISPs in Myanmar today to thwart attempts at nation-wide censorship, but our results show that the military has been able to censor its users surprisingly effectively. Since the coup, there has been an acute increase in Internet censorship in Myanmar, along multiple dimensions. In this study, we examine these censorship events using diverse datasets and show, where possible, their evolution over time.

2.2 Datasets

Internet censorship can take many forms—from blanket disruption of users' Internet connections to targeted blocking of specific domains and keywords. Obtaining a comprehensive view of censorship requires the use of complementary methods that have been designed to detect specific forms of censorship. In this study, we use the following datasets:

- **IODA** The IODA (Internet Outage Detection and Analysis) system monitors the Internet continuously to identify macroscopic Internet outages affecting the edge of the network, i.e., significantly impacting a network operator (AS) or a large fraction of a country. It uses three orthogonal data sources (Active Probing, BGP, and Internet pollution traffic reaching a darknet) to detect outages and enables visualizing Internet connectivity in near-realtime on a public site since 2016 [10]. Appendix A.1 provides additional details about these data sources.
- **OONI** The Open Observatory of Network Interference (OONI) [61] project develops free and open source software (called OONI Probe [57]) designed to *ethically* measure the blocking of websites, instant messaging apps, and circumvention tools. OONI Probe is run by volunteers that have provided informed consent in around 200 countries and territories every month, contributing millions of network measurements from local vantage points. All OONI Probe measurements are automatically submitted to OONI servers, processed, and openly published in near real-time. Since 2012, OONI has openly published more than 420 million measurements from 22 thousand unique AS networks in 239 countries and territories [56].
- **Traffic** We used a proprietary dataset consisting of aggregated traffic statistics based on *NetFlow* [41] logs from a large network observability company (Kentik) to analyze user traffic in

Myanmar. The company has over 300 customers—large telecoms, CDNs and other Internet-focused enterprises—using its solutions for NetFlow analysis and half agree for their data to be used in aggregate analysis. NetFlow is a protocol used to record metadata about IP traffic flows—including per-flow source and destination IP addresses, packet count, bytes transferred etc.—traversing a NetFlow-enabled network device (such as a router, switch, or host). Since Kentik's customers include major tier-1 ISPs and global content providers, Kentik's (sampled) NetFlow dataset includes samples collected *from Internet routers*, enabling the analysis of censorship events (among other uses). This data represents a large cross-section of traffic flowing through the Internet and is useful for large-scale understanding of Internet behavior. To protect users in Myanmar, Kentik aggregated NetFlow traffic statistics by source and destination ASes (for ASes in Myanmar) and extracted the overall traffic observed at the AS-level. We analyzed this aggregated data (collected between Jan. 30 to May 05 2021) and present normalized results.

- **Internet global routing data** We analyze BGP data collected by the RouteViews [72] and RIPE RIS[70] projects to understand the impact of an accidental announcement of Twitter address space by a Myanmar ISP on the global Internet routing system.

3 ANALYSIS

In this section, we present our analyses. Section 3.1 offers a timeline of the events that we detected. In Section 3.2, we use data from IODA and Kentik to investigate Internet connectivity shutdowns and in Section 3.3, we use data from OONI to analyze website and social-media blocks. Section 3.4 investigates a BGP hijack event targeting Twitter's address space and the collateral damage to users outside Myanmar. We published an initial (non-peer-reviewed) report about these events in Mar. 2021 soon after they had begun [84]; this paper considerably extends our analysis.

3.1 Overview: a timeline of events

The first week after the coup saw several major censorship events. The first was an Internet connectivity outage on the day of the coup itself, on Feb. 1 2021, heralding the tightening of information controls that would follow. On Feb. 4, Facebook was blocked, and a day later, so was Twitter. On the same day that Twitter was blocked, Campana Mythic (AS136168) hijacked address space belonging to Twitter—likely accidentally—leading to collateral damage for Twitter users beyond Myanmar's borders. A massive Internet outage that lasted longer than 24 hours occurred on the first weekend after the coup, as protests against the coup intensified.

Internet controls tightened in the time since, and have only recently (as of mid-May 2021) begun to show signs of relaxing. Beginning on Feb. 14, country-wide Internet outages affected Myanmar *every night* for 72 nights straight, until Apr. 28. Cellular data has been severely restricted from Mar. 15th [31] and restrictions remain, as of mid-May 2021. Similarly, social media and website blocks also continue to remain in place.

3.2 Internet connectivity outages

We analyzed measurements collected by the IODA system and traffic data from Kentik to investigate episodes where users in Myanmar were completely disconnected from the Internet. The complementary perspectives offered by IODA and Kentik allow us to detect a wider range of events. User-driven traffic originating in Myanmar has diurnal patterns, making it more challenging to observe outages in the night using Kentik's traffic. Conversely, IODA has limited visibility into the connectivity of cellular networks (e.g., because they often use Carrier Grade NAT) whereas Kentik's traffic datasets present visibility into cellular network connectivity as well.

For easy visual comparison of time series values from the four data sources (3 from IODA and 1 from Kentik), we present *normalized* values that fall between 0 and 1.

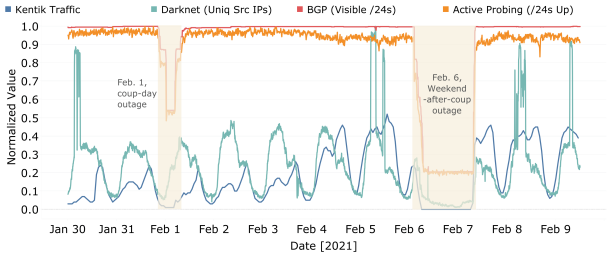

Figure 2: IODA and Kentik data show Internet connectivity outages on Feb. 1 and Feb. 6., in the first week after the coup.

Coup-day outage. We observed a significant Internet outage affecting Myanmar from 21:00 UTC (03:30 AM on Feb. 1 in local time) on Jan. 31st—the day the coup began (Figure 2). While the outage is visible in the BGP and Active Probing data sources—with the number of /24 address blocks in Myanmar reachable on BGP dropping from 695 to 376, a decrease of 46%—it is less evident in the Darknet and Kentik Traffic data sources. However, examining the Traffic data sources at the AS level shows drops in traffic for several prominent ASes at the same time as drops in IODA data sources. Further, media reports indicate that an Internet outage did indeed occur on this day [19, 38, 53, 78].

