A Multidimensional Network Forensics Investigation of a State-Sanctioned Internet Outage

Antonio Mangino and Elias Bou-Harb
{antonio.mangino, elias.bouharb}@utsa.edu
The Cyber Center For Security and Analytics. University of Texas at San Antonio, San Antonio, United States

***Abstract*—In November 2019, the government of Iran enforced a week-long total Internet blackout that prevented the majority of Internet connectivity into and within the nation. This work elaborates upon the Iranian Internet blackout by characterizing the event through Internet-scale, near real-time network traffic measurements. Beginning with an investigation of compromised machines scanning the Internet, nearly 50 TB of network traffic data was analyzed. This work discovers 856,625 compromised IP addresses, with 17,182 attributed to the Iranian Internet space. By the second day of the Internet shut down, these numbers dropped by 18.46% and 92.81%, respectively. Empirical analysis of the Internet-of-Things (IoT) paradigm revealed that over 90% of compromised Iranian hosts were fingerprinted as IoT devices, which saw a significant drop throughout the shutdown (96.17% decrease by the blackout's second day). Further examination correlates BGP reachability metrics and related data with geolocation databases to statistically evaluate the number of reachable Iranian ASNs (dropping from approximately 1100 to under 200 reachable networks). In-depth investigation reveals the top affected ASNs, providing network forensic evidence of the longitudinal *unplugging* of such key networks. Lastly, the impact's interruption of the Bitcoin cryptomining market is highlighted, disclosing a massive spike in unsuccessful (i.e., pending) transactions. When combined, these network traffic measurements provide a multidimensional perspective of the Iranian Internet shutdown.**

***Index Terms*—Internet Outage Detection, Internet Background Radiation, Internet-of-Things, Network Forensics**

I. Introduction

Present-day global geopolitics has witnessed an abrupt surge in civil unrest and protests. Citizens in various nations, ranging from South America to Asia, have begun to voice their discontent with government authority or related legal policies. Persistent civil unrest may result in nation-wide economic, diplomatic and militant repercussions. Recent protests in Iran have led to strained United States-Iranian diplomatic relations, intensifying after a Ukrainian passenger plane was shot down over Iranian airspace, killing 176 people from multiple nations. In an effort to prevent the formation of a larger movement, the Iranian government issued a state-sanctioned Internet shutdown. Beginning on November 16, 2019 and lasting one full week, Iranian citizens were unable to use the Internet for communication, could not conduct financial exchanges, nor could they connect to a large number of applications necessary for daily activities. While state-sanctioned Internet censorship is preceded by similar events, (e.g., the three year Turkish ban on Wikipedia and the Iraqi ban on Social Media), the Iranian Internet blackout marked the most thorough to date, commonly labeled by media sources as a *total* shutdown. To this end, this work offers a multidimensional, empirical analysis of the Iranian state-sanctioned Internet blackout, providing insights on the government's efforts for taking their country offline.

Research Objective. The Iranian state-sanctioned Internet shutdown is a historically important event, indicating the escalating measures governments are taking in order to quell civil unrest. Despite growing societal reliance on a resilient Internet connection, governments now have a precedent for virtually *unplugging* their nation's Internet. Therefore, to provide empirical measurements and quantify the extent of the Iranian Internet shutdown, which may emerge as a precedent for future state-sanctioned censorship events, this work offers insightful network traffic measurements observed and analyzed from various Internet-scale perspectives.

Contributions. Prompted by overwhelming global geopolitical unrest and the necessity of analyzing and recording such a momentous event for historical analysis, this work offers the following contributions towards specifically measuring the Iranian state-sanctioned Internet outage:

