Free and Open
COMMUNICATIONS
https://foci.community on the Internet

A Worldwide View of Nation-state Internet Censorship

Alexander Master
Purdue University

Christina Garman
Purdue University

Free and Open Communications on the Internet 2023(1), 1-21

A Worldwide View of Nation-state Internet Censorship

Alexander Master
Purdue University

Christina Garman
Purdue University

Abstract

Nation-states impose various levels of censorship on their Internet communications. As access to Internet resources has grown among the global population, some governments have demonstrated an increased willingness to filter content, throttle connections, or deny access to Internet resources within their sphere of influence. Researchers, policymakers, and civil liberty advocates need an understanding of the technical means that Internet censors implement. This work presents a worldwide view of nation-state Internet censorship derived from Internet measurement data and prior research. We performed a cross-sectional study of 70 countries during a one-year period, illuminating current online censorship trends. We then conducted a systematic study of prior work to illustrate if and how those same countries performed censorship over the past two decades. Our research contributions are three-fold: (1) a snapshot of current and emerging Internet censorship methods around the globe, (2) a holistic view of changes in censorship trends over the past two decades as the Internet has become a primary means of human communication, and (3) a research framework to allow for ease of continual analysis.

1 Introduction

The Internet has become one of the most significant communication mechanisms in human history. In terms of media influence, it has surpassed television, print media, and radio [50] and is a routine aspect of daily life for millions of people globally. However, some nation-states impose censorship on Internet communications within their sphere of influence. Irrespective of the motivation behind Internet censors—ideological, autocratic, legal, social, or otherwise—Internet censorship research has become a broad interdisciplinary endeavor, with emphasis on explaining *how* online censorship happens.

Several research communities focus on Internet censorship problems. Internet measurement research often characterizes traffic filtering and manipulation at scale. Reports tend to be published after notable historic events, or when countries make overt changes to their censorship practices and capture public attention. Privacy-enhancing technology groups often develop anti-censorship software to allow users in censored areas to circumvent barriers to accessing information. Sociologists and political scientists study the effects of censorship on populations of people. Less traditional works — such as reports produced by advocacy organizations — document instances of Internet shutdowns and blocking of online platforms. Other researchers publish case studies of specific nations, highlighting the government's actions and contextualizing the censorship geopolitically. While each individual contribution is valuable, these works struggle to characterize trends in Internet censorship globally. The narrow scope of a case study only shows the experience of one country or region, for a limited time period. Few works provide global insights over multi-year measurement periods.

This paper fills this gap by providing a worldwide representative view of Internet censorship methods. By drawing from several research communities and disciplines, we provide a more holistic view of the technical measures used by nation-states in a modern context and historically over the past 20 years.

Contributions. Our research contributions are three-fold:

- First, we conducted a cross-sectional study of 70 countries during a specified period of one year. We used the same countries surveyed in the Freedom on the Net (FOTN) annual report by Freedom House [73] to ensure global representation across the continents. Diverse datasets showed how Internet censors deny access to information resources and communication mediums.
- Second, we analyzed prior work to illustrate historical censorship methods from these same nation-states over the past 20 years. The results of the analysis illustrate trends in Internet censorship and changes in Internet censor methods over time. For example, we observed that most censors are seemingly willing, and in fact continue, to use "old" filtering methods, even though they are easy to bypass. And increasingly, governments deliberately perform total Inter-

net shutdowns to achieve their censorship goals.

- Finally, the methodology presented offers an easily reproducible framework for continuous reporting and studying of worldwide censor activity.

2 Background and Related Work

2.1 Nation-state Internet Censorship

The authorities of some countries go to great lengths to deny their citizens free and open access to Internet resources. Nation-state Internet censorship is generally characterized as either centralized or decentralized in nature. Centralized censorship often occurs on government-controlled infrastructure. In some nations, there are few (or only one) Internet Service Providers (ISPs) or cellular carriers for users to choose from. When the state owns the infrastructure and controls Internet routing, filtering "objectionable" material or limiting access is more straightforward. The People's Republic of China (PRC) is the most cited example of centralized censorship [16, 26, 29, 40, 55, 56, 86, 95–98, 102, 103, 108, 132, 150, 172, 180, 188, 201, 203]; their censorship apparatus is known as the "Great Firewall of China." Other examples include small countries with limited access to transnational fiber switching. Syria, which only has one government-controlled autonomous system (AS) [34], can uniformly implement technical censorship measures across its population.

In contrast, decentralized censorship tends to result in fragmented implementation. Websites available in one region may be denied in another. Examples of decentralized censorship regimes are the Russian Federation [147, 189] and India [66, 158, 198]. Authorities in these nations legally compel private-sector service providers to perform web filtering, throttling, or shutdowns. Technical implementations may vary widely between corporations, resulting in a patchwork of censorship. We will refer to any entity that manipulates network traffic for the purposes of censorship a "censor" throughout this paper. While Freedom House's data shows an overarching continual reduction in global Internet freedom overall, some nations have scaled back censorship efforts, such as Myanmar from 2012-2019 [134], The Gambia from 2017-present [80], and Saudi Arabia from 2017-present [8].

2.2 Internet Censor Methods

Internet censors use a variety of technical means to deny access to Internet resources. A crude and straightforward method is an Internet shutdown. Feldstein defines Internet shutdowns as "activities undertaken by states to intentionally restrict, constrain, or disrupt Internet or electronic communications within a given geographic area or affecting a specific population in order to exert control over the spread of information, within a timebound period" [57]. Shutdowns can be accomplished by physically disconnecting cable links, logically segmenting network traffic, or manipulating routing tables to ensure traffic does not reach its intended destination. Internet-wide disruptions have occurred when ASes in censoring countries tamper with Border Gateway Protocol (BGP) routing advertisements [115, 134]. Censors also use bandwidth throttling to limit access to particular platforms or media sources [10, 190] for a defined time period, sometimes during elections or incidents of civil unrest. Throttling can be implemented by injecting artificial latency, altering routing paths, traffic shaping, traffic policing, or applying quality of service (QoS) algorithms to "undesirable" traffic [113].

For persistent censorship, censors selectively deny content they deem objectionable. Typically, a censor observes some characteristic of the network traffic to inform a blocking decision. Censors have historically maintained Internet Protocol (IP) address blocklists, tracking servers they wish to deny all traffic to or from. Censors also use port blocking — often against transmission control protocol (TCP), User Datagram Protocol (UDP), or QUIC transport layer protocols — to broadly disallow network packets. Much of the mainstream Internet traffic today is web-based; thus, many censorship methods focus on web-based protocols: Hypertext Transfer Protocol (HTTP), Domain Name System (DNS), and Transport Layer Security (TLS). When a user requests a website, a censor can tamper with the DNS request to serve them a blockpage, redirect the user to a different site, or resolve to a non-existent IP address. With web proxies and URL filtering software, censors can also deny lists of websites from connecting, sending the web browser an HTTP error code or terminating the connection with a TCP reset.

If a censor has deep packet inspection (DPI) capabilities, they can observe the payload content of IP packets. DPI enables the filtering of HTTP, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and other traffic based on keywords in the content of the communication [21, 32, 169]. When users request websites protected by TLS, the traffic is encrypted so a passive observer cannot read its contents. However, censors can read the plaintext Server Name Indication (SNI) extension of a TLS header and block a destination website based on it. Finally, censors with more advanced capabilities use protocol fingerprinting techniques to identify particular protocols, applications, or other encrypted packets based on traffic patterns — and subsequently block associated traffic [152, 157].

2.3 Data Sources

Several concerted efforts have been undertaken in the last 17 years to develop an understanding of how and where Internet censorship happens. Deibert et al. presented results of "the first systematic, academically rigorous global study of all known state-mandated Internet filtering practices" [47], showing evidence of how 26 of 40 countries conducted Internet filtering activities — and the trend has only increased since then. The OpenNet Initiative partnership they operated under shut down research operations in 2014 [165] but made all of its datasets and published materials publicly available on its web page.

Other labs and advocacy organizations have taken on the task of measuring Internet connectivity around the globe, showing censorship where it takes place. The Open Observatory of Network Interference (OONI) began data collection on Internet censorship in 2012 and has continued through the time of this writing [130]. OONI datasets, data explorer, and API are available online[1]. Censored Planet Lab at the University of Michigan, USA, has created and hosted several global Internet measurement projects [141]. "Satellite" [160] and "Hyperquack" [145, 170] measure DNS interference and application layer HTTP/HTTPS manipulation, respectively. Their dashboard for viewing data is also publicly available online[2]. ICLab is a different global, longitudinal measurement platform that utilizes commercial virtual private networks (VPNs) to gain vantage points in countries around the globe to determine censorship activities. The Citizen Lab at the University of Toronto, Canada, has a research effort focused on freedom of expression [101] — although their reporting often focuses on specific political or social impacts of technology censorship rather than wide Internet measurements.

Freedom House is a non-governmental organization (NGO) based in Washington DC, USA. The group is a non-profit and conducts research and advocacy on democracy, political freedom, and human rights — often focusing on Internet freedoms [73]. The group has produced the FOTN report since 2009, qualitatively measuring censorship in up to 70 countries around the world. The report provides valuable macro-level analysis of how users experience the Internet and if freedom of expression is permitted on a scale of "free", "partly free", "not free", or not assessed. Surveyed results are further broken down into scores for three categories; Obstacles to Access, Limits on Content, and Violations of User Rights — the first two categories are particularly relevant to our study. The FOTN country list and rank ordering served as the foundation for our data collection.

2.4 Related Work

In 2008, Deibert et al. published their seminal report Access Denied [47], offering the first global view of Internet censorship. The study data from 2006 covered 40 countries and categorized censor methods into four categories: IP blocking, DNS tampering, Blockpage, and Keyword. We know that there are many other prevalent Internet censorship methods in use today. The authors concluded that nation-states that practiced state-mandated filtering were predominately clustered in three regions: east Asia, the Middle East/North Africa, and central Asia. Internet routing has increasingly grown in complexity since 2006, and the geopolitical landscapes censorship regimes exist within have also changed. Some censors have demonstrated a willingness to use more sophisticated, targeted, and subtle methods, while others use blunt tactics such as Internet shutdowns to achieve their goals. Researchers have also documented online censorship in self-proclaimed liberal democracies, which espouse freedom of speech and expression as values; these nations were not covered in the Access Denied reporting. Deibert et al. had to perform all their measurements using their infrastructure, vantage points, and OpenNet's methodology. They did not have the plethora of Internet measurement datasets available today. We draw inspiration from their approach and provide a broader view of Internet censorship with deeper technical detail. We survey a globally representative list of countries, using diverse datasets for overlapping coverage, and draw upon the latest research in censor methods as described in §2.2.

Tschantz et al. did a study related to ours in 2016 [166] as part of a larger systematization of knowledge (SoK). Section 4 of their paper outlines "censorship as practiced," in which they examined 31 measurement studies to attribute censor capabilities to several high-profile censoring nations. Some of the capabilities were technology-specific (e.g., Netsweeper, BlueCoat, SmartFilter), and the countries were not globally representative as we aimed to accomplish. Gill et al. performed a study similar to ours in 2015, using solely OpenNet Initiative data [65], and only focused on DNS and HTTP filtering of web URLs.

Aceto and Pescapé wrote a survey of censorship detection systems in 2015 [3]. Their work covered academic detection architectures as well as deployed Internet measurement platforms. The study relied on the design goals of the detection system authors for their characterizations, while this survey focuses on the evidence of censorship occurrences.

Many studies have attempted to provide coverage of Internet censorship through measurement platforms [11, 89, 90, 112, 119, 139, 160, 170, 204], the use of literature surveys [3, 24, 110, 179], or crowdsourced data collection [58, 121, 159]. Measurement platforms have various advantages and limitations, and we drew from several to promote overlapping coverage. Surveys provide historical context to our analysis. Prior work also has dozens of individual country censorship case studies, providing us with historical data on censor methods.