Notably, there were several differences in the extent to which ISPs were affected by this outage and in timing patterns (see Figure 6 in Appendix A.2). Some providers (Ooredoo (AS132167) and Telenor (AS133385)) experienced outages that began at 21:00 UTC whereas others (MPT (AS9988) and Mytel (AS136255)) underwent outages just after midnight UTC. Some ISPs (Frontiir (AS58952) and YTP (AS18399)) did not face a significant outage whereas others (MPT (AS9988) and Mytel (AS136255)) experienced near-complete loss of Internet connectivity.

These differences in timing patterns and extent of the outages are consistent with weak coordination from the government and/or ISPs. They also suggest the lack of *an Internet kill switch* that could cut connectivity for the entire country with one fell swoop; instead, each provider appears to have received (or at least acted) upon orders at different times and with different levels of execution.

Weekend-after-coup outage. On Saturday, Feb. 6, a 28-hour long Internet outage affected most ISPs in Myanmar (Figure 2). This outage is visible clearly in IODA's data sources, although the BGP and active probing data sources appear to suggest that some networks remain connected. The outage is also visible in traffic data

from Kentik; this data source shows that negligible traffic was sent during this time. Since IODA's data indicating (some) connectivity may be due to responses to active probes from infrastructure (like routers), the traffic dataset provides us with the additional detail that most end-users in Myanmar likely had no Internet connectivity during this outage.

IODA's measurements show that the start time of these outages had some differences across ISPs, but the outages' end-times were similar across most ISPs. This synchronization is suggestive of improved planning, coordination, and execution of this shutdown.

Nightly curfews. From the night of Feb. 14, nightly outages affected most ISPs for *72 nights*, until Apr. 28th. These outages began at the same time (18:30 UTC/01:00 local) and lasted 8 hours on most nights (Figure 7, Appendix A.2). The outages are visible in all data sources, although the traffic data source again reveals that whatever connectivity IODA reports during these times is unlikely to be from end-users, since there is negligible end-user traffic.

In contrast to the coup-day outage, the nightly outages occurred in a highly synchronized manner, with outages beginning and ending at identical times for most ISPs. This synchronization is consistent with enhanced censorship mechanisms and tools that diverse ISPs likely now possess and also with increased control over these ISPs by the government.

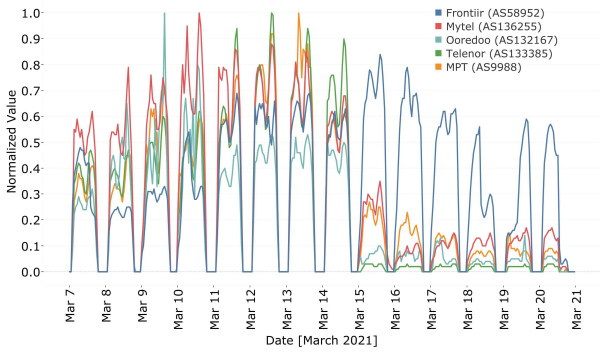

Figure 3: Traffic data from Kentik show that cellular traffic has reduced considerably from Mar. 15th.

Cellular outages. From Mar. 15th, cellular connectivity has been heavily restricted [31]. Although these outages are not visible in IODA's datasets, the drop in Kentik traffic is clearly visible in Figure 7 (Appendix A.2). In Figure 3, we break down the traffic dataset from Kentik by four large cellular providers (MPT (AS9988), Mytel (AS136255), Telenor (AS133385), and Ooredoo (AS132167)), and also include a major non-cellular provider for contrast. We see a substantial reduction in traffic from the cellular providers even during the day, whereas the non-cellular provider only observes drops in traffic during the nightly curfews. The cellular restrictions are ongoing, as of mid-May 2021.

Observing these cellular outages was only possible due to the added perspective of the traffic dataset from Kentik, and demonstrates the value of using multiple measurement techniques. Since cellular networks have some idiosyncratic differences compared to fixed-line networks, these outages are often not visible even in state-of-the-art monitoring systems such as IODA. However, by examining aggregated traffic statistics from a major company, we were able to shed light and increase awareness upon these outages as well.

3.3 Website and social media blocking

We analyzed OONI measurements collected from Myanmar from Feb. 1, 2021 to Apr. 30, 2021 [58]. Specifically, we analyzed OONI Web Connectivity [59, 60] measurements, which are designed to measure the DNS, TCP/IP, and HTTP blocking of websites.

Figure 4 shows results for some of the websites found highly blocked based on our analysis, aggregating the measurement values per day across tested ASes in Myanmar. In the 'TCP/IP', 'DNS' and 'HTTP' blocking cases, the local OONI Probe user observed a different response compared to the response from OONI's control vantage point (Section A.3 in the Appendix contains additional methodology details). We limited the findings in Figure 4 to include popular social media sites, circumvention tool sites, as well as wikipedia.org, coronavirus.app, and several websites that presented anomalies (possibly) due to collateral damage. As shown by the size of the bubbles in Figure 4, more OONI Probe users ran measurements in Feb. immediately following the coup compared to later months; the surge in Feb. was partially driven by the "Anonymous" group encouraging Myanmar users to run OONI Probe tests [26].

DNS blocking. In Figure 4, we have annotated measurements as 'Confirmed DNS blocked' when we observed DNS-based interference returning IP addresses that (previously) hosted block pages (`59.153.90.11`, `167.172.4.60`) or an address in private IP space (such as `127.0.0.1` or `172.29.8.1`). Many ISPs in Myanmar showed evidence of confirmed DNS blocking, usually resolving to an IP address that hosted a blockpage. Some ISPs responded with NXDOMAIN responses for domains like `www.facebook.com`. DNS interference was not consistent inside an ISP; some DNS resolvers implemented DNS blocking while others in the same ISP did not.

IP address blocking. We primarily observe IP-based blocking of websites, as most measurements (across ASes) show that TCP connections to the resolved IP addresses failed (when resolution succeeded in providing the right IP address for the website). Our empirical observation of IP-based blocking partially corroborates anecdotal evidence of purportedly blocked IP addresses that circulated on social media (a VPN block list circulated on Facebook, listing specific VPN IP addresses that ISPs in Myanmar may have been required to block access to [27]). This censorship technique is primarily seen in OONI data after the coup, as OONI's analysis in Myanmar in 2020 showed that DNS based interference was previously more prevalent [45].