- **Event characterization from a network telescope perspective.** A number of preceding works empirically investigate Internet outages by leveraging large-scale network traffic telescopes and Internet Background Radiation [1–3]. Aggregating data-generated metrics during the recent Iranian Internet shutdown, this work offers unique insights by analyzing nearly 50 TB of recent Internet-scale, macroscopic network traffic over a two-week time interval. Such data revealed a daily $800,000$ unique compromised host addresses actively scanning the Internet, dropping to $698,532$ during the peak of the Iranian Internet blackout. Furthermore, Iran-specific national metrics reveal a large decrease in compromised Iranian addresses, from $17,677$ before the event to an event low of $1,896$ (89.3% decrease). Moreover, additional analysis revealed that over 90% of the Iranian Internet space consisted of Internet-of-Things (IoT) devices [4] ($16,296$ discovered IoT devices vs 886 discovered non-IoT devices).
- **Analysis of ASN-level BGP routing availability.** Prior investigations into Border Gateway Protocol (BGP) reachability during nation-wide outages revealed ASN-level insights [5]. This work leverages the BGPStream utility to capture BGP routing availability across a two-week pe-

riod. Geolocation and nation-specific analysis revealed the Iranian Internet shutdown's impact on ASN reachability, which dropped by nearly 85% (1,120 reachable ASN on November 14$^{\text{th}}$ vs 173 reachable ASN on November 20$^{\text{th}}$. Further comparisons of BGP reachability from multiple global vantage points reveal a number of inconsistencies, highlighting possible nation-wide filtering of other nation's IP addresses — BGP nodes in North America and Australia were unable to communicate with nations such as Afghanistan, yet nodes located in South America and Africa did not receive the same reachability errors.

- **Impact analysis on global Bitcoin exchanges.** Analysis of the Bitcoin cryptocurrency market revealed a sharp decrease in successful transactions, correlating with the November 2019 Iranian Internet shutdown. The cryptocurrency market has seen an explosive increase in recent years, with global miners and exchanges expanding rapidly; providing a purely "online" architecture for Internet measurements. Roughly 25% of all global Bitcoin trading was interrupted (350,023 transactions on November 14$^{\text{th}}$ vs 264,370 on November 17$^{\text{th}}$). Such large-scale disruptions caused extensive delays to crypto exchanges, with abrupt inflation of `mempool` aggregate memory being used to store pending transactions (reaching maximum waiting sizes of 89,770,655 bytes).

The rest of the paper is organized as follows. The following section enumerates upon our data aggregation and methodology, while Section 3 reports our results, providing detailed measurements of the Iranian Internet shutdown. Section 4 provides a brief review of related works while Section 5 summarizes the contributions of this work while pinpointing a few future topics of interest.

II. Methodology and Data Aggregation

Here, we discuss the various data sources compiled for this work and the employed methodologies for conducting large-scale network traffic measurements.

Collection of IBR. To provide a macroscopic, Internet-scale IBR perspective, we have leveraged a /8 network telescope operated by the Center for Applied Internet Data Analysis (CAIDA). Comprised of over 16 million allocated IP addresses, the CAIDA network telescope is routable, yet does not host any legitimate services. Therefore, network traffic collected is unsolicited and oftentimes generated by compromised devices scanning the Internet space in an attempt to propagate. Such an extensive network telescope provides very good visibility of unsolicited Internet traffic. In fact, the CAIDA telescope collects roughly 3.6 TB of network traffic per day. Monitoring nearly two weeks of global IBR (Nov 14$^{\text{th}}$ — Nov 25$^{\text{th}}$ of 2019), the telescope captured nearly 50 TB of globally-generated IBR - providing a comprehensive data set relevant to the Iranian Internet shutdown.

Inferring compromised host devices. Next, a Threshold Random Walk (TRW) probing algorithm [6] is developed and used to extract packet flows generated by compromised source addresses. Similar to the approach proposed by Rossow [7], the TRW algorithm identifies malicious port scans within the aggregated IBR. To confirm that these hosts were intentionally scanning the network telescope and that collected traffic was not a product of misconfiguration, such devices were characterized as sending 64 packets during a 300 second time interval. We also filter out typically benign scanners by using various publicly available lists. If no packets were received during the time interval and the packet threshold was not met, the flow was dropped and not considered to be a compromised/unsolicited host. From the collected IBR, the employed TRW algorithm discovered roughly 850,000 unique, scanning hosts per day, globally.