3 Methodology

We used a mixed methods (quantitative and qualitative) approach to data collection in our study. Data from the 2021 FOTN report[3] served as a foundation for analysis, scoping the project while ensuring global representation. We assessed

[1] OONI: https://ooni.org/data

[2] Censored Planet: https://dashboard.censoredplanet.org

[3] While the 2022 report has since been published, it did not exist at the time of this analysis.

all 70 assessed countries from the FOTN report using our framework. We used the Internet censorship methods from the taxonomy by Master in [110] to ensure comprehensive coverage of techniques.[4] The elements of the taxonomy are those that we summarize in §2.2 above.

To begin our analysis, we used quantitative data from Internet measurement sources to determine Internet censor actions in each country during the report's timeframe (June 01, 2020 to May 31, 2021). We used the report's timeframe as the measurement period for our study, so our outputs align with their qualitative conclusions. We extracted data from the following sources:

- **OONI.** OONI [58] performs over a dozen Internet measurement tests for censorship in over 200 countries using crowdsourced data from software probes they distribute, and ingest tens of millions of data points monthly. The "web_connectivity" test provides detection mechanisms for DNS tampering, TCP/IP blocking, or blocking by a transparent HTTP proxy.
- **Censored Planet.** Censored Planet provides a web-based dashboard to display the results of their Internet censorship detection. The platform utilizes various passive remote measurement techniques in more than 200 countries. This combination of tools includes: (1) Auger [138] uses TCP/IP side channels to measure reachability between two Internet locations without the use of a vantage point, (2) Satellite [153] uses public DNS resolvers to compare how popular webpages are resolved to determine where interference happens, (3) Quack and Hyperquack [145] use Echo and Discord servers to detect DPI blocking for HTTP and HTTPS traffic.
- **Internet Society Pulse.** Internet Society Pulse curates information about Internet shutdown events occurring around the world and analyzes their economic and human impact. Data from their platform shows time-based network disconnections executed by authorities in the studied countries [159].
- **Access Now.** Access Now is a non-profit organization that promotes digital civil rights around the world [122]. The #KeepItOn project by Access Now generates an annual report and dataset to track Internet shutdowns, social media blockages, and network throttling globally [121].

Journal articles, conference proceedings, and technical reports covering the study timeframe filled gaps unobserved by the data sources above, if applicable. IClab [67, 119] did not have published data for the entirety of the study period dates and was thus excluded. Based on our findings, we filled in the columns and rows of our framework (see §4.1).

After the cross-sectional portion of the study was complete, we used a systematic literature review (SLR) approach [125] to capture the historical context of censorship methods documented outside of the measurement period for each country. We conjectured that presenting historical censorship activities with recent ones would illuminate inter-country and global trends. CensorBib [181] was the starting point for SLR citations. CensorBib is an online archive of selected research papers on Internet censorship maintained by Dr. Philipp Winter [182]; nomination submissions are open to the public. The archive captured many of the country-specific studies from relevant journals and conferences. We treated peer-reviewed journals and conferences as primary data sources, and technical reports and blog postings were considered case-by-case when primary sources were unavailable. Rather than surveying select journal proceedings, we searched for country-specific case studies of Internet censorship. Our list of surveyed nations began with the lowest scores on the FOTN 2021 report ("not free") and ended with the highest scores ("free"). Low-scoring countries tended to have the highest number of citations, while free nations had few (if any) case studies on their censorship practices, with some exceptions.

Limitations and delineations. This study does not aim to measure the quantity or frequency of particular censorship methods, only evidence of their occurrence. In pursuing our goal of illuminating global trends for censor methods, we consequently lose some granularity. For example, in a nation-state with a decentralized implementation of DNS tampering, users served by one AS may be unable to access specific websites, while citizens in other regions can because of non-uniform distribution or implementation of blocklists nationally. If there is enough evidence of censorship in at least one AS, our data will reflect the nation in question as using that censor method. Additionally, our framework does not delineate "censorship leakage" [37], in which the blocking decisions made by particular ASes impact users in other countries outside of the censor's geopolitical borders.

There are limitations inherent to the use of Internet measurement data. Fletcher and Hayes-Bircher demonstrated in [60] that remotely measured Internet censorship datasets were less likely to contain false positives than subject matter expert (SME) analysis when taken as a whole. However, platforms such as OONI have documented records of false positives [145, 198]. To minimize false positives, we manually reviewed instances of "confirmed" censorship for accuracy. We considered detected blockpages in OONI data, regardless of censor method, as definitive censorship. For Censor Planet data, we first ensured a URL with an "unexpected outcome" had a sufficient sample size from the probe (>30 count) prior to consideration. If so, we then considered the proportionality of suspected blocking behavior. If over 50% of attempts resulted in strong indicators (e.g., TCP reset packets), we considered it evidence of censorship. If the majority of attempts resulted in "matches" (page loaded correctly) or less clear-cut

[4] We chose not to include "Resource Exhaustion" (e.g., DDoS attacks) and "Computer Network Attack" from the Internet Censorship Methods Taxonomy [110] in our framework because those methods target resources outside of the censor's sphere of influence, to deny access to *all* Internet users. This study focuses on nation-state censorship against each nation's citizenry. We also combined IP blocking and port blocking into one category.

anomalies (e.g., "content mismatch"), we did not document it as evidence during the cross-sectional study period.

Research publications have limitations and potential for bias as well. Researchers often publish Internet censorship papers on "high-profile" offending countries, while some Western nations receive little scrutiny or attention. Examples include China having 35 citations in this study, while Costa Rica had zero. A globally representative study like ours helps to highlight these gaps in the literature, and point toward important open research questions. Without continual effort across the continents to assess censorship activity, reporting may lean heavily towards historic offenders and not detect new ones. Articles in the literature also tend to focus on key historical events or problems, which may bias researchers' conclusions toward a perception of ever-increasing censorship [92] while potentially leaving out nations that make progress in reducing censorship. Recent efforts by groups such as OONI and Censored Planet to quantitatively highlight emerging censor trends [129, 146, 163] may help to balance this reporting.

4 Results and Discussion

4.1 Discussion of the Framework

The final data and overall results of the study are depicted in Table 1. The 70 assessed countries are the rows of Table 1, sorted by lowest to highest FOTN "total score." The column headers are organized into four sections; (1) Country name and ISO country code, (2) FOTN scores and status data, (3) Internet censorship methods, and (4) notes.

FOTN scoring for obstacles to access, limits on content, and violations of user rights are included as columns for each country to provide context to our findings. FOTN uses 21 questions (nearly 100 sub-questions) to determine scoring in each category; the scores are summed up to determine a country's total score (100-70 = free, 69-40 = partly free, 39-0 = not free).

Internet censorship methods are listed as columns across the top, and are the central element of our study. Countries we found evidence of using a particular method during the measurement period are identified with a circle "●". If the censorship method was only instituted for a specified period of time (rather than persistent filtering), we indicated that with an unfilled circle "○". If we encountered anecdotal observations of censorship, but could not confirm it with quantitative evidence or a prior study, we marked that country with a square "□" to mean "unconfirmed"[5]. These data represent all censor activity during the study period.

After we completed the cross-sectional portion of the study and the SLR, we illustrated historically observed censorship in Table 1 using an upside-down triangle "▼"; that is, documented censor activity that occurred at some time outside of the study period over the last 20 years. The "notes" field on the far right includes additional qualitative context for each particular country. Historical events (e.g., war, conflicts, elections, civil unrest) often coincide with Internet censor activity. Exceptions or further explanations for a particular piece of evidence may have been warranted and included in the notes section as well. Table 3 documents all citations and evidence of Internet censorship methods by country; interested readers can find it in Appendix A.

The framework is notable for its approachability and flexibility. Data collection, visual investigation, and quantitative analysis can all be performed using the same document. The elements are also modular. For example, suppose a fundamental change is made to a component of the Internet protocol suite, revealing a newly viable censorship method. In that case, a column can be added to accommodate and track its use. Conversely, a column could be removed if changes are made that eliminate an entire class of censorship methods. An example could include the introduction of an Encrypted Client Hello (ECH) into the TLS standard. Because censors currently rely heavily on the plaintext SNI extension present in TLS 1.3 to target traffic for blocking, implementing encryption to obfuscate SNIs may eliminate the "TLS-based Filtering" column entirely. This outcome is not a certainty, but the framework could oblige the change if it happened. Finally, the framework supports ease of reproducibility. For example, in five years a researcher can use the document as a baseline (all data points are historic) and fill in only the gap data for the five years of coverage — revealing emerging global trends.

4.2 Analysis and Trends

Figure 1 and Table 2 are examples of quantitative analyses that can be derived from our framework. Figure 1 illustrates summary totals of countries that utilize particular censor methods. The bottom bars (red) indicate active use during the measurement period, while the top bars (pink) show countries that have historically used a censor method (but not as of 2021).

In total, 62 of the 70 surveyed nations had some evidence of Internet censorship, during the study period or as shown in historical documentation. The most popular censorship method was application layer filtering of HTTP content or URLs — over all-time as well as during the study period. BGP disruptions were the least utilized method both during the study period and over all-time.

Unfortunately, we also observed a large percentage of nations (41%) leveraging TLS-based filtering capabilities against HTTPS traffic. This trend likely occurs because of the widespread adoption of TLS encryption. Encrypting HTTP traffic denies censors' ability to filter based on the network packet content. Mozilla's telemetry reporting shows 82% of global traffic is HTTPS as of October 2021 [54], and adoption

[5] We did not report unconfirmed censor activity in any totals, discussion, or figures other than the framework in Table 1 and associated citations in Table 3.

Table 1: Framework for Evidence of Internet Censorship Methods by Country

● = observed, persistent censorship
○ = observed, time-based censorship
▼ = historical censor observations
□ = unconfirmed

