CERIAS Tech Report 2026-03

A Survey and Taxonomy of Internet Censorship Methods

by Alexander Master and Eugene H. Spafford

Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Computers & Security 171 (2026) 105076

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Full length article

A Survey and Taxonomy of Internet Censorship Methods

Alexander Master [a],*, Eugene H. Spafford [b]

[a] United States Military Academy, West Point, NY, USA
[b] Purdue University, West Lafayette, IN, USA

ARTICLE INFO

Keywords:
Internet censorship methods
Taxonomy
Nation-state censors
Networking
Circumvention

ABSTRACT

Despite the significance of the Internet in global information exchange, authorities in many jurisdictions apply censorship to online communications within their sphere of influence. Some people consider censorship a violation of human rights, such as the freedom of expression or the right to access information. Others view censorship methods as a means of social control, protecting national security or social harmony. Regardless of the motivation, researchers, policymakers, and technology practitioners should have a thorough understanding of the capabilities of Internet censors. We present a taxonomy of Internet censorship methods derived from a systematic review of the literature and analysis of the technology that has enabled the Internet's progression. We describe the technical means that censors implement, contextualized by the legal and social circumstances in which they have occurred over the past three decades. We assert that the taxonomy has pedagogical value and serves as a research framework for further studies. Our study illuminates the dynamic challenges faced in interdisciplinary research on Internet censorship, offering direction for future work on Internet measurement, censorship circumvention, and protocol standards design.

1. Introduction

Internet censorship is a relatively new phenomenon in the human experience as a means of controlling information. With the transition from the Industrial Age to the Information Age, information technology and computing systems have become central to society's functions and progress. With the advent of the World Wide Web in the 1990s and decreasing costs of technology, Internet access became available to average citizens in many nations. Internet-connected devices have continued to proliferate, allowing more people to communicate in near real-time over various mediums and protocols. At the same time, governments of nation-states around the world began to realize the power and influence of the "information superhighway". Authorities proceeded to explore methods for controlling information access and exchange through this new medium. Internet censorship has increased in size, scale, and capability over the past three decades, and now impacts billions of people globally (Master and Garman, 2023; Freedom House, 2026).

Aceto and Pescapé define Internet censorship as "the intentional impairing or blocking of access to online resources and services", regardless of the goal, scope, or legitimacy of the actions (Aceto and Pescapé, 2015). The technical means by which Internet censors implement censorship vary widely but are generally constrained by standardized protocols that enable the Internet to function as a network of networks. Some Internet censors block web pages with "objectionable"[1] content and inform users that their request was denied. Others simply drop the connection or manipulate the traffic so that the connection appears to fail. Some censors degrade the connectivity of a user when undesirable activity is detected, rendering the communication unusable. Applications that allow for unmoderated communications may be blocklisted (some previous literature refers to this practice as "blacklisting"), denied based on ports used by the application's software or signatures of its data packets. Censors can be nation-state actors or private entities. In addition to blocking communication, Internet surveillance is closely related to censorship activities. Detection of objectionable content is generally the first and most important step toward implementation of a blocking action. More aggressive nation-state censors completely disconnect Internet connectivity (Bischof et al., 2023) during perceived critical events, such as elections or periods of civil unrest (Gregorio, 2020). In some extreme cases, censorship may lead to physical confrontation with the content authors by local authorities.

Internet censorship occurs using a broad spectrum of methods and activities. In some cases, the effects of communication disconnection are overt and obvious to the user population, while other countries seek to minimize economic collateral damage from their censorship and use

* Corresponding author.
E-mail addresses: alexander.master@westpoint.edu (A. Master), spaf@purdue.edu (E.H. Spafford).