Fingerprinting exploited IoT devices. Upon discovering compromised hosts, further analysis categorized IoT devices against non-IoT devices that were found to be scanning. To accomplish this, this work leveraged the developed technique by Pour et al. [8, 9], which operated a set of learning algorithms on passively-collected banners in conjunction with active probing. The technique exploits an extensive feature set, comprised of IP/TCP packet header fields and TCP options [10]. Such packet information is readily available from IBR data, and is further augmented by actively gathering service banners. The technique in [8, 9] further induced immediate reverse scans against each identified IP address, in order to probe a range of nearly 50 ports and services. These scans are intended to retrieve service banners and application-level protocol details (e.g., HTTP(s), TELNET, SMTP(s), SSH, FTP, etc.). Unsecured IoT devices will typically respond to such scans, replying with text-based banners that contain vital operating system information (e.g., embedded, RouterOS, FritzOS), to be used during IoT-device fingerprinting. Readers that are further interested in the leveraged technique and its detailed *modus operandi* are kindly referred to [8, 9].

To this end, in this work, a Random Forest (RF) classifier was employed as part of the leveraged technique to identify over 250,000 global and 16,000 Iranian IoT devices, daily. Employing a shallow machine learning classifier such as the RF model reduces processing time and complexity, while providing accurate characterizations and interpretable feature sets.

Investigating AS reachability. After fingerprinting globally exploited devices, we employed a two-dimensional approach for longitudinally measuring Iranian AS reachability. First, the compromised hosts identified by the employed TRW algorithm were geographically located using the MaxMind GeoLite 2 database. Iranian-specific IP addresses were identified, as well as network blocks of neighboring nation states (e.g., Afghanistan, Turkey, etc.). Nearly 150 Iranian-based ASNs were characterized as hosting such compromised devices. Next, we supplement these measurements through utilizing CAIDA's BGPStream framework [5]. The BGPStream framework consists of multinational nodes, continually scanning the Internet space for reachable ASNs (e.g., /24 networks). Information retrieved by these scans includes BGP routes directly retrieved from responding routers, their routing tables and their neighboring peers. Over 1000 Iranian-based

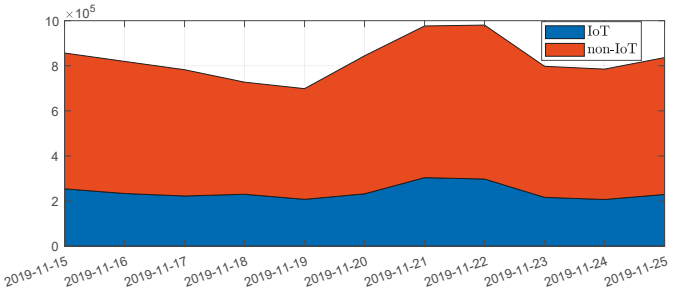


Fig. 1: The total number of compromised IoT devices and non-IoT (desktop) machines scanning the Internet

ASNs were identified by active BGP probing, dropping to an event low of just under 200 during the Iranian Internet shutdown.

The CAIDA IODA project. We validate our findings by analyzing and corroborating measurements retrieved from CAIDA's IODA project [11]. The IODA project provides comprehensive network measurements through analyzing IBR, conducting ICMP scans and performing BGP analysis for operational monitoring. The data published by IODA assists this work in providing a detailed measurement of the Iranian Internet shutdown by supplementing ASN-level and geographic results.

III. Empirical Results

To shed light on the impact of the Iranian Internet shutdown, we leverage various vantage points to empirical illustrate the state of the Iranian Internet. This section enumerates upon the executed multidimensional measurements of the Iranian Internet space.

Discovery of compromised devices. Analyzing nearly 50 TB of IBR revealed a significant $856,625$ compromised devices scanning the Internet space, visualized in Figure 1. The first day of the Iranian shutdown saw a 4.35% decrease in global compromised devices ($819,392$ unique addresses), while the lowest number of recorded devices was discovered on the fourth day, with a 18.46% decrease ($698,532$ unique addresses). While such a significant decrease is not only indicative by the Iranian Internet shutdown, correlating trends were discovered during Iran-specific device analysis. Following the employment of the MaxMind GeoLite database, exploited devices were geolocated and Iranian addresses were discovered for further processing.