Study period for ●/○: June 01, 2020 to May 31, 2021

COUNTRY	ISO 3166-1 Country Code	FOTN 2021 Total Score	Obstacles to Access	Limits on Content	Violations of User Rights	FOTN 2021 Status	Internet Shutdowns	IP Address or Port Blocking	BGP Attacks and Disruption	Bandwidth Throttling	DNS Tampering	HTTP/URL/Keyword Filtering	TLS-based Filtering	Protocol Fingerprinting	Notes
China	CN	10	8	2	0	Not Free	○	○●		▼	●	●	●	●	Centralized active blocking of VPNs, circumvention tools, and secure messengers
Iran	IR	16	8	5	3	Not Free	○	○●*		▼	●	●	●	●	*Particular endpoints associated with QUIC/UDP targets, and residual censorship
Myanmar (Burma)	MM	17	4	7	6	Not Free	○	●	●	○	●	▼			Military junta coup d'état after 2020 elections
Cuba	CU	21	5	9	7	Not Free	○					●	●	▼	Mass anti-government protests of COVID-19 pandemic response, censored social media
Vietnam	VN	22	12	6	4	Not Free					▼	▼			Censorship focus in print media
Saudi Arabia	SA	24	12	8	4	Not Free		▼			▼	●	●		Reduced overall Internet filtering between 2017-2020
Pakistan	PK	25	5	13	7	Not Free	○	▼	▼*		▼	●	●		*Global YouTube disruption via BGP 24FEB2008
Egypt	EG	26	12	10	4	Not Free	○	●			●	●	●	●	
Ethiopia	ET	27	4	12	11	Not Free	○	▼				●	▼	▼	Tigray civil war
United Arab Emirates	AE	27	12	9	6	Not Free					●	●	●	▼	
Uzbekistan	UZ	28	9	12	7	Not Free	○					●	●		
Venezuela	VE	28	6	12	10	Not Free					▼	●	●		
Bahrain	BH	30	16	8	6	Not Free					▼	●	●		
Russia	RU	30	12	10	8	Not Free	○	●	▼	○	●	●	○●	●	Decentralized, novel hybrid censor approaches observed
Belarus	BY	31	10	14	7	Not Free	○	▼			●	●	●		
Kazakhstan	KZ	33	11	11	11	Not Free	○	○●		▼	▼	●	●	▼	Nation-wide deployment of government-issued root certificate, MITM interception 2019
Sudan	SD	33	6	15	12	Not Free	○					▼			
Turkey	TR	34	15	10	9	Not Free	▼	▼	▼*	▼	●	●	●		*Global Internet disruption via BGP routes to Turkey 24DEC2004
Azerbaijan	AZ	35	10	14	11	Not Free	○	▼				●	●		Second Nagorno-Karabakh war, late 2020
Thailand	TH	36	16	13	7	Not Free					▼	●			High levels of inconsistency in routing, content mismatches
Rwanda	RW	38	13	11	14	Not Free						▼			
Bangladesh	BD	40	12	17	11	Partly Free	○			▼		●	●		
Iraq	IQ	41	11	16	14	Partly Free	○				▼				
Cambodia	KH	43	13	18	12	Partly Free						●	●		
Zimbabwe	ZW	46	8	22	16	Partly Free	▼					▼			
Jordan	JO	47	13	17	17	Partly Free		▼		○*	●	●	●		*Throttling of a social media service during public protests
Indonesia	ID	48	14	17	17	Partly Free					▼	●	●		
Libya	LY	48	7	25	16	Partly Free	▼		▼						
Nicaragua	NI	48	12	18	18	Partly Free						●	●		
India	IN	49	11	21	17	Partly Free	○	▼		○	●	●	●		89 Internet shutdowns during the measurement period
Uganda	UG	49	11	19	19	Partly Free	○	▼				●	□*		2021 elections - shutdowns and social media; *Potential DPI censorship from AS21491
Lebanon	LB	51	11	22	18	Partly Free						□*			*Limited data available
Sri Lanka	LK	51	11	23	17	Partly Free	○								
Kyrgyzstan	KG	53	13	23	17	Partly Free						▼			Inconclusive for evidence of URL filtering during study period
Morocco	MA	53	15	22	16	Partly Free					▼				
The Gambia	GM	53	12	22	19	Partly Free	▼					□			Internet freedom improvement since 2017
Singapore	SG	54	19	17	18	Partly Free					●	□			
Malaysia	MY	58	18	21	19	Partly Free	▼				●	▼			
Malawi	MW	59	11	25	23	Partly Free	□*					□**			*2019 elections; **2011 alleged short-term blocking of news and social media
Nigeria	NG	59	17	25	17	Partly Free	○	▼			▼	▼			
Zambia	ZM	59	15	24	20	Partly Free	▼					▼	▼		2021 elections, social media platform blocking (outside study period)
Mexico	MX	60	18	25	17	Partly Free		▼*				●	●**		*Blocking of Tor directory authorities; **state-owned AS8151 TLS-based filtering
Angola	AO	62	12	30	20	Partly Free							●*		*Blocking of anti-censorship software websites
Ecuador	EC	62	17	25	20	Partly Free						●	●		
Ukraine	UA	62	20	21	21	Partly Free					●	●	●		
Tunisia	TN	63	16	28	19	Partly Free		▼				▼			
Brazil	BR	64	20	24	20	Partly Free					▼	▼			
Ghana	GH	64	14	27	23	Partly Free						●	●		
Colombia	CO	65	19	25	21	Partly Free	□*					▼			*Potential shutdown in parallel with anti-government protests
Philippines	PH	65	17	26	22	Partly Free	▼*					●		▼	*Cellular telephony service shutdowns
Kenya	KE	66	16	27	23	Partly Free									Government orders for removal of content in leu of blocking actions
South Korea	KR	67	22	24	21	Partly Free		▼	▼		▼	●	●		Authorities have publicized their use of TLS-based filtering for illegal content
Hungary	HU	70	21	24	25	Free						□*	□*		*AS60436 potentially performing filtering actions
Argentina	AR	71	19	27	25	Free					▼				
Armenia	AM	71	19	26	26	Free	●					●	●		Second Nagorno-Karabakh war, late 2020
Serbia	RS	71	21	25	25	Free						▼*			*State blocking of gambling websites
South Africa	ZA	73	17	29	27	Free									
Australia	AT	75	23	27	25	Free			▼			□			State blocks gambling, torrent, and streaming sites
United States	US	75	21	29	25	Free									Law Enforcement compels the removal of intellectual property theft rather than blocking
Italy	IT	76	21	30	25	Free					●*				*Mostly blocking alleged criminal activity or copyright infringement
Japan	JP	76	21	29	26	Free									
Georgia	GE	77	19	31	27	Free						□*			*Temporary blocking of "pro-Islamic State" websites 2015
France	FI	78	23	30	25	Free					●	●			State blocking of websites related to "terrorism" and copyright infringement
United Kingdom	GB	78	23	30	25	Free	▼	▼				●	●		IWF maintains court-ordered blocklist ("extreme pornography" and copyright infringement)
Germany	DE	79	22	29	28	Free					▼	▼			Repeal of the Access Impediment Law (Zugangserschwerungsgesetz) 2011
Taiwan	TW	80	24	31	25	Free						□*			*City of Taipei filters select websites on its public wifi
Canada	CA	87	23	32	32	Free		▼	▼		●	●			State blocking of copyright infringement
Costa Rica	CR	87	20	33	34	Free									
Estonia	EE	94	25	32	37	Free					●*				*State blocking of gambling websites
Iceland	IS	96	25	34	37	Free					□*				*State blocking of copyright infringement

Table 2: Percentage of Countries that Use Each Internet Censorship Method in the Framework

Censor Method	% During Study Period	% All-Time
Internet Shutdowns	29	40
IP or Port Blocking	9	30
BGP Attacks/Disruption	1	11
Bandwidth Throttling	6	13
DNS Tampering	24	46
HTTP/URL/Keyword Filtering	49	69
TLS-based Filtering	41	44
Protocol Fingerprinting	6	13

has only increased since then. Given this dilemma, censors with higher motivation have invested in hardware and software capable of targeting SNI in TLS headers of HTTPS requests.

Oddly enough, HTTP-based censorship remains the most utilized censor method (49%), despite the proliferation of TLS. This suggests that some censors are satisfied to sponsor content-based censorship regimes, despite being ineffective against most web traffic. Some of these governments may not have agencies or individuals that understand the technology thoroughly enough to make informed decisions about updating their censorship architecture. There is also the unfortunate reality that some parts of the world are underserved by HTTPS compared to more developed nations [83], and older censor methods may continue to work in these countries until system administrators update their web servers.

Some censor methods are reflected as mostly historic. IP and port blocking occurred frequently in the past (30%) but seldom during the study period (9%, or six countries). These will be discussed further in §4.3. BGP disruptions were also infrequent — likely because of the nature of manipulation of BGP announcements, which impact Internet routing far beyond a nation's borders. Two famous examples of malicious actions by nation-states illustrate BGP-based censorship attempts [115, 134], and both were short-lived.

4.3 Discussion

Global Internet censorship has generally increased over the years, with a handful of nations as exceptions. In documenting the technical means by which these countries deny access to Internet resources, we illuminated several trends to inform future research.

DPI technologies have long been assumed to be too resource intensive to implement at a national scale. Our data indicates otherwise; an increasing number of countries are willing and able to filter application-layer content. The most aggressive censors utilize hybrid approaches (Russia) [190], active probing of VPN and anti-censorship services (China) [55, 120], and allowlisting prior to censorship-in-depth (Iran) [28]. We also highlight the overall increased use of TLS-based blocking, often when a censor targets the unencrypted SNI to deny access to particular domains. This entire class of censorship techniques could potentially be eliminated with the upgrade to Encrypted Client Hellos (ECH) — which is still in IETF draft [149]. Encrypted SNI (ESNI) was an earlier attempt to address privacy concerns of SNI targeting, but faced implementation issues and was only supported by one major web browser, Mozilla Firefox [136]. PRC also took the unprecedented step of blocking most ESNI traffic [26]. Firefox has since abandoned ESNI in favor of supporting ECH development [88]; ECH will need to be widely deployed to ensure the cost of overblocking deters authorities from blocking the newest version of TLS.

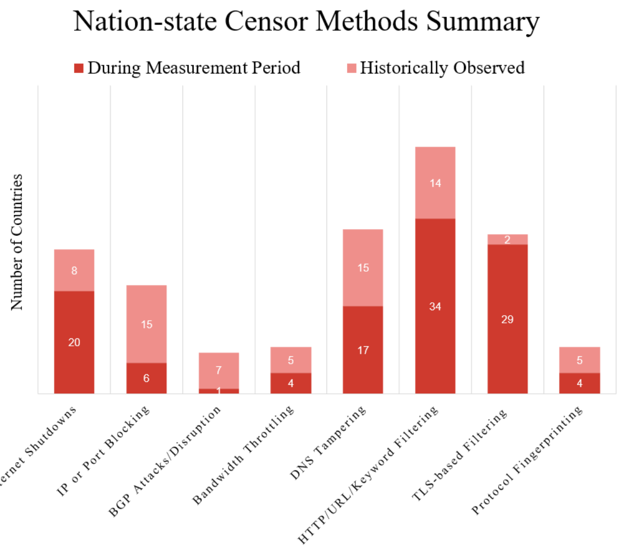

Figure 1: Bottom bars indicate countries that censored using a given method during the measurement period; Top bars indicate historical evidence of censorship (but not during the measurement period).

As end-to-end encrypted (E2EE) messaging services gain popularity for their security and privacy properties, censoring nation-states have targeted these protocols with existing methods as well as more advanced protocol fingerprinting techniques. The proliferation of encrypted traffic analysis (ETA) tools or next-generation firewalls (NGFWs) that can block applications such as Signal or Tor Browser may pose a threat to freedom of expression if implemented by a censor. Notably, all evidence of censorship in the protocol fingerprinting category came from focused individual studies, not from the primary data sources in §3.

More targeted censorship methods enable regimes to meet their censorship goals while avoiding overblocking, minimizing economic collateral damage. Censors may also use sophisticated methods because they are more subtle, and deniability that censorship is occurring may avoid the political implications of public outcry. At the same time, countries in other parts of the world are increasingly willing to use blunt instruments of censorship — often total Internet shutdowns — during tumultuous periods of civil unrest or political change.

We also observed that nations typically understudied in terms of Internet censorship have some level of filtering happening within their borders. Several countries (e.g., Italy, France, Estonia, Iceland) use DNS tampering to block content considered illegal (e.g., intellectual property theft, gambling, pornography, terrorism, child sexual abuse materials) in their society. Some surprising Western examples included when Canada blocked COVID-19 information [176] and when police in the United Kingdom turned off WiFi in subway systems during environmental activism protests [175].

There are several positive trends for Internet freedom advocates in our data. We observed a decline in the use of naive methods such as IP blocklists. This is possibly the case for several reasons: (1) difficulty in maintaining blocklists, as IP addresses are often ephemeral, (2) collateral damage, as blocking an IP range belonging to a CDN can deny access to large swaths of the Internet, and (3) as IPv6 is more widely deployed, the total IP address space grows exponentially. This observation could be partially distorted based on bias in the literature as outlined in §3. However, in our study we rarely observed port blocking in use for censorship. Typical web traffic occurs on ports 443, 80, and 53, and applications using other ports are not necessarily required to follow standard conventions when hosting their services. Iran is a notable exception in that it has implemented allowlisting for the three ports mentioned above on several occasions, denying access to all others [28]. Another recent study highlighted "residual censorship," where censors detect an objectionable connection using one censorship method, then proceed to deny all connections between the two endpoints for a short duration using a 3-tuple (client IP + server IP + port) or 4-tuple (client IP + port + server IP + port) [27]. Bock et al. observed this renewed, time-based approach to IP and port blocking in China, Iran, and Kazakhstan; further research is needed to determine if other nation-states are implementing similar functionality into their censorship systems.