[1] Objectionable is locally defined by policy or statute, and appropriateness is thus subjective. In the following, we will refer to objectionable content without judgment as to actual subject matter.

https://doi.org/10.1016/j.cose.2026.105076
Received 30 March 2026; Received in revised form 10 July 2026; Accepted 23 July 2026
Available online 4 August 2026

more targeted techniques. Some authorities wish to conceal that they are censoring content and resort to techniques such as the use of artificial Transmission Control Protocol (TCP) Reset packets (Wang et al., 2017; Weaver et al., 2009; Fallows, 2008) or bandwidth throttling (Xue et al., 2021; Mühlenmeier, 2020; Esfandiari, 2013). In these cases, users may believe that they are experiencing poor network service, which increases the difficulty for Internet measurement researchers to detect censor activity and changes over time. Furthermore, as end-to-end encrypted (E2EE) messaging services gain popularity for their security and privacy properties, censoring nation-states have shown an increased willingness to target these protocols. The proliferation of encrypted traffic analysis (ETA) software or next-generation firewalls (NGFWs) that can block applications such as Signal (Xynou and Filastò, 2021; Yang, 2021; Peters, 2024) and Tor Browser (Dunna et al., 2018) may represent new threats to private communications.

Given censorship's wide-ranging implications, in this study we sought to systematize the knowledge of Internet censorship methods by answering the following research question: "What are the technical threats to Internet-based communications within the context of censorship?" We present the results in Section 5 as a taxonomy of Internet censorship methods. We demonstrate the taxonomy's validity using a systematic review of several decades of multidisciplinary literature surrounding Internet-based censorship and how it has evolved. We assert that the taxonomy has pedagogical value and serves as a research framework for further studies. Our study illuminates challenges faced in interdisciplinary research on Internet censorship, offering direction for future work on Internet measurement, censorship circumvention, and protocol standards design.

2. Background

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 (ISP) 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), whose censorship apparatus is known as the "Great Firewall of China", is considered by many to be the most sophisticated and aggressive centralized state censor (Ortiz Freuler, 2022; Zhu et al., 2020; Bock et al., 2020a; Roberts, 2020; Velghe, 2019; Chandel et al., 2019; Ensafi et al., 2015b). Other examples include small countries with limited access to transnational fiber switching. Syria, which only has one government-controlled autonomous system (AS) (Chaabane et al., 2014), 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 (Ramesh et al., 2020; Xue et al., 2022a) and India (Gosain et al., 2018; Singh et al., 2020; Yadav et al., 2018). Authorities in these nations legally compel private-sector service providers to perform web filtering, throttling, or shutdowns. Technical implementations may vary widely among corporations, resulting in a patchwork of censorship. China has even shown signs of uneven implementation of censorship across regions in recent years (Wu et al., 2025).

Internet censorship also intersects with human conceptions of governance. The proliferation of Internet access has enabled the rapid and widespread exchange of information around the world, accelerating scientific discovery, enabling technological and economic development, and democratizing access to knowledge. The Internet has surpassed television, print media, and radio in terms of media influence and has become one of "the irreplaceable elements of our lives since the 2000s" (Dolunay et al., 2017). While this has been largely a global phenomenon, leaders of some countries wish to assert control over the information environment within their geopolitical borders. In some cases, globalization has been met with the creation of "splinternets", attempts to create separate and independent online resources that reduce or eliminate reliance on global Internet resources. For many years, the Russian Federation has attempted to sever its ties with Western and international web resources and, on several occasions, has tested its ability to operate when disconnected from transnational fiber connectivity (Luxmoore and Czerny, 2026; Soldatov and Borogan, 2015; Marrow and Antonov, 2021). The Islamic Republic of Iran provides an intranet of government-provided information, maintained by the Islamic Revolutionary Guard Corps (IRGC), for when the government shuts down external Internet access for its population (see Section 4.9). The Democratic People's Republic of Korea (DPRK, commonly known as North Korea) has long maintained a policy of denying external Internet connectivity to most of its citizens (Howard et al., 2015). As part of China's strategic goal of promoting and maintaining social harmony, the Communist Party of China (CCP) has pursued a strategy of "cyber sovereignty", which presupposes that the state has the right to control cyberspace within its sphere of control (Master and Gomber, 2026). Aside from its Social Credit System (Chen and Grossklags, 2022) and the Great Firewall, China offers replacement online platforms for Western websites it blocks, creating a media and information environment in which it can control messages, themes, and narratives through surveillance or coercion (Roberts, 2018).[2] Concerns about "splinternets" and erosion of the global Internet have also emerged in Western contexts, when consumer privacy legislation in the European Union has begun to demand data sovereignty (non-reliance on foreign technology firms) and rights granted to EU citizens concerning their personal data (Madiega and Luca, 2023; Grover et al., 2024). Among these global developments, Internet censorship remains one of the most direct and pervasive means of limiting individual freedom of expression.