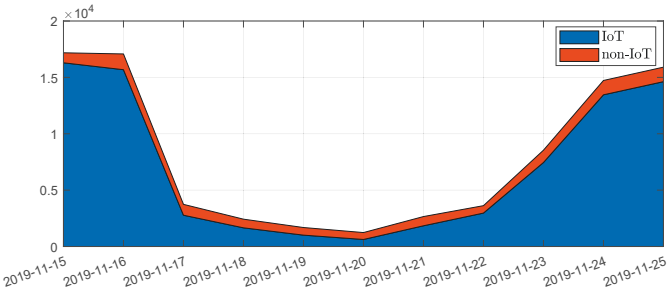
Investigation into Iranian IP addresses revealed a total of $17,182$ compromised Iranian addresses scanning the Internet space on November 15^{th}, visualized in Figure 2a.

Witnessing a sharp decrease on the first day of the shutdown, exploited hosts actively producing IBR dropped by 78.24% (3739 unique addresses). By November 20^{th}, Iranian connectivity reached its lowest point, with only $1,237$ scanning devices (92.80% decrease). On November 21^{st}, the Iranian government began to revive the Internet in its capital Tehran, correlating with a 26.67% increase in exploited addresses. Furthermore, our results illustrate the gradual recovery of the Iranian Internet, with a measure of normalcy returning by November 24^{th} ($14,727$ total compromised scanning devices, 85.71% restored).

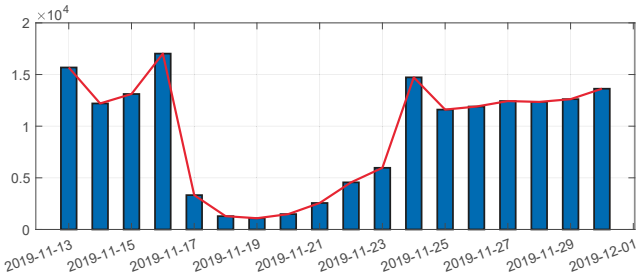
To corroborate our Iranian-specific measurements, we explore the publicly available data published by the Internet search engine ZoomEye, illustrated in Figure 2b. Internet search engines continually scan the Internet space in an effort to identify Internet-facing devices with open ports and services. The statistics published by ZoomEye reveal a direct correlation with our findings. $15,502$ Iranian devices were identified on November 14^{th}, dropping to an event-low of $1,084$ on November 20^{th} (93.01% decrease). The Iranian Internet shutdown saw near-immediate results, resulting in an extreme decline in outbound network traffic.

Identification of exploited IoT devices. Following the identification of globally and Iranian-specific compromised hosts, we identified exploited IoT devices through the aforementioned shallow machine learning classifier. Of the compromised Iranian devices discovered on November 14^{th} ($17,182$), $16,296$ were identified as IoT devices. Interestingly, nearly 94.8% of all compromised Iranian IP addresses were attributed as IoT, necessitating a longitudinal analysis of Iranian IoT devices in comparison with non-IoT, traditional machines.

These results are not entirely unexpected — the original



(a) IBR results



(b) ZoomEye results

Fig. 2: The total number of Iranian devices discovered from IBR and ZoomEye, respectively

developers of the machine learning classifier, Pour et al. [9], reported Iran as hosting 10.17% of globally infected IoT devices. Our results reveal that the $16,296$ discovered Iranian devices equaled 7.32% of recorded global IoT devices

ASN	Nov15	Nov16	Nov17	Nov18	Nov19	Nov20	Nov21	Nov22	Nov23	Nov24	Nov25
48159	3,518	3,375	298	1	1	1	35	242	1,976	3,139	3,446
12880	1,845	1,792	1,792	313	10	9	53	205	1,110	1,790	1,721
16322	1,688	1,276	409	264	172	168	212	187	362	1,622	1,606
58085	1,036	1,056	0	0	0	0	0	34	51	694	1,119
43754	916	1,040	211	187	155	138	209	191	613	913	1,044
58224	880	931	381	0	0	0	0	195	755	910	935
31549	610	613	2	2	5	5	93	235	459	576	591
25124	369	272	0	0	0	0	64	239	163	305	354
1756	138	114	17	9	0	0	8	0	10	64	58