Collateral damage. IP based blocking can potentially lead to collateral damage, affecting the accessibility of other domains hosted on a blocked IP address. We found 2 such cases:

(i) Domains hosted on the IP 172.217.194.121. This IP address belongs to the Google hosting network and includes domains such as www.snapchat.com, www.getoutline.org, www.paganpride.org, and www.privaterra.org, all of which presented TCP/IP anomalies between Feb. 24 - 27, 2021 (as illustrated in Figure 4). The fact that

Figure 4: Blocking of websites in Myanmar from Feb. to Apr. 2021 based on OONI measurements. The bars (left Y-axis) show the percentage of measurements with specific results on a particular day; the circles show the total measurements on that day (Log scale, right Y-axis). The size of the circles shows the number of distinct ASes that produced measurements on that day. Measurements to social media websites and circumvention tool websites faced high rates of TCP/IP and DNS blocking.

these domains are hosted on the same IP address, and presented the same TCP/IP anomalies during the same time period, suggests that some of them may have temporarily been blocked unintentionally as a result of collateral damage. We observed 4 ASes that blocked this IP address during the same time period, suggesting that there was some coordination in blocking among ASes. However, other ASes did not show this blocking.

(ii) Domains hosted on the IP 151.101.1.195. This address belongs to the Fastly network and includes the domains coronavirus.app and getintra.org, both of which started to present TCP/IP anomalies on Mar. 2, 2021. Reverse IP lookups indicate that the blocking of this IP may lead to the blocking of more than 10,000 websites, showing the severity of collateral damage due to IP blocking [75].

Censorship variance across networks. Our findings show that different websites are blocked on different networks. Some of the blocked websites listed in Figure 4 are accessible on certain networks in Myanmar. This suggests that Internet censorship in Myanmar is *not* centralized and that local ISPs may implement blocking at their own discretion.

We also observe variance in censorship methods across networks and over time. After the coup on Feb. 1, we primarily observe IP based blocking of websites across ASes. However, we also continue to observe DNS based interference, returning IP addresses that (previously) hosted block pages or an address in private IP space. In some cases, we observe both censorship techniques being used on the same ASes.

Non-deterministic censorship. OONI measurements show that IP blocks are *not* implemented consistently, offering additional signs that ISPs operated independently and (sometimes) arbitrarily. Within the same AS, we do not observe IP blocking for *all* the addresses associated with a domain. One cause of this inconsistency could potentially be the result of ISPs using incomplete address-lists for blocking. E.g.: OONI measurements collected from the testing of facebook.com on Frontiir (AS58952) show the blocking of Facebook's IP 157.240.15.36, but not of Facebook's IP 31.13.82.36.

3.4 Twitter hijack and collateral damage

On Feb. 5th—the same day that Twitter was blocked in Myanmar—Campana Mythic (AS136168) announced the 104.244.42.0/24 prefix, belonging to Twitter. The proximity of this hijacking event in time to the blocking of Twitter in other Myanmar ISPs suggests that the original intent was to *blackhole* traffic to Twitter for users of this Myanmar ISP[1]. However this route accidentally leaked to the global Internet, appearing as if AS136168 owned/hosted Twitter's address space. This accidental event offers additional evidence that providers used various ways to perform IP-level blocking to censor domains (Section 3.3).

[1]Private communication corroborated that the hijack was accidental.

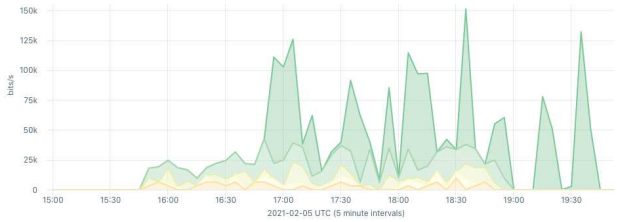

Figure 5: Collateral damage to Twitter users outside Myanmar as a result of the BGP hijack event affecting Twitter's address space. The figure shows Twitter traffic observed by Kentik from different source ASes (indicated by different colors) that was being routed towards Campana Mythic (AS136168).

Our analysis of BGP data collected by the Routeviews and RIPE RIS projects shows the illegitimate route propagated (at least) to operators in Singapore (AS4844, AS56300, AS24482, AS132132) and Vietnam (AS45903) who received, accepted, and further propagated it. This resulted in collateral damage for Twitter users outside Myanmar. We quantify the extent of this collateral damage in Figure 5, which shows that a small volume of traffic from Kentik's customers *outside Myanmar* was directed towards the hijacker AS136168 instead of AS13414 (Twitter).

4 DISCUSSION

The censorship events in Myanmar reflect emerging patterns of politically inspired censorship and offer insight into the ways in which authoritarian regimes combine censorship approaches strategically to achieve their immediate goals. First, the timing of censorship during a coup is consistent with many studies that have shown that Internet censorship is targeted during sensitive political time periods and periods of potential power transitions, such as elections and large-scale protests [23, 25, 44, 47, 73]. Among many, recent examples of outages during political transitions have occurred in January 2021 in Uganda [82] and in the summer of 2020 during large-scale protests in Belarus [83].

The fact that the initial outages were implemented by the challenger rather than the incumbent government lends support to recent theoretical and empirical work that suggests that Internet censorship during a coup attempt can increase the probability of a successful coup [9]. Conspirators in a coup may benefit from shutting communications quickly, to prevent public or government coordination against their coup attempt [39]. Yet, as we mentioned before, the haphazard nature of the outages during the initial coup in Myanmar may reflect the difficulty of the challenger in implementing this censorship, and could be a reflection of their initial lack of political control.

After consolidating power, the new junta in Myanmar began imposing Internet curfews, shutting down the Internet during the night while keeping it on in the day. While the imposition of nightly curfews has long been a tactic by authoritarian (and some democratic) regimes to quell protests, it has recently been adopted in the virtual world in the midst of large scale unrest. Recent examples of similar Internet curfews include Libya in 2011 [17] and Gabon in 2016 [13]. Like physical curfews, regimes may implement Internet curfews to target organization of political dissent while minimizing the impact on the economy, as many sectors require Internet access during the day. Indeed, evidence suggests that the junta is aware of the economic impacts of censorship—Myanmar restored access to banking apps at the end of April coincident with the lifting of curfews, perhaps as a way to reinvigorate economic activity [76].