Application layer filtering, specifically HTTP content and URL blocking, has also seen a decline in effectiveness. The broad adoption of encryption via TLS limits a censor's ability to analyze and target packet contents. DNS tampering occurs less often than HTTP-based application layer filtering, and several circumvention techniques remain available for DNS-based censorship: (1) changing the DNS server a user device submits requests to, (2) using encrypted DNS protocols, such as DNS over TLS or DNS over HTTPS, (3) using web proxies that support DNS traffic, such as SOCKS5, (4) using VPNs and tunnel-based anti-censorship tools. Detection and documentation of censors that block DoT/DoH and QUIC endpoints [20, 52] are also points of serious consideration for Internet measurement researchers.

5 Future Directions

In addition to being a valuable tool for investigating and tracking global censorship trends, our analysis and the resulting framework point to several interesting and open research directions. Our framework helps highlight gaps in existing work, both from a country-specific and a technical perspective, and can serve as a well-informed springboard for future studies.

We report several anecdotal instances of censor activity (e.g., social media, blog posts) in multiple countries that lack quantitative evidence or scientific studies to corroborate. Some of these nations present little evidence of censorship in available Internet measurement datasets; this may point to areas currently under-studied or that would benefit from further research. Are these true censorship events or isolated instances resulting from external circumstances? Have these countries shown repeated instances of censor activity but received less attention because they are not part of the often-studied country sets? What political or social circumstances may lead to future censorship trends in these countries?

While prior work has explored censorship methods based on geographical regions, deeper analysis of the global dataset prompted us to ask: Are there different ways to group countries and datasets that may lead to valuable insights? For example, we wonder if there are notable similarities or trends among politically allied nations. Do allied countries influence each others' likelihood of censor activity, censorship methods, pace of deployment of their censorship apparatus, or content filtered, to name a few? What other international factors might influence a nation's censorship activities?

We believe this is an important area of future work because it benefits censored citizens and policymakers supportive of free expression online. Comprehensively understanding *how* censorship happens is a crucial first step towards change. The global nature of our methodology and framework allows one to better ask (and answer) broader questions of research relevance towards Internet governance.

6 Conclusion

Understanding global trends in Internet censorship can empower researchers, policymakers, and civil liberty advocates. While substantial prior work focuses on single-nation or regional censorship, we sought to expand this perspective by providing a worldwide view of Internet censorship methods over time. To do this, we developed a comprehensive framework that is approachable and flexible — it allows for easy visual investigation, further quantitative analysis, and straightforward updates as new findings emerge. We conducted a cross-sectional study over a one-year period and a historical 20-year survey of 70 countries within the framework. This allowed us to provide unique, data-driven insights into global Internet censorship trends and point out interesting directions for future research.

Acknowledgments

We would like to express our gratitude to the research groups whose tireless efforts have made censorship data available over the past decade, specifically OONI, Censored Planet, Freedom House, Access Denied, and Internet Society. Without your tireless efforts this work would not have been possible. We would also like to thank the anonymous reviewers for their detailed and helpful feedback that improved the quality of this paper.

Availability

The framework documents and all datasets used in this study are publicly available at https://doi.org/10.5281/zenodo.8040694.

References

[1] Giuseppe Aceto, Alessio Botta, Antonio Pescapè, M. Faheem Awan, Tahir Ahmad, and Saad Qaisar. Analyzing Internet Censorship in Pakistan. In *Research and Technologies for Society and Industry*. IEEE, 2016. URL: https://doi.org/10.1109/RTSI.2016.7740626.

[2] Giuseppe Aceto, Alessio Botta, Antonio Pescapè, Nick Feamster, M. Faheem Awan, Tahir Ahmad, and Saad Qaisar. Monitoring Internet Censorship with UBICA. In *Traffic Monitoring and Analysis*. Springer, 2015. URL: http://wpage.unina.it/giuseppe.aceto/pub/aceto2015monitoring_TMA.pdf.

[3] Giuseppe Aceto and Antonio Pescapé. Internet Censorship detection: A survey. *Computer Networks*, 83:381–421, June 2015. URL: https://linkinghub.elsevier.com/retrieve/pii/S1389128615000948, doi:10.1016/j.comnet.2015.03.008.

[4] Sadia Afroz and David Fifield. Timeline of Tor Censorship. URL: http://www1.icsi.berkeley.edu/~sadia/tor_timeline.pdf.

[5] Mustafa Akgül and Melih Kırlıdoğ. Internet censorship in Turkey. *Internet Policy Review*, 4(2), June 2015. URL: https://policyreview.info/node/366, doi:10.14763/2015.2.366.

[6] Khalid M Al-Tawil. The Internet in Saudi Arabia. *Telecommunications Policy*, 25(8-9):625–632, September 2001. URL: https://linkinghub.elsevier.com/retrieve/pii/S0308596101000362, doi:10.1016/S0308-5961(01)00036-2.

[7] Sodiq Alabi. President Buhari's Secret War on Free Speech, November 2017. URL: https://paradigmhq.org/president-buharis-secret-war-on-free-speech/.

[8] Fatemah Alharbi, Michalis Faloutsos, and Nael Abu-Ghazaleh. Opening Digital Borders Cautiously yet Decisively: Digital Filtering in Saudi Arabia. *USENIX Workshop on Free and Open Communications on the Internet*, 2020. URL: https://www.usenix.org/system/files/foci20-paper-alharbi_0.pdf.

[9] Collin Anderson. The Hidden Internet of Iran: Private Address Allocations on a National Network. Technical Report, Technical Report, 2012. URL: https://arxiv.org/pdf/1209.6398v1.pdf.

[10] Collin Anderson. Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran. Technical Report arXiv:1306.4361, Technical Report, University of Pennsylvania, Philadelphia, PA, June 2013. arXiv:1306.4361 [cs]. URL: http://arxiv.org/abs/1306.4361.

[11] Collin Anderson, Philipp Winter, and Roya. Global Network Interference Detection over the RIPE Atlas Network. In *Free and Open Communications on the Internet*. USENIX, 2014. URL: https://www.usenix.org/system/files/conference/foci14/foci14-anderson.pdf.

[12] Anonymous. The collateral damage of internet censorship by DNS injection. *ACM SIGCOMM Computer Communication Review*, 42(3):21–27, June 2012. URL: https://dl.acm.org/doi/10.1145/2317307.2317311, doi:10.1145/2317307.2317311.

[13] Anonymous. Towards a Comprehensive Picture of the Great Firewall's DNS Censorship. In *Free and Open Communications on the Internet*. USENIX, 2014. URL: https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf.

[14] Simurgh Aryan, Homa Aryan, and J Alex Halderman. Internet Censorship in Iran: A First Look. *Proceedings of Free and Open Communications on the Internet (FOCI)*, 2013. URL: https://www.usenix.org/system/files/conference/foci13/foci13-aryan.pdf.

[15] Muhammed S. Bah. Gambia: Are Social Networking Applications Blocked?, August 2016. URL: https://allafrica.com/stories/201608240945.html.

[16] David Bamman, Brendan O'Connor, and Noah Smith. Censorship and deletion practices

in Chinese social media. *First Monday*, 17, March 2012. URL: https://journals.uic.edu/ojs/index.php/fm/article/view/3943, doi:10.5210/fm.v17i3.3943.

[17] Guy Baron and Gareth Hall. Access Online: Internet Governance and Image in Cuba. *Bulletin of Latin American Research*, 34(3), July 2015. URL: https://onlinelibrary.wiley.com/doi/10.1111/blar.12263, doi:10.1111/blar.12263.

[18] Thomas A. Bass. *Censorship in Vietnam: brave new world*. University of Massachusetts Press, Amherst, 2017.

[19] Simone Basso. DNS over TLS blocked in Iran, June 2020. URL: https://ooni.org/post/2020-iran-dot/.

[20] Simone Basso. Measuring DoT/DoH blocking using OONI Probe: a preliminary study. In *Network and Distributed System Security (NDSS) Symposium*. NDSS, 2021. URL: https://www.ndss-symposium.org/wp-content/uploads/dnspriv21-02-paper.pdf.

[21] Ralf Bendrath and Milton Mueller. The end of the net as we know it? Deep packet inspection and internet governance. *New Media & Society*, 13(7):1142–1160, November 2011. URL: http://journals.sagepub.com/doi/10.1177/1461444811398031, doi:10.1177/1461444811398031.

[22] Karyn Benson, Alberto Dainotti, K. C. Claffy, and Emile Aben. Gaining Insight into AS-level Outages through Analysis of Internet Background Radiation. In *Traffic Monitoring and Analysis*. IEEE, 2013. URL: https://cseweb.ucsd.edu/~kbenson/papers/tma13.pdf.

[23] Mehrab Bin Morshed, Michaelanne Dye, Syed Ishtiaque Ahmed, and Neha Kumar. When the Internet Goes Down in Bangladesh. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 1591–1604, Portland Oregon USA, February 2017. ACM. URL: https://dl.acm.org/doi/10.1145/2998181.2998237, doi:10.1145/2998181.2998237.

[24] Constance Bitso, Ina Fourie, and Theo J D Bothma. Trends in transition from classical censorship to Internet censorship: selected country overviews. *Innovation : journal of appropriate librarianship and information work in Southern Africa*, 2013. URL: https://journals.co.za/doi/abs/10.10520/EJC148135.

[25] Tax and Customs Board. Blokeeritud hasartmängu internetileheküljed ["Blocked gambling websites"], June 2020. URL: https://web.archive.org/web/20201204203801/https://www.emta.ee/et/eraklient/maa-soiduk-mets-hasartmang/blokeeritud-hasartmangu-internetilehekuljed.

[26] Kevin Bock, Anonymous, Louis-Henri Merino, David Fifield, Amir Houmansadr, and Dave Levin. Exposing and Circumventing China's Censorship of ESNI, August 2020. URL: https://gfw.report/blog/gfw_esni_blocking/en/.

[27] Kevin Bock, Pranav Bharadwaj, Jasraj Singh, and Dave Levin. Your Censor is My Censor: Weaponizing Censorship Infrastructure for Availability Attacks. In *2021 IEEE Security and Privacy Workshops (SPW)*, pages 398–409, San Francisco, CA, USA, May 2021. IEEE. doi:10.1109/SPW53761.2021.00059.

[28] Kevin Bock, Yair Fax, Kyle Reese, Jasraj Singh, and Dave Levin. Detecting and Evading Censorship-in-Depth: A Case Study of Iran's Protocol Filter. *Free and Open Communications on the Internet (FOCI)*, 2020. URL: https://www.usenix.org/system/files/foci20-paper-bock.pdf.

[29] Kevin Bock, Gabriel Naval, Kyle Reese, and Dave Levin. Even Censors Have a Backup: Examining China's Double HTTPS Censorship Middleboxes. In *Free and Open Communications on the Internet*. ACM, 2021. URL: https://doi.org/10.1145/3473604.3474559.

[30] Yana Breindl and Joss Wright. Internet Filtering Trends in Western Liberal Democracies: French and German Regulatory Debates. *USENIX Workshop on Free and Open Communications on the Internet*, 2012. URL: https://www.usenix.org/system/files/conference/foci12/breindl2012foci.pdf.

[31] Davide Brunello, Arturo Filastò, Maria Xynou, and Simone Basso. Italy blocks Gutenberg book publishing website, September 2021. URL: https://ooni.org/post/2021-italy-blocks-gutenberg-book-publishing-website/.

[32] Tomasz Bujlow, Valentín Carela-Español, and Pere Barlet-Ros. Independent comparison of popular DPI tools for traffic classification. *Computer Networks*, 76:75–89, January 2015. URL: https://linkinghub.elsevier.com/retrieve/pii/S1389128614003909, doi:10.1016/j.comnet.2014.11.001.

[33] Baboucarr Ceesay. Gambia: Government's internet phobia and censorship, March 2014. URL: https://web.archive.org/web/20171123161754/

africareview.com/News/Gambia-Government-Internet-phobia-and-censorship-/-/979180/2261770/-/3uqtqtz/-/index.html.

[34] Abdelberi Chaabane, Terence Chen, Mathieu Cunche, Emiliano De Cristofaro, Arik Friedman, and Mohamed Ali Kaafar. Censorship in the Wild: Analyzing Internet Filtering in Syria. In *Internet Measurement Conference*, Vancouver BC Canada, 2014. ACM. URL: https://dl.acm.org/doi/10.1145/2663716.2663720, doi:10.1145/2663716.2663720.