TABLE I: Top identified Iranian ASN by discovered IP address count

on November 14th (254, 408). Iranian IoT devices witnessed the largest impact of the Iranian Internet shutdown and by November 17th, 78.23% of such devices were no longer scanning the Internet space (2, 776 IoT devices, 82.97% decrease). Iranian IoT-specific connectivity reached its lowest point on November 20th, with only 624 discovered scanning devices (96.17% decrease). IoT devices witnessed a 96.17% drop (624 devices).

Additional investigation into the disparity between Iranian IoT and non-IoT devices revealed that a higher number of IoT-specific scanners were affected by the Internet outage than traditional computers. On November 15th, the ratio of device composition was equal to 18.39 IoT against 1.00 non-IoT, respectively (16, 296 IoT vs 886 non-IoT devices). However, by November 20th, that ratio dropped to 1.02 IoT against 1.00 non-IoT, respectively (624 IoT vs 613 non-IoTdevices). The number of Iranian IoT devices detected by the network telescope dropped by 96.17%, whereas only 56.12% of non-IoT devices were affected, visualized in Figure 3. One characteristic that may have attributed this large

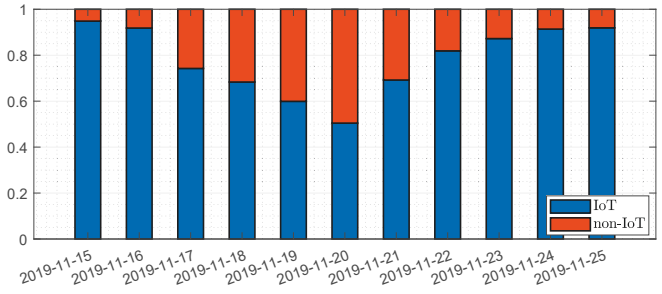


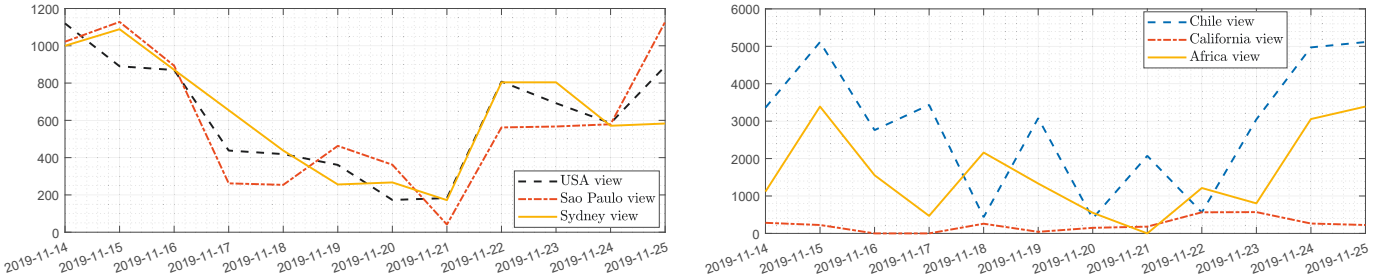
Fig. 3: The ratio of compromised Iranian IoT devices against non-IoT devices

variance is the actual scanning techniques of IoT and non-IoT devices. Because IoT devices were found to be scanning at lower throughput rates, once these rates were decreased by the Internet shutdown, they were no longer identified as scanners by the developed methodology. Consequently, because non-IoT devices generally scan the Internet space at higher frequencies, the Internet outage had less of an affect on their discovery and characterization.