Many instances of Internet censorship have occurred in the last three decades. Social movements, such as the "Arab Spring" in the early 2010s, were aided by the use of technology to organize protests and thus became targets for censorship. Authoritarian leaders have shown willingness to selectively censor information they deem a threat to their maintenance of power. Some governments have gone as far as completely disconnecting Internet connectivity during turbulent periods (Gregorio, 2020; Access Now, 2026).

Examples of state-sponsored censorship have been documented around the world. From March 2018 to July 2019, the Republic of Chad in Africa blocked access to all major social media platforms, including WhatsApp, Twitter, Instagram, YouTube, and Facebook, for "security reasons in the context of terrorist attacks" (Dahir, 2019). In August 2019, the longest-running Internet shutdown imposed by a democratic government occurred in the region of Jammu and Kashmir after the Indian government revoked the region's special autonomous status. The resulting communications blackout and Internet restrictions lasted approximately 18 months, with cellular mobile Internet access not fully restored until February 2021 (Internet Society Pulse, 2021). In February 2021, after the military forces of Myanmar (formerly Burma) overthrew the elected government in a coup d'état, the Burmese people experienced cellular network shutdowns, nightly Internet curfews, and blocking of social networks (Facebook, Twitter, and Instagram) (Padmanabhan et al., 2021). In July 2021, Cubans took to the streets to protest their government's response to the COVID-19 pandemic. Government officials restricted access to Facebook and WhatsApp during

[2] Examples of Chinese platforms include: Sina Weibo, which provides microblogging services; WeChat, which enables ride-sharing, instant messaging, ticket sales, and more; Douyin, which provides short-form video social media (similar to TikTok); Zhihu, which serves as a question-and-answer website (similar to Quora); and Baidu, China's most popular search engine.

demonstrations. Many Cubans used the anti-censorship tool Psiphon for open access to the Internet (David, 2021).

In February 2022, metrics of total TOR network usage showed an increase of more than 300% in connections originating from Ukraine immediately after the invasion by Russia (Tor, 2022). Ukrainians continued to rely on virtual private networks (VPNs) and anti-censorship technologies as the Russian Federation diverted Ukrainian Internet traffic through Russian service providers (Satariano, 2022) to censor information sources and conduct surveillance operations. Domestically, Roskomnadzor — the federal agency responsible for monitoring, controlling, and censoring Russian mass media — ordered the blocking of popular apps such as Telegram and filtering traffic from media sources such as the British Broadcasting Company (BBC), Deutsche Welle, Radio Free Europe, and Voice of America, among others (Reuters, 2022). During the United States' 2026 conflict with Iran, Iranians experienced months of Internet blackout, denying them access to information from outside of their country (Burgess and Newman, 2026).

Censorship is a broad issue that encompasses numerous aspects of modern societies. Some censorship is mandated by law in particular countries, for reasons ranging from morality to political manipulation and control of the information environment. This study does not assert value judgments about the reasons for Internet-based censorship. Instead, we recognize that international expectations and norms are violated in some locations. Article 19 of the Universal Declaration of Human Rights states that freedom of expression is an inherent right, including the "freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers" (United Nations, 1948). Internet censorship, without broad agreement from those subjected to censorship about what materials are objectionable, limits their individual expression as well as the propagation of knowledge.