The evolution of censorship throughout this time period underscores the importance of being able to track multiple methods of censorship to gain a holistic understanding of the digital strategy of autocrats, something that has as of yet been difficult to do at scale [42]. While nightly outages have now ended, the social media and website blocking we described that has persisted since February 5 may indicate a move toward more selective methods of censorship [28]. This shift is consistent with a pattern in authoritarian regimes of engaging in targeted censorship to maximize political impact while minimizing its cost [5, 71]. We hope this paper can provide a template of combining Internet measurements to provide a broader understanding of digital strategy of autocrats, an effort that could be scaled and replicated cross-nationally in future work.

5 CONCLUSION

In this study, we used multiple complementary datasets to investigate the censorship events that occurred in Myanmar following the military coup on February 1 2021. These datasets revealed different facets of censorship: IODA data showed episodes of complete disconnection from the Internet with accurate timing, data from Kentik presented insights into cellular traffic restrictions, and OONI data demonstrated the blocking of social media and various websites.

These datasets are complementary at various levels. One key difference is in their goals and design. OONI seeks to measure website/social media blocking, whereas IODA and the use of Kentik's data target full connectivity disruption of Internet users. As such, they operate at different layers of the network stack and with different granularity. Though data from both IODA and Kentik can be used to measure full connectivity shutdowns, their measurements are distinct in nature and thus can each reveal unique insight on how disconnections affect different networks (*e.g.,* IODA's data can reveal outage timing patterns with more accuracy than Kentik's, but IODA's data sometimes lacks visibility into disconnections of cellular operators, whereas in this paper we show that Kentik's data can be used to study such events).

We believe that the lenses offered by these diverse datasets will be highly beneficial to analyses of future censorship events. Similar to Myanmar, recent Internet censorship efforts in other countries have also used a variety of censorship methods [62, 82, 83]. As censors evolve in their use of information controls, our ability to understand them will also need to develop. Thankfully, an increasing variety of open tools and datasets are being actively developed and deployed, enabling deeper and more timely visibility into network interference phenomena.

Ethical considerations. We recognize that some of our results could be used by censors to implement more rigorous measures. However, since the majority of our analyses were derived from publicly available datasets, we believe that the benefits yielded by an empirical understanding of these events outweigh the risks [18, 49].

ACKNOWLEDGMENTS

We thank the anonymous reviewers and our shepherd, Masashi Crete-Nishihata, for their helpful feedback. We also would like to thank Prof. Michael L. Best for discussing with us our preliminary findings. This research was partially supported by National Science Foundation grant CNS-1705024.

REFERENCES

[1] Access Now. 2020. Access Now reports on 2019 trends in internet shutdowns, approaches to defending free expression. https://web.archive.org/web/20210611124134/https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf.

[2] Access Now. 2021. Internet shutdowns report: Shattered dreams and lost opportunities — a year in the fight to #KeepItOn. https://web.archive.org/web/20210522195750/https://www.accessnow.org/cms/assets/uploads/2021/03/KeepItOn-report-on-the-2020-data_Mar-2021_3.pdf.

[3] Anonymous, Arian Akhavan Niaki, Nguyen Phong Hoang, Phillipa Gill, and Amir Houmansadr. 2020. Triplet Censors: Demystifying Great Firewall's DNS Censorship Behavior. In *Free and Open Communications on the Internet*. USENIX.

[4] Simurgh Aryan, Homa Aryan, and J. Alex Halderman. 2013. Internet Censorship in Iran: A First Look. In *Free and Open Communications on the Internet*. USENIX.

[5] Nikkei Asis. 2021. *Myanmar junta builds 'walled garden' of internet services - Nikkei Asia.* https://web.archive.org/web/20210513221939/https://asia.nikkei.com/Spotlight/Myanmar-Coup/Myanmar-junta-builds-walled-garden-of-internet-services

[6] K. Benson, A. Dainotti, k. claffy, and E. Aben. 2013. Gaining Insight into AS-level Outages through Analysis of Internet Background Radiation. In *Traffic Monitoring and Analysis Workshop (TMA)*.

[7] Kevin Bock, George Hughey, Louis-Henri Merino, Tania Arya, Daniel Liscinsky, Regina Pogosian, and Dave Levin. 2020. Come as You Are: Helping Unmodified Clients Bypass Censorship with Server-side Evasion. In *SIGCOMM*. ACM.

[8] Kevin Bock, George Hughey, Xiao Qiang, and Dave Levin. 2019. Geneva: Evolving Censorship Evasion Strategies. In *Computer and Communications Security*. ACM.

[9] Raphael Boleslavsky, Mehdi Shadmehr, and Konstantin Sonin. 2018. Media Freedom in the Shadow of a Coup. *Journal of the European Economic Association* (2018).

[10] CAIDA. [n.d.]. IODA: Internet Outage Detection and Analysis. https://ioda.caida.org/ioda/dashboard.

[11] china-cdn 2014. CDN providers blocked by China. https://web.archive.org/web/20210702012211/https://www.cdnfinder.com/cdn-providers-blocked-china.

[12] CNET. 2021. *Facebook temporarily blocked in Myanmar after military coup - CNET.* https://web.archive.org/web/20210702005018/https://www.cnet.com/news/facebook-temporarily-blocked-in-myanmar-after-military-coup/

[13] Abdi Latif Dahir. 2016. Gabon has been imposing a 12-hour-a-day internet curfew as its political crisis grows. https://web.archive.org/web/20210702012309/https://qz.com/africa/781752/gabon-has-been-imposing-a-12-hour-a-day-internet-curfew-as-its-political-crisis-grows/.

[14] Abdi Latif Dahir. 2017. Internet shutdowns are costing African governments more than we thought. https://web.archive.org/web/20210701133002/https://qz.com/africa/1089749/internet-shutdowns-are-increasingly-taking-a-toll-on-africas-economies/.

[15] A. Dainotti, C. Squarcella, E. Aben, K. Claffy, M. Chiesa, M. Russo, and A. Pescapè. 2014. Analysis of Country-wide Internet Outages Caused by Censorship. *IEEE/ACM Transactions on Networking* 22, 6 (Dec 2014), 1964–1977.

[16] 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 *ACM IMC*.

[17] 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*. 1–18.

[18] D. Dittrich and E. Kenneally. 2012. *The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research.* Technical Report. U.S. Department of Homeland Security.