Investigation into ASN reachability. Subsequent to the identification of compromised scanner devices originating from the Iranian Internet space, we attributed known devices to their Internet Service Providers and related ASNs. On November 15th, network traffic originated from 145 unique Iranian ASN. The lowest number of discovered Iranian ASN was 93, on November 20th (35.86% decrease). The total number of ASNs communicating from Iran did not see a dramatic decrease equivalent to the drop of actively communicating devices; however, the ASN that were disconnected or blocked hosted the largest number of compromised devices. To this end, our results provide evidence that the Iranian government specifically targeted and disconnected larger ASNs, a tactic which have been also used by the Egyptian government during censorship of riots in 2011.

Table I illustrates the Iranian ASNs that hosted the largest number of compromised devices, as well as the date that they were *disconnected* by the Iranian government. The largest ASN, 48159, hosted 3518 exploited addresses on November 15th. By November 17th, only 298 addresses were generating network traffic, and by November 18th only 1 address was actively communicating. Similarly, the majority of the ASN summarized within the table saw dramatic decreases on November 17th, with many being completely disconnected by November 18th (1756, 58085, 25124 were found to have 0 active hosts). These ASN did not begin recovering until November 22nd, reaching near-peak numbers by November 24th. Interestingly, a number of specific ASNs were not affected to the same degree. For example, ASN 16322 witnessed a 90.05% decrease (in comparison to ASN 48159's 99.99%), yet never dropped below 160 active addresses. ASNs 43754 and 42337 saw a similar trend, indicating that these ASN may have hosted critical, or essential networks and were thus spared from a complete disconnect.

In comparison with our IBR results, this work leveraged 6 BGPStream nodes to retrieve global BGP reachability data. These nodes are located in North America, South America, Africa and Australia. Figure 4a demonstrates the total number of reachable Iranian ASNs discovered by the North American, South American and Australian nodes. Such results are fairly consistent with one another, illustrating a major drop from roughly 1000 reachable ASN down to 200 throughout the Iranian Internet shutdown. However, comparing the results of each node revealed widespread inconsistencies of BGP scan data, visualized in Figure 4b. The node located in Chile received the highest number of responses for reachable Iranian ASNs (peak equal to 5114 on Nov 15th, closely followed by



(a) The total number of reachable Iranian ASNs discovered by BGP scans

(b) Inconsistencies of BGP scan data

Fig. 4: ASN reachability results from the BGPStream utility [5]

the node located in Africa (peak equal to 3390 on Nov15th. However, the node located in California received vastly lower results, never receiving more than 550 responses. Additional comparisons between the nodes illustrated a similar picture in Iraq, Pakistan, Afghanistan, Saudi Arabia and Turkey. In fact, all BGP packets sent to the Afghanistan IP address space were dropped if they did not originate from the node located in Africa, while the South American node received responses on select days. These findings hint upon nation-wide filtering of specific addresses based on their origin country.

Examination of the Bitcoin cryptocurrency exchange. Evaluating Bitcoin cryptocurrency exchange data made publicly available by *Blockchain.com*, we examine correlations between Iranian Internet outages and global Bitcoin crypto-mining trends. While these correlations may not be solely caused by the Iranian Internet outages, examining traffic measurements of a "purely online" market such as the Bitcoin cryptocurrency provides an alternative perspective of global Internet connectivity. Furthermore, the drastic decrease in successful Bitcoin transactions reveals a linear correlation with the Iranian Internet shutdown. On November 15th, 325,145 Bitcoin transactions were successfully carried out; however, only 283,468 transactions were completed on November 16th (12.82% decrease). By November 17th, only 264,370 Bitcoin transactions were finalized (18.69% decrease). While cryptocurrency markets are relatively volatile, such data does not necessarily equate to fewer Bitcoins being mined or put up for sale. Rather, there was a *choke* on the market, with offers being left uncompleted and waiting in memory to be processed and sold. However, to provide correlation between this symbolic decrease in transactions, we investigate the total number awaiting processing within the aggregate `mempool` (current number of bits being help by a node for pending transactions).