2.1. Related work

Deibert et al. published the seminal *Access Denied* report in 2008, which was the first attempt at a global study on Internet censorship. Their work covered practices in 40 countries and divided technical censorship techniques into four categories: IP blocking, DNS tampering, blockpage, and keyword (Deibert et al., 2008). The Internet has since become increasingly complex. Global Internet user penetration rates continue to increase, and changing geopolitical landscapes impact the resources that censors are willing to implement to deny access to information. Many Internet measurement organizations and platforms are now providing data that were not available a decade ago.

Aceto and Pescapé wrote a survey of censorship detection systems in 2015 (Aceto and Pescapé, 2015). That work covered academic detection architectures as well as deployed Internet measurement platforms. It relied on the detection systems' design goals (as stated by their authors) for its characterizations, whereas this work focuses on evidence of censorship and characterizes it using the technical methods implemented by nation-state censors, within the historical context of how it occurred over the past three decades. While the section three of their paper lists many of the examples found in this survey, our taxonomy provides the comprehensive abstraction of censor methods, as well as benefits from ten additional years of research to build on.

Hall et al. have a draft informational request for comments (RFC) online, which serves to document ways in which regimes around the world block or impair Internet traffic (Hall et al., 2022). The page is a helpful reference for designers, implementers, and users of Internet protocols to understand the properties of Internet technologies that are being exploited to censor end-user access to information. The RFC suggests that it is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress". Our work bolsters these efforts by surveying the academic literature to systemize our knowledge of censor methods, rather than relying on anecdotes.

Master and Garman conducted a worldwide study of nation-state Internet censorship (Master and Garman, 2023). Their study used a globally representative sample of 70 countries and found that 62 of these countries over a 20-year study period used at least one censorship method against their citizens. They used a preliminary version of our Internet Censorship Methods Taxonomy (Master, 2023) as a basis for their study.

Khattak et al. performed a systematization of knowledge study on systems they termed "Censorship Resistance Systems" (CRSs). Their subjects included deployed software and theoretical systems from academic papers and "access-centric" and "publication-centric" schemes. The paper surveyed 73 such systems (Khattak et al., 2016) and offered an abstract censor attack model. The authors focused on the goals of CRS designers, not necessarily on censor abilities directly.

Wendzel et al. also conducted a survey of Internet censorship and its measurement (Wendzel et al., 2025), similar to Aceto and Pescapé (Aceto and Pescapé, 2015). While their summary of censorship methods is robust, it is a precursor to their primary goal of characterizing censorship measurement methodology. We focus on censors themselves and the historical context surrounding those methods, as well as abstracting censor methods into a comprehensive taxonomy.

In a partially related study, Tschantz et al. performed an extensive survey of evaluation criteria for CRSs (Tschantz et al., 2016). The authors compare the evaluation criteria elements from the literature to observed "real-world" censor behavior derived from field reports and bug tickets, revealing that they are often incongruent. Their goals were to enumerate the evaluation criteria and identify trends rather than to systematize the censor behavior.

To our knowledge, our study is the first to offer a taxonomy of Internet censorship methods. We focus on the technical means by which censors deny access to Internet communications over the past three decades. We provide a synthesis of our systematic literature review in the form of a taxonomy, which has pedagogical value for educators and new researchers to the field, as well as providing a research framework for future studies.

3. Methodology

The research question we address in this work is "What are the technical threats to Internet-based communications within the context of censorship?" To comprehensively address the topic, we used a systematization of knowledge (SoK) approach. SoK studies provide a comprehensive overview of the literature for a particular topic. These works save researchers significant time and effort in discovering the edges of the state-of-the-art.