[35] Zimo Chai, Amirhossein Ghafari, and Amir Houmansadr. On the Importance of Encrypted-SNI (ESNI) to Censorship Circumvention. In *Free and Open Communications on the Internet*. USENIX, 2019. URL: https://www.usenix.org/system/files/foci19-paper_chai_update.pdf.

[36] Mariengracia Chirinos, Andrés Azpúrua, Leonid Evdokimov, and Maria Xynou. The State of Internet Censorship in Venezuela, August 2018. URL: https://ooni.org/post/venezuela-internet-censorship/.

[37] Shinyoung Cho, Rishab Nithyanand, Abbas Razaghpanah, and Phillipa Gill. A Churn for the Better: Localizing Censorship using Network-level Path Churn and Network Tomography. In *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*. ACM, 2017. URL: https://doi.org/10.1145/3143361.3143386.

[38] Catalin Cimpanu. KlaySwap crypto users lose funds after BGP hijack, February 2022. URL: https://therecord.media/klayswap-crypto-users-lose-funds-after-bgp-hijack/.

[39] Richard Clayton. Failures in a Hybrid Content Blocking System. In *Privacy Enhancing Technologies*, pages 78–92. Springer, 2006. URL: https://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf.

[40] Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson. Ignoring the Great Firewall of China. In *Privacy Enhancing Technologies*, volume 4258, pages 20–35. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006. Series Title: Lecture Notes in Computer Science. URL: http://link.springer.com/10.1007/11957454_2, doi:10.1007/11957454_2.

[41] The Korea Communications Commission. Press Release, 2019.

[42] Jedidiah R. Crandall, Daniel Zinn, Michael Byrd, Earl Barr, and Rich East. ConceptDoppler: A Weather Tracker for Internet Censorship. In *Computer and Communications Security*, pages 352–365. ACM, 2007. URL: http://www.csd.uoc.gr/~hy558/papers/conceptdoppler.pdf.

[43] Alberto Dainotti, Claudio Squarcella, Emile Aben, Kimberly C. Claffy, Marco Chiesa, Michele Russo, and Antonio Pescapè. Analysis of Country-wide Internet Outages Caused by Censorship. In *Internet Measurement Conference*, pages 1–18. ACM, 2011. URL: http://conferences.sigcomm.org/imc/2011/docs/p1.pdf.

[44] Jakub Dalek, Bennett Haselton, Helmi Noman, Adam Senft, Masashi Crete-Nishihata, Phillipa Gill, and Ronald J. Deibert. A method for identifying and confirming the use of URL filtering products for censorship. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 23–30, Barcelona Spain, October 2013. ACM. URL: https://dl.acm.org/doi/10.1145/2504730.2504763, doi:10.1145/2504730.2504763.

[45] Jakub Dalek and Adam Senfit. Behind Blue Coat: Investigations of commercial filtering in Syria and Burma, November 2011. URL: https://citizenlab.ca/2011/11/behind-blue-coat/.

[46] Shepardson David. Censorship circumvention tool helps 1.4 million Cubans get internet access, July 2021. URL: https://www.reuters.com/world/americas/censorship-circumvention-tool-helps-14-million-cubans-get-internet-access-2021-07-16/.

[47] Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, and Janice Stein. *Access Denied: The Practice and Policy of Global Internet Filtering*. Project MUSE: Information Revolution and Global Politics. The MIT Press, 2008. URL: https://muse.jhu.edu/book/60844.

[48] Ronald Deibert, Jonathan Zittrain, Rafal Rohozinski, and John Palfrey, editors. *Access contested: security, identity, and resistance in Asian cyberspace information revolution and global politics*. Information revolution and global politics. MIT Press, Cambridge, MA, 2012.

[49] Lucas Dixon, Thomas Ristenpart, and Thomas Shrimpton. Network Traffic Obfuscation and Automated Internet Censorship. *IEEE Security & Privacy*, 14(6):43–53, November 2016. URL: http://ieeexplore.ieee.org/document/7782699/, doi:10.1109/MSP.2016.121.

[50] Ayhan Dolunay, Fevzi Kasap, and Gökçe Keçeci. Freedom of Mass Communication in the Digital Age in the Case of the Internet: "Freedom House" and the USA Example. *Sustainability*, 9(10):1739, October 2017. URL: http://www.mdpi.com/2071-1050/9/10/1739, doi:10.3390/su9101739.

[51] Maximillian Dornseif. Government mandated blocking of foreign Web content. In *DFN-Arbeitstagung über Kommunikationsnetze*, pages 617–647. Gesellschaft für Informatik, 2003. URL: https://censorbib.nymity.ch/pdf/Dornseif2003a.pdf.

[52] Kathrin Elmenhorst, Bertram Schütz, Nils Aschenbruck, and Simone Basso. Web censorship measurements of HTTP/3 over QUIC. In *Proceedings of the 21st ACM Internet Measurement Conference*, pages 276–282, Virtual Event, November 2021. ACM. URL: https://dl.acm.org/doi/10.1145/3487552.3487836, doi:10.1145/3487552.3487836.

[53] Paul Emmanuel. These African countries have various forms of Internet censorship, May 2020. URL: https://techpoint.africa/2020/05/21/african-countries-censor-internet/.

[54] Let's Encrypt. Let's Encrypt Statistics, October 2021. URL: https://letsencrypt.org/stats/.

[55] Roya Ensafi, David Fifield, Philipp Winter, Nick Feamster, Nicholas Weaver, and Vern Paxson. Examining How the Great Firewall Discovers Hidden Circumvention Servers. In *Proceedings of the 2015 Internet Measurement Conference*, pages 445–458, Tokyo Japan, October 2015. ACM. URL: https://dl.acm.org/doi/10.1145/2815675.2815690, doi:10.1145/2815675.2815690.

[56] Roya Ensafi, Philipp Winter, Abdullah Mueen, and Jedidiah R. Crandall. Analyzing the Great Firewall of China Over Space and Time. *Proceedings on Privacy Enhancing Technologies*, 2015(1):61–76, April 2015. URL: https://www.sciendo.com/article/10.1515/popets-2015-0005, doi:10.1515/popets-2015-0005.

[57] Steven Feldstein. *The rise of digital repression: how technology is reshaping power, politics, and resistance*. Carnegie Endowment for International Peace. Oxford University Press, New York, NY, 2021. OCLC: on1206228409.

[58] Arturo Filastò and Jacob Appelbaum. OONI: Open Observatory of Network Interference. In *Free and Open Communications on the Internet*. USENIX, 2012. URL: https://www.usenix.org/system/files/conference/foci12/foci12-final12.pdf.

[59] Arturo Filastò, Arthur Gwagwa, and Maria Xynou. The Gambia: Internet Shutdown during 2016 Presidential Election, December 2016. URL: https://ooni.org/post/gambia-internet-shutdown/.

[60] Terry Fletcher and Andria Hayes-Birchler. Comparing Measures of Internet Censorship: Analyzing the Tradeoffs between Expert Analysis and Remote Measurement. *Data For Policy 2020*, July 2020. Publisher: Zenodo. URL: https://zenodo.org/record/3967397, doi:10.5281/ZENODO.3967397.

[61] Andrea Di Florio, Nino Vincenzo Verde, Antonio Villani, Domenico Vitali, and Luigi Vincenzo Mancini. Bypassing Censorship: A Proven Tool against the Recent Internet Censorship in Turkey. In *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, pages 389–394, Naples, Italy, November 2014. IEEE. URL: https://ieeexplore.ieee.org/document/6983872, doi:10.1109/ISSREW.2014.93.

[62] Iginio Gagliardone and Frederick Golooba-Mutebi. The Evolution of the Internet in Ethiopia and Rwanda: Towards a "Developmental" Model? *Stability: International Journal of Security and Development*, 5(1):8, August 2016. URL: http://www.stabilityjournal.org/articles/10.5334/sta.344/, doi:10.5334/sta.344.

[63] Genevieve Gebhart and Tadayoshi Kohno. Internet Censorship in Thailand: User Practices and Potential Threats. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 417–432, Paris, April 2017. IEEE. URL: https://ieeexplore.ieee.org/document/7961994/, doi:10.1109/EuroSP.2017.50.

[64] Arzu Geybullayeva, Maria Xynou, and Arturo Filastò. Media censorship in Azerbaijan through the lens of network measurement, July 2021. URL: https://ooni.org/post/2021-azerbaijan/.

[65] Phillipa Gill, Masashi Crete-Nishihata, Jakub Dalek, Sharon Goldberg, Adam Senft, and Greg Wiseman. Characterizing Web Censorship Worldwide: Another Look at the OpenNet Initiative Data. *ACM Transactions on the Web*, 9(1), 2015. Publisher: ACM. URL: https://censorbib.nymity.ch/pdf/Gill2015a.pdf.

[66] Devashish Gosain, Anshika Agarwal, Sahil Shekhawat, H. B. Acharya, and S. Chakravarty. Mending Wall: On the Implementation of Censorship in India. *arXiv:1806.06518 [cs]*, June 2018. arXiv: 1806.06518. URL: http://arxiv.org/abs/1806.06518.

[67] Calipr Networking Group. ICLab Data, November 2021. URL: https://iclab.gitlab.io/post/iclab_data/.

[68] Gurshabad Grover and Kushagra Singh. Reliance Jio is using SNI inspection to block websites, November 2019. URL: https://cis-india.org/internet-governance/blog/reliance-jio-is-using-sni-inspection-to-block-websites.

[69] Brynjólfur Þór Guðmundsson. Gangi ekki upp nema of langt sé gengið [Doesn't work unless you go too far], September 2015. Discussion of DNS-blocking copyright infringing materal. URL: https://www.ruv.is/frettir/innlent/gangi-ekki-upp-nema-of-langt-se-gengid.

[70] Ming-Syuan Ho. Taiwan Internet Transparency Report. Technical report, Taiwan Association for Human Rights, Taiwan, 2018. URL: http://transparency.tahr.org.tw/TITR_Report_2018_en.pdf.

[71] Nguyen Phong Hoang, Arian Akhavan Niaki, Jakub Dalek, Jeffrey Knockel, Pellaeon Lin, Bill Marczak, Masashi Crete-Nishihata, Phillipa Gill, and Michalis Polychronakis. How Great is the Great Firewall? Measuring China's DNS Censorship. Technical report, New York University, Technical Report, New York University, 2007. URL: https://www.usenix.org/system/files/sec21-hoang.pdf.

[72] John Holowczak and Amir Houmansadr. CacheBrowser: Bypassing Chinese Censorship without Proxies Using Cached Content. In *Computer and Communications Security*. ACM, 2015. URL: https://people.cs.umass.edu/~amir/papers/CacheBrowser.pdf.

[73] Freedom House. Freedom on the Net - Annual Report. URL: https://freedomhouse.org/report/freedom-net.

[74] Freedom House. Freedom on the Net 2021 - China. URL: https://freedomhouse.org/country/china/freedom-net/2021.

[75] Freedom House. Freedom on the Net 2021 - Canada, 2021. URL: https://freedomhouse.org/country/canada/freedom-net/2021.

[76] Freedom House. Freedom on the Net 2021 - Germany, 2021. URL: https://freedomhouse.org/country/germany/freedom-net/2021.

[77] Freedom House. Freedom on the Net 2021 - Kenya, 2021. URL: https://freedomhouse.org/country/kenya/freedom-net/2021.

[78] Freedom House. Freedom on the Net 2021 - Russia, 2021. URL: https://freedomhouse.org/country/russia/freedom-net/2021.

[79] Freedom House. Freedom on the Net 2021 - Singapore, 2021. URL: https://freedomhouse.org/country/singapore/freedom-net/2021.

[80] Freedom House. Freedom on the Net 2021 - The Gambia, 2021. URL: https://freedomhouse.org/country/gambia/freedom-net/2021.