[19] DW. 2021. *Myanmar coup: Aung San Suu Kyi detained as military seizes power | DW | 01.02.2021.* https://web.archive.org/web/20210702005944/https://www.dw.com/en/myanmar-coup-aung-san-suu-kyi-detained-as-military-seizes-power/a-56400678

[20] Arturo Filastò and Jacob Appelbaum. 2012. OONI: Open Observatory of Network Interference. In *Free and Open Communications on the Internet*. USENIX.

[21] Arturo Filastò and Jacob Appelbaum. 2012. OONI: Open Observatory of Network Interference. In *2nd USENIX Workshop on Free and Open Communications on the Internet (FOCI 12)*.

[22] Forbes. 2021. *Social Media Blackout: Myanmar Military Government Blocks Twitter, Instagram.* https://web.archive.org/web/20210702004902/https://www.forbes.com/sites/rachelsandler/2021/02/05/social-media-blackout-myanmar-military-government-blocks-twitter-instagram/?sh=40409fec2f05

[23] Tina Freyburg and Lisa Garbe. 2018. Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa. *International Journal of Communication* 12 (2018), 3896–3916.

[24] Jennifer Gandhi and Jane Lawrence Sumner. 2020. Measuring the consolidation of power in nondemocracies. *The Journal of Politics* 82, 4 (2020), 1545–1558.

[25] Anita R Gohdes. 2015. Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research* 52, 3 (2015), 352–367.

[26] Anonymous Group. 2021. *Tweet: Anonymous encourages the use of OONI for monitoring censorship in Myanmar.* https://web.archive.org/web/20210701134156/https://twitter.com/YourAnonCentral/status/1359777805131677699?s=20

[27] Facebook group. 2021. *Image posted on Facebook group shows IP addresses of VPN services that were ordered to be blocked.* https://web.archive.org/web/20210507134042/https://www.facebook.com/groups/yesagyogp/permalink/1119533741827118/

[28] Telenor Group. 2020. *The case for open internet in Myanmar.* https://web.archive.org/web/20210521052853/https://www.telenor.com.mm/en/article/the-case-for-open-internet-in-myanmar

[29] Telenor Group. 2020. *Internet services restricted in Myanmar townships (Updated 12 May 2020).* https://web.archive.org/web/20210510032911/https://www.telenor.com/internet-services-restricted-in-five-townships-in-myanmar-03-february-2020/

[30] Telenor Group. 2021. *Directive to block social media service - Telenor Group.* https://web.archive.org/web/20210508213547/https://www.telenor.com/directive-to-block-social-media-service/

[31] Telenor Group. 2021. *Tweet: Telenor announces that cellular restrictions have been in place since March 15.* https://web.archive.org/web/20210513080349/https://twitter.com/TelenorGroup/status/1372097178676641793

[32] Andreas Guillot, Romain Fontugne, Philipp Winter, Pascal Mérindol, Alistair King, Alberto Dainotti, and Cristel Pelsser. 2019. Chocolatine: Outage Detection for Internet Background Radiation. In *Traffic Monitoring and Analysis Conference (TMA)*.

[33] Freedom House. 2020. *Myanmar: Freedom on the Net 2020 Country Report | Freedom House.* https://freedomhouse.org/country/myanmar/freedom-net/2020

[34] Philip N Howard, Sheetal D Agarwal, and Muzammil M Hussain. 2011. When do states disconnect their digital networks? Regime responses to the political uses of social media. *The Communication Review* 14, 3 (2011), 216–232.

[35] OpenNet Initiative. 2004. *Internet Filtering in Saudi Arabia in 2004.* https://web.archive.org/web/20210702013116/https://opennet.net/studies/saudi

[36] OpenNet Initiative. 2005. *Internet Filtering in Iran in 2004-2005: A Country Study.* https://web.archive.org/web/20210702012952/https://opennet.net/studies/iran2005

[37] OpenNet Initiative. 2005. *Internet Filtering in Yemen in 2004-2005: A Country Study.* https://web.archive.org/web/20210702013032/https://opennet.net/studies/yemen

[38] Amnesty International. 2021. *Myanmar: New internet blackout "heinous and reckless".* https://web.archive.org/web/20210702012636/https://www.amnesty.org/en/latest/news/2021/02/myanmar-new-internet-blackout/

[39] Harvey G Kebschull. 1994. Operation" Just Missed": Lessons from failed coup attempts. *Armed Forces & Society* 20, 4 (1994), 565–579.

[40] Kentik. [n.d.]. *Kentik.* https://www.kentik.com/

[41] Kentik. [n.d.]. *NetFlow Guide: Types of Network Flow Analysis.* https://www.kentik.com/netflow-guide-types-of-network-flow-analysis/

[42] Eda Keremoğlu and Nils B Weidmann. 2020. How dictators control the internet: a review essay. *Comparative Political Studies* 53, 10-11 (2020), 1690–1703.

[43] A. King, A. Dainotti, B. Huffaker, and k. claffy. 2014. A Coordinated View of the Temporal Evolution of Large-scale Internet Events. *Computing* 96, 1 (Jan 2014), 53–65.

[44] Gary King, Jennifer Pan, and Margaret E Roberts. 2013. How censorship in China allows government criticism but silences collective expression. *American Political Science Review* (2013), 326–343.

[45] Phyu Phyu Kyaw, Maria Xynou, and Arturo Filastò. 2020. *Myanmar blocks "fake news" websites amid COVID-19 pandemic.* https://ooni.org/post/2020-myanmar-blocks-websites-amid-covid19/

[46] Citizen Lab. 2021. *Citizen Lab test lists repository.* https://github.com/citizenlab/test-lists

[47] Philipp M Lutscher, Nils B Weidmann, Margaret E Roberts, Mattijs Jonker, Alistair King, and Alberto Dainotti. 2020. At home and abroad: The use of denial-of-service attacks during elections in nondemocratic regimes. *Journal of Conflict Resolution* 64, 2-3 (2020), 373–401.