Fink defines a systematic literature review as "a systematic, explicit, and reproducible method for identifying, evaluating, and synthesizing the existing body of a completed and recorded work by researchers, scholars, and practitioners" (Fink, 2005). Systematic reviews and meta-analyses found early success in medical research (Moher et al., 2009), and other communities have since benefited from their insights and approaches. Research must move quickly as new technologies are developed, a challenge in rapidly advancing fields. In 2010, Okoli and Schabram published "A Guide to Conducting a Systematic Literature Review of Information Systems Research" to address the challenges IS researchers face (Okoli and Schabram, 2010). We utilized Okoli and Schabram's approach to systematize the literature pertaining to Internet censorship.

In our study, Internet censorship methods are technical threats to Internet-based communications that a governmental authority or Internet Service Provider (ISP) can impose. The technical means by which Internet censors implement censorship vary widely but are generally constrained by the standardized protocols that allow the Internet to function: Internet Protocol (IP), Border Gateway Protocol (BGP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP),

and QUIC.[3] Several application-layer protocols are covered in depth because of their importance to the World Wide Web. Thus, literature focused on technology was the primary source of data collection. Communications, political science, and social science journals were also referenced when the domains intersected.

Peer-reviewed journals and conferences were our primary data sources in the research protocol. In cases of emerging technology where scholarly work was not yet available, we utilized government reports, technical reports, and technology blogs. Data sets from Internet measurement communities were often central to these reports. Finally, if appropriate, we cited qualitative data from advocacy organizations and media reporting.

CensorBib[4] was our starting point for data collection. CensorBib is a curated online archive of research papers in the field of Internet censorship (Winter, 2023). Its focus is on papers that approach Internet censorship from a technical perspective. Given their predominance in the dataset on CensorBib, the following conferences and workshops were thoroughly surveyed: IEEE Security & Privacy, USENIX Security Symposium, ACM Computer and Communications Security, Network and Distributed System Security (NDSS) Symposium, the Privacy Enhancing Technologies Symposium (PETS), the Workshop on Free and Open Communications on the Internet (FOCI), and the ACM Internet Measurement Conference (IMC). All are venues for high-quality, technology-focused research. Papers were initially screened by title and abstract for relevance. We noted techniques and methods as we worked through the review. We also pursued citations within the references or bibliography section of identified papers, as applicable.

After reviewing the research publications, we constructed the initial elements of the taxonomy. Internet censorship happens on computing systems; using the OSI conceptual model (Day and Zimmermann, 1983) that describes computing system interconnection assisted in ensuring the comprehensiveness of the taxonomy. Each censorship method was grouped and abstracted based on the experience of the authors and informal peer review of researchers at our institutions. A second round of data collection then filled gaps and provided additional supporting sources for the taxonomy elements. We used keywords derived from the first round with Google Scholar, our institutions' digital libraries of subscriptions, and two search engines (Google and DuckDuckGo). This allowed coverage of scholarly sources not included in CensorBib or the preselected venues, as well as government reports and blog posts.

Limitations and Constraints. This study offers a global view of the issues related to Internet censorship. We acknowledge that this work is influenced by Western philosophy given that it originates in the United States and is also limited to sources available in English. In this paper, censorship will specifically refer to that experienced by Internet users, unless otherwise specified. Our research does not quantitatively measure the prevalence of any given censorship method; it uses a qualitative approach, with case studies and a comprehensive survey of research papers, to provide a synthesis of the literature (see Section 5). Research, in and of itself, can reflect biases of the researchers conducting it. Researchers may perceive relevance or novelty of a particular topic area, and more citations pointing to a particular censorship method (see Table 2) may not reflect widespread use or imply its potential for significant impact to online communications.

4. Survey of internet censorship methods

4.1. HTTP/URL filtering

Uniform Resource Locators (URLs) were one of the early targets for filtering Internet content. URLs are defined in RFC 1738 (Masinter and McCahill, 1994) and consist of a protocol (e.g., http, https, ftp), subdomain (optional), domain name, top-level domain, and potentially a directory path and file name (e.g., https://testdummy.com/uploads/index.html). URLs direct web browsers and other applications to specific Internet resources. URLs can be restricted using URL blocklists that define restricted sites. An administrator can also use URL regular expressions (regex) to filter based on sets of characters or words.