[81] Freedom House. Freedom on the Net 2021 - United Kingdom, 2021. URL: https://freedomhouse.org/country/united-kingdom/freedom-net/2021.

[82] Freedom House. Freedom on the Net 2021 - Venezuela, 2021. URL: https://freedomhouse.org/country/venezuela/freedom-net/2021.

[83] Troy Hunt and Scott Helme. Why No HTTPS?, August 2021. URL: https://whynohttps.com/.

[84] Singapore IMDA. Internet Regulatory Framework, December 2020. URL: https://web.archive.org/web/20220925231358/https://www.imda.gov.sg/regulations-and-licensing-listing/content-standards-and-classification/standards-and-classification/internet.

[85] OpenNet Initiative. Country profile: Kazakhstan, 2010. URL: https://opennet.net/research/profiles/kazakhstan.

[86] OpenNet Initiative. Internet Filtering in China. Technical report, OpenNet Initiative, Technical Report, 2009. URL: http://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf.

[87] Gunnar Eyal Wolf Iszaevich. Distributed Detection of Tor Directory Authorities Censorship in Mexico. In *International Conference on Networks*. IARIA, 2019. URL: https://tics.site/proceedings/2019a/icn_2019_6_20_38010.pdf.

[88] Kevin Jacobs. Encrypted Client Hello: the future of ESNI in Firefox, January 2021. URL: https://blog.mozilla.org/security/2021/01/07/encrypted-client-hello-the-future-of-esni-in-firefox/.

[89] Lin Jin, Shuai Hao, Haining Wang, and Chase Cotton. Understanding the Practices of Global Censorship through Accurate, End-to-End Measurements. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 5(3):1–25, December

2021. URL: https://dl.acm.org/doi/10.1145/3491055, doi:10.1145/3491055.

[90] Ben Jones and Nick Feamster. Can Censorship Measurements Be Safe(r)? In *HotNets '15*. ACM, 2015. URL: http://conferences.sigcomm.org/hotnets/2015/papers/jones.pdf.

[91] Ben Jones, Tzu-Wen Lee, Nick Feamster, and Phillipa Gill. Automated Detection and Fingerprinting of Censorship Block Pages. In *Proceedings of the Internet Measurement Conference 2014*, pages 299–304, Vancouver BC Canada, November 2014. ACM. URL: https://dl.acm.org/doi/10.1145/2663716.2663722, doi:10.1145/2663716.2663722.

[92] David Kanouse. Explaining Negativity Biases in Evaluation and Choice Behavior: Theory and Research. *Advances in Consumer Research*, 11:703–708, 1984. URL: https://www.acrwebsite.org/volumes/6335/.

[93] Simin Kargar and Keith McManamen. Censorship and Collateral Damage: Analyzing the Telegram Ban in Iran. *SSRN Electronic Journal*, 2018. URL: https://www.ssrn.com/abstract=3244046, doi:10.2139/ssrn.3244046.

[94] Sheharbano Khattak, Mobin Javed, Syed Ali Khayam, Zartash Afzal Uzmi, and Vern Paxson. A Look at the Consequences of Internet Censorship Through an ISP Lens. In *Internet Measurement Conference*. ACM, 2014. URL: http://conferences2.sigcomm.org/imc/2014/papers/p271.pdf.

[95] Gary King, Jennifer Pan, and Margaret E. Roberts. How Censorship in China Allows Government Criticism but Silences Collective Expression. *American Political Science Review*, 2012. URL: https://gking.harvard.edu/files/censored.pdf.

[96] Gary King, Jennifer Pan, and Margaret E. Roberts. Reverse-engineering censorship in China: Randomized experimentation and participant observation. *Science*, 345(6199), 2014. Publisher: AAAS. URL: http://cryptome.org/2014/08/reverse-eng-cn-censorship.pdf.

[97] Jeffrey Knockel, Masashi Crete-Nishihata, Jason Q. Ng, Adam Senft, and Jedidiah R. Crandall. Every Rose Has Its Thorn: Censorship and Surveillance on Social Video Platforms in China. In *Free and Open Communications on the Internet*. USENIX, 2015. URL: https://www.usenix.org/system/files/conference/foci15/foci15-paper-knockel.pdf.

[98] Jeffrey Knockel and Lotus Ruan. Measuring QQMail's Automated Email Censorship in China. In *Free and Open Communications on the Internet*. ACM, 2021. URL: https://doi.org/10.1145/3473604.3474560.

[99] Zhanna Kozhamberdiyeva. Freedom of Expression on the Internet: A Case Study of Uzbekistan. *Review of Central and East European Law*, 33(1), 2008. URL: https://brill.com/view/journals/rela/33/1/article-p95_2.xml, doi:10.1163/092598808X262542.

[100] Censored Planet Lab. Censored Planet Dashboard 20200601-20210531. URL: https://dashboard.censoredplanet.org/.

[101] The Citizen Lab. Free Expression Online. URL: https://citizenlab.ca/category/research/free-expression-online/.

[102] Graham Lowe, Patrick Winters, and Michael L Marcus. The Great DNS Wall of China. Technical report, New York University, Technical Report, New York University, 2007. URL: https://censorbib.nymity.ch/pdf/Lowe2007a.pdf.

[103] Zhen Lu, Zhenhua Li, Jian Yang, Tianyin Xu, Ennan Zhai, Yao Liu, and Christo Wilson. Accessing Google Scholar under Extreme Internet Censorship: A Legal Avenue. In *Middleware*. ACM, 2017. URL: https://censorbib.nymity.ch/pdf/Lu2017a.pdf.

[104] Ryan Macasero. Signal shutdown to proceed during Sinulog 2020 events, January 2020. URL: https://www.rappler.com/nation/249581-signal-shutdown-sinulog-2020/.

[105] Michael Malakata. Malawi blocks social media networks to quell protests, July 2011. URL: https://web.archive.org/web/20110726185847/http://news.idg.no/cw/art.cfm?id=3DFADEBE-1A64-67EA-E44251D79A4C6F57.

[106] Antonio Mangino and Elias Bou-Harb. A Multidimensional Network Forensics Investigation of a State-Sanctioned Internet Outage. In *2021 International Wireless Communications and Mobile Computing (IWCMC)*, pages 813–818, Harbin City, China, June 2021. IEEE. URL: https://ieeexplore.ieee.org/document/9498743/, doi:10.1109/IWCMC51323.2021.9498743.

[107] Eleanor Marchant and Nicole Stremlau. The Changing Landscape of Internet Shutdowns in Africa. *International Journal of Communication*, 14, 2020. URL: https://ijoc.org/index.php/ijoc/article/view/11490/3182.

[108] Bill Marczak, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ron Deibert, and Vern Paxson. An Analysis of China's "Great Cannon". In *Free and Open Communications on the Internet*. USENIX, 2015. URL: https://www.usenix.org/system/files/conference/foci15/foci15-paper-marczak.pdf.

[109] Samvel Martirosyan. The main issues of Internet freedom in Armenia (in Armenian), January 2021. URL: https://media.am/hy/critique/2021/01/18/25891/.

[110] Alexander Master. *Modeling and Characterization of Internet Censorship Technologies*. Dissertation, Purdue University, West Lafayette, IN, 2023.

[111] Dan McDevitt. Rwanda censors critical, independent media in targeted fashion: report, October 2017. URL: https://www.opentech.fund/news/new-report-investigates-internet-censorship-during-rwandas-2017-presidential-election/.

[112] Allison McDonald, Matthew Bernhard, Luke Valenta, Benjamin VanderSloot, Will Scott, Nick Sullivan, J. Alex Halderman, and Roya Ensafi. 403 Forbidden: A Global View of CDN Geoblocking. In *Internet Measurement Conference*. ACM, 2018. URL: http://delivery.acm.org/10.1145/3280000/3278552/p218-McDonald.pdf.

[113] Lennart Mühlenmeier. Jordan does not block, it throttles internet access, June 2020. URL: https://netzpolitik.org/2020/jordan-throttles-not-blocks-internet-access-shutdowns-keepiton/#netzpolitik-pw.

[114] Zubair Nabi. The Anatomy of Web Censorship in Pakistan. *Free and Open Communications on the Internet*, August 2013. URL: https://www.usenix.org/system/files/conference/foci13/foci13-nabi.pdf.

[115] RIPE NCC. YouTube Hijacking: A RIPE NCC RIS case study, 2008. URL: https://web.archive.org/web/20080405030750/http://www.ripe.net/news/study-youtube-hijacking.html.

[116] NetBlocks. Iraq introduces nightly internet curfew, October 2019. URL: https://netblocks.org/reports/iraq-introduces-nightly-internet-curfew-JAp1DKBd.

[117] NetBlocks. Facebook Live streams restricted in Jordan during Teachers' Syndicate protests, July 2020. URL: https://netblocks.org/reports/facebook-live-streams-restricted-in-jordan-during-teachers-syndicate-protests-XB7K1xB7.

[118] NetBlocks. Internet disrupted in Colombia amid anti-government protests, May 2021. URL: https://netblocks.org/reports/internet-disrupted-in-colombia-amid-anti-government-protests-YAEvMvB3.

[119] Arian Akhavan Niaki, Shinyoung Cho, Zachary Weinberg, Nguyen Phong Hoang, Abbas Razaghpanah, Nicolas Christin, and Phillipa Gill. ICLab: A Global, Longitudinal Internet Censorship Measurement Platform. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 135–151, San Francisco, CA, USA, May 2020. IEEE. URL: https://ieeexplore.ieee.org/document/9152784/, doi:10.1109/SP40000.2020.00014.

[120] Daiyuu Nobori and Yasushi Shinjo. VPN Gate: A Volunteer-Organized Public VPN Relay System with Blocking Resistance for Bypassing Government Censorship Firewalls. In *Networked Systems Design and Implementation*. USENIX, 2014. URL: https://www.usenix.org/system/files/conference/nsdi14/nsdi14-paper-nobori.pdf.

[121] Access Now. #KeepItOn Coalition dataset 2016-2021. URL: https://www.accessnow.org/keepiton-2016-2021-data.

[122] Access Now. Access Now, 2022. URL: https://www.accessnow.org/about-us/.

[123] Dawn C Nunziato. The Beginning of the End of Internet Freedom. *Georgetown Journal of International Law*, 2014. URL: http://ssrn.com/abstract=2995714.

[124] Federal Court of Australia. Roadshow Films vs Telstra Corporation, April 2020. URL: https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2020/2020fca0507.

[125] Chitu Okoli and Kira Schabram. A Guide to Conducting a Systematic Literature Review of Information Systems Research. *SSRN Electronic Journal*, 2010. URL: http://www.ssrn.com/abstract=1954824, doi:10.2139/ssrn.1954824.

[126] Babatunde Okunoye, Maria Xynou, Arturo Filastò, and Gabreal Odunsi. Nigeria's 2019 elections through the lens of network measurements, May 2019. URL: https://ooni.org/post/2019-nigeria-internet-censorship/.

[127] OONI. Argentina blocking Uber website and app. URL: https://explorer.ooni.org/search?since=2017-01-01&until=2021-05-31&failure=false&probe_cc=AR&test_name=web_connectivity&domain=www.uber.com&only=anomalies.

[128] OONI. OONI Probe Data Set 20200601-20210531. URL: https://ooni.org/data/.

[129] OONI. OONI Research Reports Blog. URL: https://ooni.org/reports/.

[130] OONI. Open Observatory of Network Interference: Global community measuring Internet censorship since 2012. URL: https://ooni.org/.

[131] OONI. Estonia blocking gambling sites query, 2021. URL: https://explorer.ooni.org/search?since=2020-06-01&until=2021-05-31&failure=true&probe_cc=EE&test_name=web_connectivity&only=anomalies&category_code=GMB.

[132] Juan Ortiz Freuler. The weaponization of private corporate infrastructure: Internet fragmentation and coercive diplomacy in the 21st century. *Global Media and China*, November 2022. URL: http://journals.sagepub.com/doi/10.1177/20594364221139729, doi:10.1177/20594364221139729.