Typical drops in successful trades, such as from October 5th (326,683 transactions) to October 6th (277,613 transactions), did not witness a large increase in pending transactions (4,403 to 4,057, respectively). However, the decrease in transactions beginning on November 14th reached a peak of 15,088 pending transactions. Moreover, the aggregate `mempool` size saw drastic inflation. Reaching sizes of up to 89,770,655 bits, the aggregate Bitcoin `mempool` witnessed a 85.91% weekly increase, in contrast to the week prior's high of 12,645,599 bits. Therefore, we can ascertain that the November 2019 global decrease in Bitcoin cryptocurrency exchange was a peculiar event - one that follows a similar pattern to an alternative, yet recent *choke* on the Bitcoin market. In the first weeks of February, 2020, large-scale distributed denial of service attacks against the Iranian Internet infrastructure dropped the nation's connectivity by nearly 25%. A similar effect was seen on the Bitcoin cryptocurrency market, with the `mempool` size peaking at 27,351,731 bits, up from the previous week's peak of 13,559,610 bits (101.71% increase). To this end, this highlights the correlation between Iranian outages and global Bitcoin market. This correlation may be caused by a number of factors, primarily, the large number of devices actively mining cryptocurrency in Iran [12].

IV. Related Work

In this section, we investigate related works that contribute to large-scale network traffic measurements. Specifically, we discuss outage characterization and prediction-based methodologies as well as we enumerate upon analytical measurements of large-scale Internet outages.

Prediction and classification of large-scale Internet outages. Despite societal reliance on a reliable Internet connection, Internet outages are frequent. Aceto et al. [13] conducted a comprehensive survey on Internet outages at large. Their work proposed guidelines for characterizing outages, while systematically analyzing related methodologies for investigating large-scale outage events. Furthermore, Quan et al. [14] constructed an ICMP-based model for identifying global Internet outages. By probing the Internet space at regular intervals, this work reported Internet stability as a whole. Moreover, improving upon their outage detecting system, Quan et al. later developed Trinocular [15]. The Trinocular methodology leverages ICMP probes to scan the Internet space and detect outage events — with an efficient, low-interaction model to determine points of interest.

These works illustrates the diversity of Internet outages. While some events may last only a few minutes or effect small populations, nation-wide Internet outages may debil-

itate critical infrastructure. During state-sanctioned Internet shutdowns, such national assets are expected to remain *online*. Our results disclose that a portion of the Iranian Internet space was still actively communicating across the Internet, possibly attributed to devices deployed within government or critical infrastructure.

Empirical measurements of state-sanctioned Internet outages. Preceding works that investigate large-scale Internet outages can generally be split into two categories: outage identification through active probing (e.g., BGP or ICMP scanning) and outage identification by analyzing Internet Background Radiation (IBR). Shavitt et al. [16] conducted active measurements to investigate the Arab Spring geopolitical events of 2011. Leveraging 3.63 million traceroute measurements, their work reports the condition of the Egyptian, Libyan and Syrian Internets during the Arab Spring. Employing both active BGP inter-domain probing and analyzing IBR, Dainotti et al. [17] performed a similar investigation into the Egyptian and Libyan Internet outages of 2011Recently, the outage detection classifier Chocolatine was developed by Guillot et al. [18]. Investigation into Internet-scale IBR collected at a network telescope exposed a consistent trend; the number of scanning IP addresses from each geographical ASN remains constant. Leveraging such observations, seasonal ARIMA was used for time series forecasting, predicting and evaluating the number of unique IP addresses generating IBR from individual ASNs, attributing deviations or drops to Internet outages.

The aforementioned literature introduce methodologies for identifying and measuring Internet outages through active probing and IBR analysis. Similarly, the presented work leverages BGP inter-domain routing tables and an Internet-scale network telescope to uniquely investigate and analyze the Iranian Internet shutdown. Moreover, further contributions towards the categorization of collected IBR reveal interesting IoT-specific insights on the Iranian Internet space, as well as identify the systematic shutdown of key operational ASNs.