[48] Frontier Myanmar. 2018. *Myanmar's broadband price war | Frontier Myanmar.* https://web.archive.org/web/20210702011029/https://www.frontiermyanmar.net/en/myanmars-broadband-price-war/

[49] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. 1978. *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research.* National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research.
[50] BBC News. 2021. *Myanmar coup: Aung San Suu Kyi detained as military seizes control - BBC News.* https://web.archive.org/web/20210702004615/https://www.bbc.com/news/world-asia-55882489
[51] BBC News. 2021. *Myanmar coup: What is happening and why? - BBC News.* https://web.archive.org/web/20210513073730/https://www.bbc.com/news/world-asia-55902070
[52] Arian Akhavan Niaki, Shinyoung Cho, Zachary Weinberg, Nguyen Phong Hoang, Abbas Razaghpanah, Nicolas Christin, and Phillipa Gill. 2020. ICLab: A Global, Longitudinal Internet Censorship Measurement Platform. In *Symposium on Security & Privacy*. IEEE.
[53] Access Now. 2021. *Update: internet access, censorship, and the Myanmar coup - Access Now.* https://web.archive.org/web/20210702010941/https://www.accessnow.org/update-internet-access-censorship-myanmar/
[54] Voice of America. 2021. *Myanmar Leader Aung San Suu Kyi, Others Detained by Military | Voice of America - English.* https://web.archive.org/web/20210203131316/https://www.voanews.com/east-asia-pacific/myanmar-leader-aung-san-suu-kyi-others-detained-military
[55] Voice of America. 2021. *Myanmar military seizes power, detains elected leader Aung San Suu Kyi.* https://web.archive.org/web/20210201053645/https://news.trust.org/item/20210201014444-5u7cm
[56] Open Observatory of Network Interference (OONI). 2021. *OONI Explorer.* https://explorer.ooni.org/
[57] Open Observatory of Network Interference (OONI). 2021. *OONI Probe.* https://ooni.org/install/
[58] Open Observatory of Network Interference (OONI). 2021. *OONI web connectivity measurements for Myanmar from February 1st to April 30th 2021.* https://explorer.ooni.org/search?until=2021-05-01&since=2021-02-01&probe_cc=MM&test_name=web_connectivity/
[59] Open Observatory of Network Interference (OONI). 2021. *OONI Web Connectivity test.* https://web.archive.org/web/20210710223322/https://ooni.org/nettest/web-connectivity/
[60] Open Observatory of Network Interference (OONI). 2021. *OONI Web Connectivity test specification.* https://github.com/ooni/spec/blob/master/nettests/ts-017-web-connectivity.md
[61] Open Observatory of Network Interference (OONI). 2021. *OONI Website.* https://ooni.org/
[62] Ramakrishna Padmanabhan, Alberto Dainotti, Nima Fatemi, Arturo Filastò, Maria Xynou, and Simone Basso. 2019. *Iran's nation-wide Internet blackout: Measurement data and technical observations.* https://ooni.org/post/2019-iran-internet-blackout/
[63] Ramakrishna Padmanabhan, Amogh Dhamdhere, Emile Aben, kc claffy, and Neil Spring. 2016. Reasons Dynamic Addresses Change. In *Internet Measurement Conference (IMC)*.
[64] Ramakrishna Padmanabhan, Patrick Owen, Aaron Schulman, and Neil Spring. 2015. Timeouts: Beware Surprisingly High Delay. In *Internet Measurement Conference (IMC)*.
[65] Ramakrishna Padmanabhan, Aaron Schulman, Alberto Dainotti, Dave Levin, and Neil Spring. 2019. How to find correlated Internet failures. In *Passive and Active Measurement Conference (PAM)*.
[66] Ramakrishna Padmanabhan, Aaron Schulman, Dave Levin, and Neil Spring. 2019. Residential links under the weather. In *ACM SIGCOMM*.
[67] Irene Poetranto. 2012. *Update on information controls in Burma.* https://web.archive.org/web/20210702012858/https://opennet.net/blog/2012/10/update-information-controls-burma
[68] Lin Quan, John Heidemann, and Yuri Pradkin. 2013. Trinocular: Understanding Internet Reliability Through Adaptive Probing. In *ACM SIGCOMM*.
[69] Reethika Ramesh, Ram Sundara Raman, Matthew Bernhard, Victor Ongkowijaya, Lenoid Evdokimov, Anne Edmundson, Steven Sprecher, Muhammad Ikram, and Roya Ensafi. 2020. Decentralized Control: A Case Study of Russia. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA*.
[70] RIPE NCC. [n.d.]. *Routing Information Service (RIS).* https://web.archive.org/web/20210702012121/https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/routing-information-service-ris
[71] Margaret E Roberts. 2020. *Censored: Distraction and Diversion Inside China's Great Firewall.* Princeton University Press.
[72] RouteViews. 2020. *RouteViews Routing Table Archive.* Retrieved 2020-06-29 from http://www.routeviews.org
[73] Ram Sundara Raman, Prerana Shenoy, Katharina Kohls, and Roya Ensafi. 2020. Censored Planet: An Internet-wide, Longitudinal Censorship Observatory. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*.
[74] Myanmar Times. 2019. *Internet shut down in nine townships in Rakhine, Chin.* https://web.archive.org/web/20210702012732/https://www.mmtimes.com/news/internet-shut-down-nine-townships-rakhine-chin.html
[75] Security Trails. 2021. 151.101.1.195 reverse IP lookup. https://web.archive.org/web/20210702012440/https://securitytrails.com/list/ip/151.101.1.195.
[76] Rory Wallace. 2021. Myanmar junta builds 'walled garden' of internet services. *Nikkei Asia* (2021). https://asia.nikkei.com/Spotlight/Myanmar-Coup/Myanmar-junta-builds-walled-garden-of-internet-services
[77] Stephanie Wang and Shishir Nagaraja. 2007. *Pulling the Plug: A Technical Review of the Internet Shutdown in Burma.* https://web.archive.org/web/20210701131103/https://opennet.net/sites/opennet.net/files/ONI_Bulletin_Burma_2007.pdf
[78] Human Rights Watch. 2021. *Myanmar Military Blocks Internet During Coup | Human Rights Watch.* https://web.archive.org/web/20210702010850/https://www.hrw.org/news/2021/02/02/myanmar-military-blocks-internet-during-coup
[79] Christopher Williams. 2011. How Egypt shut down the internet. https://web.archive.org/web/20210701132830/https://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html.
[80] Philipp Winter, Ramakrishna Padmanabhan, Alistair King, and Alberto Dainotti. 2019. Geo-locating BGP prefixes. In *Traffic Monitoring and Analysis Conference (TMA)*.
[81] Kay Yen Wong, Maria Xynou, Arturo Filastò, Khairil Yusof, Tan Sze Ming, and Myanmar ICT for Development Organization (MIDO). 2017. *The State of Internet Censorship in Myanmar.* https://ooni.org/post/myanmar-report/
[82] Maria Xynou, Simone Basso, Ramakrishna Padmanabhan, Arturo Filastò, DefendDefenders, and Defenders Protection Initiative. 2020. *Uganda: Data on internet blocks and nationwide internet outage amid 2021 general election.* https://ooni.org/post/2020-belarus-internet-outages-website-censorship/
[83] Maria Xynou and Arturo Filastò. 2020. *Belarus protests: From internet outages to pervasive website censorship.* https://ooni.org/post/2020-belarus-internet-outages-website-censorship/
[84] Maria Xynou, Ramakrishna Padmanabhan, Phyu Kyaw, and Arturo Filastò. 2021. *Myanmar: Data on internet blocks and internet outages following military coup.* https://ooni.org/post/2021-myanmar-internet-blocks-and-outages/
[85] Tarun Kumar Yadav, Akshat Sinha, Devashish Gosain, Piyush Kumar Sharma, and Sambuddho Chakravarty. 2018. Where The Light Gets In: Analyzing Web Censorship Mechanisms in India. In *Internet Measurement Conference (IMC)*. ACM.