[133] Barbara Ortutay, Frank Bajak, and Tali Arbel. Cuba's internet cutoff: A go-to tactic to suppress dissent, July 2021. URL: https://apnews.com/article/business-technology-cuba-ca1ae7975e04481e8cbd56d62a7fb30e.

[134] Ramakrishna Padmanabhan, Arturo Filastò, Maria Xynou, Ram Sundara Raman, Kennedy Middleton, Mingwei Zhang, Doug Madory, Molly Roberts, and Alberto Dainotti. A multi-perspective view of Internet censorship in Myanmar. In *Proceedings of the ACM SIGCOMM 2021 Workshop on Free and Open Communications on the Internet*, pages 27–36, Virtual Event USA, August 2021. ACM. URL: https://dl.acm.org/doi/10.1145/3473604.3474562, doi:10.1145/3473604.3474562.

[135] Jong Chun Park and Jedidiah R. Crandall. Empirical Study of a National-Scale Distributed Intrusion Detection System: Backbone-Level Filtering of HTML Responses in China. In *Distributed Computing Systems*, pages 315–326. IEEE, 2010. URL: https://www.cs.unm.edu/~crandall/icdcs2010.pdf.

[136] Christopher Patton. Good-bye ESNI, hello ECH!, December 2020. URL: https://blog.cloudflare.com/encrypted-client-hello/.

[137] Katy Pearce. While Armenia and Azerbaijan fought over Nagorno-Karabakh, their citizens battled on social media, December 2020. URL: https://www.washingtonpost.com/politics/2020/12/04/while-armenia-azerbaijan-fought-over-nagorno-karabakh-their-citizens-battled-social-media/.

[138] Paul Pearce, Roya Ensafi, Frank Li, Nick Feamster, and Vern Paxson. Augur: Internet-Wide Detection of Connectivity Disruptions. In *Symposium on Security & Privacy*. IEEE, 2017. URL: https://www.ieee-security.org/TC/SP2017/papers/586.pdf.

[139] Paul Pearce, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. Global Measurement of DNS Manipulation. *Proceedings of the 26th USENIX Security Symposium*, 2017. URL: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-pearce.pdf.

[140] Chris Phiri. Zambia Reports, Watchdog 'Unblocked', April 2014. URL: https://web.archive.org/web/20190424160446/https://zambiareports.com/2014/04/04/zambia-reports-watchdog-unblocked/.

[141] Censored Planet. Censored Planet. URL: https://censoredplanet.org/.

[142] Louis Poinsignon. BGP leaks and cryptocurrencies, April 2018. URL: https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/.

[143] Andrea Purdeková. 'Even if I am not here, there are so many eyes': surveillance and state reach in Rwanda. *The Journal of Modern African Studies*, 49(3):475–497, September 2011. URL: https://www.cambridge.org/core/product/identifier/S0022278X11000292/type/journal_article, doi:10.1017/S0022278X11000292.

[144] Ram Sundara Raman, Leonid Evdokimov, Eric Wurstrow, J. Alex Halderman, and Roya Ensafi. Investigating Large Scale HTTPS Interception in Kazakhstan. In *Proceedings of the ACM Internet Measurement Conference*, pages 125–132. ACM, October 2020. URL: https://dl.acm.org/doi/10.1145/3419394.3423665, doi:10.1145/3419394.3423665.

[145] Ram Sundara Raman, Adrian Stoll, Jakub Dalek, Reethika Ramesh, Will Scott, and Roya Ensafi. Measuring the Deployment of Network Censorship Filters at Global Scale. In *Proceedings 2020 Network and Distributed System Security Symposium*, San Diego, CA, 2020. Internet Society. URL: https://www.ndss-symposium.org/wp-content/uploads/2020/02/23099.pdf, doi:10.14722/ndss.2020.23099.

[146] Ram Sundara Raman, Apurva Virkud, Sarah Laplante, Vinicius Fortuna, and Roya Ensafi. Advancing the Art of Censorship Data Analysis. In *Free and Open Communications on the Internet*, 2023. URL: https://petsymposium.org/foci/2023/foci-2023-0003.pdf.

[147] Reethika Ramesh, Ram Sundara Raman, Matthew Bernhard, Victor Ongkowijaya, Leonid Evdokimov, Anne Edmundson, Steven Sprecher, Muhammad Ikram, and Roya Ensafi. Decentralized Control: A Case Study of Russia. In *Proceedings 2020 Network and Distributed System Security Symposium*, San Diego, CA, 2020. Internet Society. URL: https://www.ndss-symposium.org/wp-content/uploads/2020/02/23098.pdf, doi:10.14722/ndss.2020.23098.

[148] Representative. Media Release: Taking action against illegal offshore gambling websites, November 2019. URL: https://www.paulfletcher.com.au/media-releases/media-release-taking-action-against-illegal-offshore-gambling-websites.

[149] Eric Rescorla, Kazuho Oku, Nick Sullivan, and Christopher Wood. TLS Encrypted Client Hello, Internet-Draft RFC. Draft RFC, Internet Engineering Task Force (IETF), 2022. URL: https://datatracker.ietf.org/doc/draft-ietf-tls-esni/15.

[150] Margaret E. Roberts. *Censored: distraction and diversion inside China's great firewall*. Princeton University Press, Princeton, 2020.

[151] Denham Sadler. Arbitrary site blocks a 'slippery slope', March 2019. URL: https://www.innovationaus.com/arbitrary-site-blocks-a-slippery-slope/.

[152] Ferry Astika Saputra, Isbat Uzzin Nadhori, and Balighani Fathul Barry. Detecting and blocking onion router traffic using deep packet inspection. In *2016 International Electronics Symposium (IES)*, pages 283–288, Denpasar, Indonesia, September 2016. IEEE. URL: http://ieeexplore.ieee.org/document/7861018/, doi:10.1109/ELECSYM.2016.7861018.

[153] Will Scott, Thomas Anderson, Tadayoshi Kohno, and Arvind Krishnamurthy. Satellite: Joint Analysis of CDNs and Network-Level Interference. *Proceedings of the 2016 USENIX Annual Technical Conference*, June 2016. URL: https://www.usenix.org/system/files/conference/atc16/atc16_paper-scott.pdf.

[154] Wendy Seltzer. Infrastructures of Censorship and Lessons from Copyright Resistance. *USENIX Workshop on Free and Open Communications on the Internet*, 2011. URL: https://www.usenix.org/legacy/events/foci11/tech/final_files/Seltzer.pdf.

[155] Serbia. Zakon o igrama na sreću [The Law about Gambling], 2020. URL: https://www.paragraf.rs/propisi/zakon_o_igrama_na_srecu.html.

[156] Andreas Sfakianakis, Elias Athanasopoulos, and Sotiris Ioannidis. CensMon: A Web Censorship Monitor. In *Free and Open Communications on the Internet*. USENIX, 2011. URL: https://www.usenix.org/legacy/events/foci11/tech/final_files/Sfakianakis.pdf.

[157] Justine Sherry, Chang Lan, Raluca Ada Popa, and Sylvia Ratnasamy. BlindBox: Deep Packet Inspection over Encrypted Traffic. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, pages 213–226, London United Kingdom, August 2015. ACM. URL: https://dl.acm.org/doi/10.1145/2785956.2787502, doi:10.1145/2785956.2787502.

[158] Kushagra Singh, Gurshabad Grover, and Varun Bansal. How India Censors the Web. In *12th ACM Conference on Web Science*, pages 21–28, Southampton United Kingdom, July 2020. ACM. URL: https://dl.acm.org/doi/10.1145/3394231.3397891, doi:10.1145/3394231.3397891.

[159] Internet Society. Internet Society Pulse - Internet Shutdown Tracker 2020-2021. URL: https://pulse.internetsociety.org/shutdowns.

[160] Ram Sundara Raman, Prerana Shenoy, Katharina Kohls, and Roya Ensafi. Censored Planet: An Internet-wide, Longitudinal Censorship Observatory. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 49–66, Virtual Event USA, October 2020. ACM. URL: https://dl.acm.org/doi/10.1145/3372297.3417883, doi:10.1145/3372297.3417883.

[161] Rima Tanash, Zhouhan Chen, Dan Wallach, and Melissa Marschall. The Decline of Social Media

Censorship and the Rise of Self-Censorship after the 2016 Failed Turkish Coup. In *Free and Open Communications on the Internet*. USENIX, 2017. URL: https://www.usenix.org/system/files/conference/foci17/foci17-paper-tanash.pdf.

[162] Rima S. Tanash, Zhouhan Chen, Tanmay Thakur, Dan S. Wallach, and Devika Subramanian. Known Unknowns: An Analysis of Twitter Censorship in Turkey. In *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society*, pages 11–20, Denver Colorado USA, October 2015. ACM. URL: https://dl.acm.org/doi/10.1145/2808138.2808147, doi:10.1145/2808138.2808147.

[163] Berhan Taye, Maria Xynou, Leonid Evdokimov, and Moses Karanja. Ethiopia: Verifying the unblocking of websites, June 2018. URL: https://ooni.org/post/ethiopia-unblocking/.

[164] Tbilisi. Georgia Blocks Access to Pro-Islamic State Websites, November 2015. URL: https://old.civil.ge/eng/article.php?id=28801?id=28801.

[165] ONI Team. Looking Forward: A Note of Appreciation and Closure on a Decade of Research, December 2014. URL: https://opennet.net/blog/2014/12/looking-forward-note-appreciation-and-closure-decade-research.

[166] Michael Carl Tschantz, Sadia Afroz, Anonymous, and Vern Paxson. SoK: Towards Grounding Censorship Circumvention in Empiricism. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 914–933, San Jose, CA, May 2016. IEEE. URL: http://ieeexplore.ieee.org/document/7546542/, doi:10.1109/SP.2016.59.

[167] Todd Underwood. Internet-wide Catastrophe - Last Year, December 2005. URL: https://web.archive.org/web/20080228131639/http://www.renesys.com/blog/2005/12/internetwide_nearcatastrophela.shtml.

[168] Unknown. Dozens detained at Kazakhstan political prisoner protest, February 2021. URL: https://www.aljazeera.com/news/2021/2/28/dozens-detained-at-kazakhstan-political-prisoner-protest.

[169] Brian Van Leeuwen, Jason Gao, Haikuo Yin, Benjamin Anthony, and Vincent Urias. Networked-based Cyber Analysis using Deep Packet Inspection (DPI) for High-Speed Networks. Technical Report SAND2019-13774, 1863848, 705224, Sandia National Lab, U.S. Department of Energy, November 2019. URL: https://www.osti.gov/servlets/purl/1863848/, doi:10.2172/1863848.

[170] Benjamin VanderSloot, Allison McDonald, Will Scott, J Alex Halderman, and Roya Ensafi. Quack: Scalable Remote Measurement of Application-Layer Censorship. *USENIX Security Symposium*, page 16, 2018.

[171] Joana Varon, Rebecca Gomperts, Maria Xynou, Federico Ceratto, and Arturo Filastò. On the blocking of abortion rights websites: Women on Waves & Women on Web, October 2019. URL: https://ooni.org/post/2019-blocking-abortion-rights-websites-women-on-waves-web/#brazil.

[172] Pieter Velghe. “Reading China”: The Internet of Things, Surveillance, and Social Management in the PRC. *China Perspectives*, 2019(1):85–89, March 2019. URL: http://journals.openedition.org/chinaperspectives/8874, doi:10.4000/chinaperspectives.8874.

[173] John-Paul Verkamp and Minaxi Gupta. Inferring Mechanics of Web Censorship Around the World. In *2nd USENIX Workshop on Free and Open Communications on the Internet (FOCI 12)*, Bellevue, WA, August 2012. USENIX Association. URL: https://www.usenix.org/conference/foci12/workshop-program/presentation/Verkamp.

[174] Vasilis Ververis, Maria Xynou, Tawanda Mugari, and Will Scott. OONI Data Reveals How WhatsApp Was Blocked (Again) in Brazil, May 2016. URL: https://ooni.org/post/brazil-whatsapp-block/.