V. Concluding Remarks

This study empirically measures a nation-scale censorship event. Processing nearly 50TB of unsolicited Internet Background Radiation revealed over $17,000$ compromised devices scanning the global Internet from the Iranian IP space, with $16,296$ attributed as IoT. Furthermore, our results characterize a drastic decrease in Iranian ASN reachability (145 active ASN dropped to 93). Further, we shed light on global BGP inconsistencies due to nation-wide filtering of specific IP address spaces. Finally, we analyze the Bitcoin cryptocurrency market to reveal a decrease in successful transactions against the amount of `mempool` memory storing pending transactions. Future work can provide an in-depth analysis of network packets, specifically those generated by IoT devices. Additionally, future works that leverage crypto nodes or related infrastructure [19] to characterize Internet outages could offer insightful inferences related to Internet routing and connectivity.

References

[1] Karyn Benson el al. Gaining insight into as-level outages through analysis of internet background radiation. In *2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 447–452. IEEE, 2013.

[2] Ryan Bogutz, Yuri Pradkin, and John Heidemann. Identifying important internet outages (extended). Technical report, TR ISI-TR-735, USC/ISI, 2019.

[3] Farooq Shaikh, Elias Bou-Harb, Nataliia Neshenko, Andrea P Wright, and Nasir Ghani. Internet of malicious things: Correlating active and passive measurements for inferring and characterizing internet-scale unsolicited iot devices. *IEEE Communications Magazine*, 56(9):170–177, 2018.

[4] Nataliia Neshenko, Elias Bou-Harb, Jorge Crichigno, Georges Kaddoum, and Nasir Ghani. Demystifying iot security: an exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations. *IEEE Communications Surveys & Tutorials*, 21(3):2702–2733, 2019.

[5] Chiara Orsini et al. Bgpstream: a software framework for live and historical bgp data analysis. In *Proceedings of the 2016 Internet Measurement Conference*, pages 429–444, 2016.

[6] Elias Bou-Harb, Mourad Debbabi, and Chadi Assi. A novel cyber security capability: Inferring internet-scale infections by correlating malware and probing activities. *Computer Networks*, 94:327–343, 2016.

[7] Christian Rossow. Amplification hell: Revisiting network protocols for ddos abuse. In *NDSS*, 2014.

[8] Morteza Safaei Pour et al. Data-driven curation, learning and analysis for inferring evolving iot botnets in the wild. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, page 6. ACM, 2019.

[9] Morteza Safaei Pour et al. On data-driven curation, learning, and analysis for inferring evolving internet-of-things (iot) botnets in the wild. *Computers & Security*, page 101707, 2019.

[10] Elias Bou-Harb, Nour-Eddine Lakhdari, Hamad Binsalleeh, and Mourad Debbabi. Multidimensional investigation of source port 0 probing. *Digital Investigation*, 11:S114–S123, 2014.

[11] Internet outage detection and analysis (ioda). https://www.caida.org/projects/ioda/.

[12] Iran seizes 1,000 bitcoin mining machines after power spike. https://www.bbc.com/news/technology-48799155, 2019.

[13] Giuseppe Aceto, Alessio Botta, Pietro Marchetta, Valerio Persico, and Antonio Pescapé. A comprehensive survey on internet outages. *Journal of Network and Computer Applications*, 113:36–63, 2018.

[14] Lin Quan et al. Detecting internet outages with precise active probing (extended). *USC/Information Sciences Institute, Tech. Rep*, 2012.

[15] Lin Quan, John Heidemann, and Yuri Pradkin. Trinocular: Understanding internet reliability through adaptive probing. *ACM SIGCOMM Computer Communication Review*, 43(4):255–266, 2013.

[16] Yuval Shavitt and Noa Zilberman. Arabian nights: Measuring the arab internet during the 2011 events. *IEEE Network*, 26(6):75–80, 2012.

[17] Alberto Dainotti et al. Analysis of country-wide internet outages caused by censorship. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, pages 1–18, 2011.

[18] Andreas Guillot et al. Chocolatine: Outage detection for internet background radiation. In *2019 Network Traffic Measurement and Analysis Conference (TMA)*, pages 1–8. IEEE, 2019.

[19] Elias Bou-Harb. A brief survey of security approaches for cyber-physical systems. In *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–5. IEEE, 2016.