A APPENDIX

Appendices are supporting material that has not been peer-reviewed.

A.1 IODA data sources

IODA uses three distinct and complementary sources of Internet measurement data:

- **Darknet/Internet Background Radiation (IBR)**: Internet Background Radiation (IBR) is one-way unsolicited traffic generated by millions of Internet hosts worldwide, due to misconfiguration, malware propagation, scanning, etc. From IBR, the system filters out spoofed traffic and bursty traffic components (e.g., due to scanning from large botnets) and extracts a "liveness signal" based on the number of distinct source IP addresses observed from a given geographic region or AS. The IBR traffic is collected through the UCSD Network Telescope, an almost entirely unutilized /8 IPv4 address block, estimated to observe 1/256th of all the IBR generated in the Internet.
- **BGP**: IODA uses the collection infrastructure operated by the RouteViews and RIPE RIS projects and infers the state of the routing tables exported by hundreds of operational routers by processing BGP updates and RIB dumps. It extracts information about which network blocks (BGP prefixes) appear reachable on the Internet control plane from most of these vantage points. IODA's approach counts visible */24 blocks* instead of prefixes, quantifying which fraction of the address space normally announced by an AS or from a region is reachable at a certain point in time.

- **Active Probing**: The IODA system periodically probes approximately 3.5 M /24 network blocks worldwide and adaptively send more probes upon lack of response using the Trinocular methodology developed by ISI/USC [68]. It uses responses to determine when /24 blocks get disconnected from the Internet.

IODA's methodology and data sources are under active development, drawing upon lessons from a wide body of recent research [6, 15, 16, 32, 43, 63–66, 68, 80].

A.2 Additional analyses of Internet connectivity outages

Here, we present additional analyses and details about the Internet connectivity shutdowns that occurred in Myanmar following the military coup. Figure 6 shows how the Internet outage that occurred on the day of the coup (Feb 1) affected various networks and highlights differences in the timing and extent of the outage. We then proceed to show in Figure 7 a time period that includes the start of cellular restrictions (March 15th) and a sample of the nightly Internet connectivity shutdowns that affected almost all Myanmar Internet users between Feb. 14 to Apr. 28th.

A.3 Detailed methodology for observing censorship using OONI datasets

To investigate the blocking of websites and social media, we analyzed OONI measurements collected from Myanmar (similarly to our previous studies in 2020 [45] and 2017 [81]). OONI measurements are regularly collected and contributed by users of the OONI Probe app [57], which is free and open source, designed to measure various forms of internet censorship and network interference. Here, we present additional details about how we used measurements collected by OONI probe to identify potential censorship.

OONI Probe's web connectivity test [59, 60] examines whether websites (included in the Citizen Lab test lists [46]) are reachable, and if they are not, the test attempts to determine whether access to them is blocked by means of DNS tampering, TCP/IP blocking or by a transparent HTTP proxy. The web connectivity test performs four steps: *Resolver identification, DNS lookup, TCP connect*, and *HTTP GET request*. By default, this test performs the above (excluding the first step, which is performed only over the network of the user) both over a control server and over the network of the user. If the results from both networks match, then there is no clear sign of network interference; but if the results are different, the result is flagged as "anomalous". Depending on the type of anomaly detected (DNS, TCP/IP, HTTP), we can infer the type of blocking.

A.3.1 Web connectivity test details. Below we provide information about how each step performed under the Web Connectivity test works.

(1) *Resolver identification* Internet Service Providers, amongst others, run DNS resolvers which map IP addresses to host names. In some circumstances though, ISPs map the requested host names to the wrong IP addresses, which is a form of tampering. As a first step, the web connectivity test attempts to identify which DNS resolver is being used by the user. It does so by performing a DNS query to special domains (such as whoami.akamai.com) which will disclose the IP address of the resolver.
(2) *DNS lookup* Once the web connectivity test has identified the DNS resolver of the user, it then attempts to identify which addresses are mapped to the tested host names by the resolver. It does so by performing a DNS lookup, which asks the resolver to disclose which IP addresses are mapped to the tested host names, as well as which other host names are linked to the tested host names under DNS queries.
(3) *TCP connect* The web connectivity test will then try to connect to the tested websites by attempting to establish a TCP session on port 80 (or port 443 for URLs that begin with HTTPS) for the list of IP addresses that were identified in the previous step (DNS lookup).
(4) *HTTP GET request* As the web connectivity test connects to tested websites (through the previous step), it sends requests through the HTTP protocol to the servers which are hosting those websites. A server normally responds to an HTTP GET request with the content of the webpage that is requested.

A.3.2 Comparison of results: Identifying censorship. Once the above steps of the web connectivity test are performed *both* over a control server and over the network of the user, the collected results are then compared with the aim of identifying whether and how tested websites are tampered with. If the compared results do *not* match, then there is a sign of network interference.