[175] James Vincent. UK police shut off Wi-Fi in London Tube stations to deter climate protestors, April 2019. URL: https://www.theverge.com/2019/4/17/18411820/london-underground-tube-wi-fi-down-shut-off-protests-extinction-rebellion.

[176] Anjali Vyas, Ram Sundara Raman, Nick Ceccio, Philipp M. Lutscher, and Roya Ensafi. Lost in Transmission: Investigating Filtering of COVID-19 Websites. In Nikita Borisov and Claudia Diaz, editors, *Financial Cryptography and Data Security*, volume 12675, pages 417–436, Berlin, Heidelberg, 2021. Springer Berlin Heidelberg. Series Title: Lecture Notes in Computer Science. URL: https://link.springer.com/10.1007/978-3-662-64331-0_22, doi:10.1007/978-3-662-64331-0_22.

[177] Ben Wagner. The Politics of Internet Filtering: The United Kingdom and Germany in a

Comparative Perspective. *Politics*, 34(1):58–71, February 2014. URL: http://journals.sagepub.com/doi/10.1111/1467-9256.12031, doi:10.1111/1467-9256.12031.

[178] Christopher Walker and Robert W. Orttung. Breaking the News: The Role of State-Run Media. *Journal of Democracy*, 25(1):71–85, 2014. URL: http://muse.jhu.edu/content/crossref/journals/journal_of_democracy/v025/25.1.walker.html, doi:10.1353/jod.2014.0015.

[179] Barney Warf. Geographies of global Internet censorship. *GeoJournal*, 76(1):1–23, February 2011. URL: http://link.springer.com/10.1007/s10708-010-9393-3, doi:10.1007/s10708-010-9393-3.

[180] Zachary Weinberg, Diogo Barradas, and Nicolas Christin. Chinese Wall or Swiss Cheese? Keyword filtering in the Great Firewall of China. In *Proceedings of the Web Conference 2021*, pages 472–483, Ljubljana Slovenia, April 2021. ACM. URL: https://dl.acm.org/doi/10.1145/3442381.3450076, doi:10.1145/3442381.3450076.

[181] Philipp Winter. CensorBib: Selected Research Papers in Internet Censorship. URL: https://censorbib.nymity.ch/.

[182] Philipp Winter. NullHypothesis / censorbib. URL: https://github.com/NullHypothesis/censorbib.

[183] Philipp Winter and Stefan Lindskog. How the Great Firewall of China is Blocking Tor. In *Free and Open Communications on the Internet*. USENIX, 2012. URL: https://www.usenix.org/system/files/conference/foci12/foci12-final2.pdf.

[184] Sebastian Wolfgarten. Investigating large-scale Internet content filtering. Technical Report, Technical Report, Dublin City University, Dublin, Ireland, 2006. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.133.5778&rep=rep1&type=pdf.

[185] Alexander Wong. Malaysian authorities start blocking servers that stream pirated content, February 2020. URL: https://soyacincau.com/2020/02/28/malaysia-block-server-ip-illegal-copyright-streaming-android-tv/.

[186] Samuel Woodhams and Simon Migliano. Cost of Internet Shutdowns Report 2021, January 2022. URL: https://www.top10vpn.com/research/cost-of-internet-shutdowns/2021/.

[187] Joss Wright. Regional Variation in Chinese Internet Filtering. Technical report, University of Oxford, 2012. URL: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2265775_code1448244.pdf?abstractid=2265775&mirid=3.

[188] Xueyang Xu, Z. Morley Mao, and J. Alex Halderman. Internet Censorship in China: Where Does the Filtering Occur? In Neil Spring and George F. Riley, editors, *Passive and Active Measurement*, volume 6579, pages 133–142. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011. Series Title: Lecture Notes in Computer Science. URL: http://link.springer.com/10.1007/978-3-642-19260-9_14, doi:10.1007/978-3-642-19260-9_14.

[189] Diwen Xue, Benjamin Mixon-Baca, ValdikSS, Anna Ablove, Beau Kujath, Jedidiah R. Crandall, and Roya Ensafi. TSPU: Russia's decentralized censorship system. In *Proceedings of the 22nd ACM Internet Measurement Conference*, pages 179–194, Nice France, October 2022. ACM. URL: https://dl.acm.org/doi/10.1145/3517745.3561461, doi:10.1145/3517745.3561461.

[190] Diwen Xue, Reethika Ramesh, Valdik S S, Leonid Evdokimov, Andrey Viktorov, Arham Jain, Eric Wustrow, Simone Basso, and Roya Ensafi. Throttling Twitter: an emerging censorship technique in Russia. In *Proceedings of the 21st ACM Internet Measurement Conference*, pages 435–443, Virtual Event, November 2021. ACM. URL: https://dl.acm.org/doi/10.1145/3487552.3487858, doi:10.1145/3487552.3487858.

[191] Maria Xynou, Simone Basso, Ramakrishna Padmanabhan, and Arturo Filastò. Uganda: Data on internet blocks and nationwide internet outage amid 2021 general election, January 2021. URL: https://ooni.org/post/2021-uganda-general-election-blocks-and-outage/.

[192] Maria Xynou and Arturo Filastò. How Uganda blocked social media, again, May 2016. URL: https://ooni.org/post/uganda-social-media-blocked/.

[193] Maria Xynou and Arturo Filastò. Belarus protests: From internet outages to pervasive website censorship, September 2020. URL: https://ooni.org/post/2020-belarus-internet-outages-website-censorship/.

[194] Maria Xynou and Arturo Filastò. How countries attempt to block Signal Private Messenger App around the world, October 2021. URL: https://ooni.org/post/2021-how-signal-private-messenger-blocked-around-the-world/.

[195] Maria Xynou and Arturo Filastò. Zambia: Social media blocked amid 2021 general elections, August 2021. URL: https://ooni.org/post/2021-zambia-social-media-blocks-amid-elections/.

[196] Maria Xynou, Arturo Filastò, and Moses Karanja. Ethiopia: From internet blackouts to the blocking of WhatsApp and Telegram, June 2019. URL: https://ooni.org/post/ethiopia-whatsapp-telegram/.

[197] Maria Xynou, Arturo Filastò, Tawanda Mugari, and Natasha Msonza. Zimbabwe protests: Social media blocking and internet blackouts, January 2019. URL: https://ooni.org/post/venezuela-internet-censorship/.

[198] Tarun Kumar Yadav, Akshat Sinha, Devashish Gosain, Piyush Kumar Sharma, and Sambuddho Chakravarty. Where The Light Gets In: Analyzing Web Censorship Mechanisms in India. In *Internet Measurement Conference*. ACM, 2018. doi:10.1145/3278532.3278555.

[199] Stephanie Yang. China Appears to Block Popular Encrypted Messaging App Signal, March 2021. URL: https://www.wsj.com/articles/china-appears-to-block-signal-one-of-last-popular-encrypted-messaging-apps-11615883434.

[200] Bilge Yesil, Efe Kerem Sozeri, and Emad Khazraee. Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance. Technical Report, University of Pennsylvania, Philadelphia, PA, February 2017. URL: https://repository.upenn.edu/internetpolicyobservatory/22/.

[201] Pengxiong Zhu, Keyu Man, Zhongjie Wang, Zhiyun Qian, Roya Ensafi, J. Alex Halderman, and Haixin Duan. Characterizing Transnational Internet Performance and the Great Bottleneck of China. *Measurement and Analysis of Computing Systems*, 4(1), 2020. Publisher: ACM. URL: https://dl.acm.org/doi/pdf/10.1145/3379479.

[202] Jonathan Zittrain and Benjamin Edelman. Documentation of Internet filtering in Saudi Arabia. Technical report, Berkman Center for Internet & Society, Harvard Law School, September 2002. URL: https://cyber.harvard.edu/filtering/saudiarabia/.

[203] Jonathan Zittrain and Benjamin Edelman. Internet Filtering in China. *IEEE Internet Computing*, 7(2), 2003. URL: https://ieeexplore.ieee.org/abstract/document/1189191, doi:10.1109/MIC.2003.1189191.

[204] Jonathan L. Zittrain, Robert Faris, Helmi Noman, Justin Clark, Casey Tilton, and Ryan Morrison-Westphal. The Shifting Landscape of Global Internet Censorship. *SSRN Electronic Journal*, 2017. URL: https://www.ssrn.com/abstract=2993485, doi:10.2139/ssrn.2993485.

A Data

Table 3: Evidence of Internet Censor Methods by Country

China	[4, 12, 13, 20, 27, 35, 40, 42, 48, 55, 56, 65, 71, 72, 74, 86, 89, 96, 102, 108, 120, 128, 135, 138, 139, 173, 180, 183, 184, 187, 188, 194, 199, 201, 203]
Iran	[4, 9, 10, 10, 14, 19, 20, 27, 28, 52, 65, 89, 93, 106, 121, 128, 138, 139, 159, 166, 173, 194]
Myanmar (Burma)	[45, 65, 91, 121, 128, 134, 159]
Cuba	[17, 46, 121, 133, 141, 159, 194]
Vietnam	[18, 47, 65]
Saudi Arabia	[6, 8, 44, 47, 89, 91, 173, 202]
Pakistan	[1, 2, 47, 49, 89, 94, 114, 115, 128, 159]
Egypt	[43, 49, 65, 89, 100, 159]
Ethiopia	[4, 47, 49, 100, 121, 159, 163, 166, 196]
United Arab Emirates	[4, 44, 47, 65, 89, 91, 128, 166]
Uzbekistan	[89, 99, 128, 159, 194]
Venezuela	[36, 65, 82]
Bahrain	[47, 89, 128, 173]
Russia	[11, 65, 78, 89, 121, 128, 138, 142, 147, 173, 186, 189, 190]
Belarus	[49, 121, 128, 139, 159, 193]
Kazakhstan	[4, 20, 27, 49, 65, 85, 89, 121, 139, 144, 159, 166, 168]
Sudan	[47, 138, 159]
Turkey	[5, 11, 49, 61, 89, 128, 138, 161, 162, 166, 167, 173, 200]
Azerbaijan	[47, 64, 91, 100, 128, 137, 159]
Thailand	[4, 47, 48, 63, 65, 91, 100, 128, 166, 173]
Rwanda	[62, 111, 143, 178]
Bangladesh	[23, 89, 100, 121, 159, 173]
Iraq	[116, 139, 159]
Cambodia	[100]
Zimbabwe	[197]
Jordan	[47, 89, 100, 107, 113, 117, 156]
Indonesia	[65, 128, 139]
Libya	[22, 43, 130, 138]
Nicaragua	[100]
India	[47, 65, 68, 89, 100, 121, 128, 158, 159, 173, 198]
Uganda	[100, 121, 159, 191, 192]
Lebanon	[100]
Sri Lanka	[100, 159]
Kyrgyzstan	[65, 100]
Morocco	[65]
The Gambia	[15, 33, 59]
Singapore	[79, 84, 100]
Malaysia	[65, 91, 100, 128, 173, 185]
Malawi	[53, 105]
Nigeria	[7, 65, 126, 159]
Zambia	[140, 195]
Mexico	[87, 89, 100]
Angola	[100]
Ecuador	[89, 100]
Ukraine	[89, 128]
Tunisia	[4, 47, 91, 166]
Brazil	[171, 174]
Ghana	[100]
Colombia	[47, 118]
Philippines	[4, 100, 104, 166]
Kenya	[77]
South Korea	[38, 41, 47, 65, 89, 100, 128, 173]
Hungary	[100]
Argentina	[127]
Armenia	[100, 109, 186]
Serbia	[155]
South Africa	-
Australia	[22, 124, 148, 151]
United States	[24, 81, 123, 154, 175, 177]
Italy	[2, 31, 128]
Japan	-
Georgia	[164]
France	[65, 89, 128]
United Kingdom	[39, 81, 89, 138, 175]
Germany	[30, 51, 65, 76, 156, 177]
Taiwan	[70]
Canada	[22, 75, 176]
Costa Rica	-
Estonia	[25, 131]
Iceland	[69]