Below are the conditions under which the following types of blocking are identified:

- *Confirmed DNS blocking*: If the DNS response observed by the user contains IP addresses that (previously) hosted blockpages or an address in private IP address ranges.
- *DNS blocking*: If the DNS responses (such as the IP addresses mapped to host names) do not match. Note that DNS blocking is not a superset of "Confirmed DNS blocking"; we only list a test result as "DNS blocking" if it was not categorized as "Confirmed DNS blocking" per the above specification.
- *TCP/IP blocking* If a TCP session to connect to websites was not established over the network of the user.
- *HTTP blocking* If the HTTP request over the user's network failed, or the HTTP status codes don't match, or all of the following apply:
  (1) The body length of compared websites (over the control server and the network of the user) differs by some percentage
  (2) The HTTP headers names do not match
  (3) The HTML title tags do not match

Figure 4 shows the aggregated results of the web connectivity tests run by Myanmar users and presents details about the types of anomalies observed.

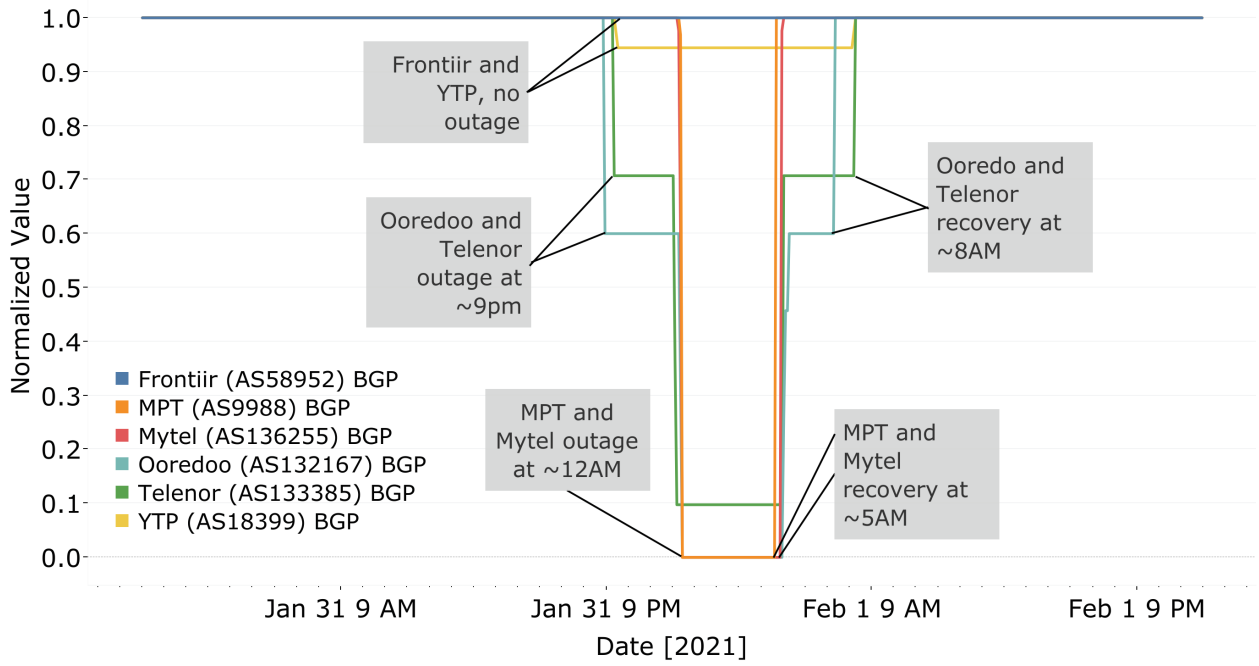

Figure 6: IODA's BGP signals show the differences in timing and extent of the Internet connectivity outage that occurred on Feb. 1 (the day of the coup). While some ASes observed an initial drop in connectivity at 21:00 UTC on Jan 31, others experienced an outage just after midnight UTC on Feb 1. These timing differences are also visible when examining the outages' end-times. Further, a few ASes experienced only minor outages during this period.

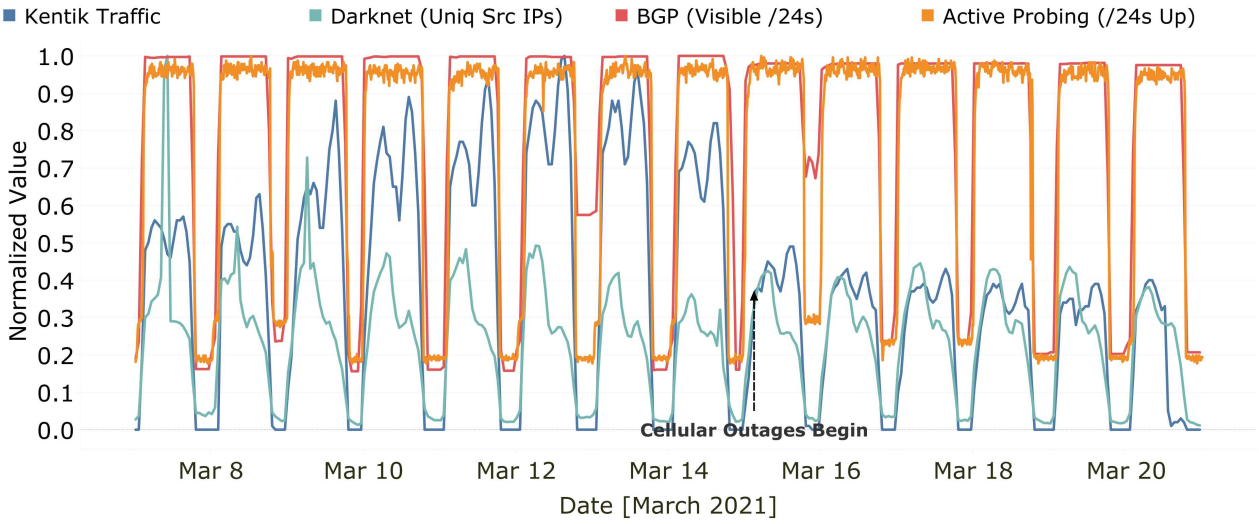

Figure 7: Nightly Internet outages and cellular restrictions. From February 14 to April 28, complete Internet connectivity outages occurred every night in Myanmar. In this figure, we use data from IODA and Kentik to show a two week period where these nightly outages occurred. In the "Kentik Traffic" curve—which shows the traffic seen by Kentik for all ASes in Myanmar aggregated together—we observe a significant reduction after March 15; this reduction corresponds with the beginning of cellular data restrictions that have been in place from March 15 onward. In Figure 3, we break down the traffic by individual ASes and show that cellular ASes, in particular, observed a massive reduction in traffic from March 15.