URL filtering is done for many reasons. Companies may limit the types of websites that employees can access while working: some materials may be deemed inappropriate or pose a distraction in a workplace setting. Filtering may also be performed for security if the company subscribes to cyber threat intelligence (CTI) (Dykstra et al., 2022) feeds that provide blocklists of domains associated with malware. Public resources, such as libraries and Internet cafes, may limit the websites patrons can visit to comply with the laws of their jurisdiction (FCC, 2000; Dawn, 2010; FTC, 1998; Garcia, 2019; Gardner, 2000). Depending on the country and the situation, filtering online content may not be considered censorship — but from a technical perspective, the software and tactics for filtering content are the same. Sambaluk noted that "Students of technology history have long understood that technologies do not have sympathies and do not play sides or favorites... and they seldom voice a preference about who uses them" (Sambaluk and Spafford, 2020). This applies not only to privacy-preserving communication applications but also to cybersecurity controls. Controversially, multiple commercial products originating from the USA intended for commercial Internet filtering have been observed in use in nation-state censorship. For example, products such as Blue Coat have been identified in use in Burma, Egypt, Kuwait, Qatar, Saudi Arabia, and United Arab Emirates (UAE); McAfee SmartFilter has been used by Bahrain, Iran, Kuwait, Oman, Saudi Arabia, Tunisia, and UAE; and Netsweeper in Qatar, UAE, Yemen, and Pakistan (Dalek et al., 2013; Dalek and Senfit, 2011).

URL filtering can be performed locally or as traffic traverses a network. In the context of nation-state censorship, client-side filtering is rare, as managing configurations across numerous platforms (and gaining access to user devices) is difficult. Usually, a proxy, firewall, or middlebox performs network-based filtering upstream of many clients.

URL filtering relies on the ability of the censor to match the destination URL against a blocklist. Transport Layer Security (TLS) encrypts HTTP request and response contents, mitigating some basic URL-filtering mechanisms. Firefox Telemetry reported in October 2021 that 82% of global web traffic from the Firefox browser was encrypted using TLS (Let's Encrypt, 2021). Results for Japan and the United States were higher, at 86% and 92%, respectively. In October 2017, Google published a transparency report with an analysis of the top 100 most-accessed (non-Google) web pages globally, showing that all 100 had a modern TLS configuration allowing use of HTTPS, and 95 of the 100 sites directed users to HTTPS by default without user interaction (Google, 2017). This change improves the security and privacy of all Internet users and presents challenges to censors that rely on simple URL-filtering mechanisms to block unencrypted websites.

Despite these developments, some important web pages are still served as unencrypted HTTP (Hunt and Helme, 2021; HTTP Archive, 2024). The ease with which these connections can be manipulated or denied is seen as a problem by Internet freedom advocates. Efforts such as the "HTTPS Everywhere" campaign encouraged the use of TLS by default. Major web browsers (Google Chrome, Microsoft Edge, Mozilla Firefox, and Apple Safari) now have built-in functionality to upgrade connections where available (Hancock, 2021). In 2018, Troy Hunt launched a website to perform analysis on global web pages that do not automatically perform TLS redirection by default and offer resources to server administrators to help implement HTTPS at low or no cost (Hunt and Helme, 2021). Notably, projects such as *Let us Encrypt*, a non-profit certificate authority, provide X.509 certificates at no cost, regardless of which registrar maintains the domain (Internet Security Research Group, 2023). Let us Encrypt was founded by the

[3] According to RFC 9000 (Lyengar and Thomson, 2021), QUIC is the name of the transport protocol and is not an acronym.

[4] Available at https://censorbib.nymity.ch/

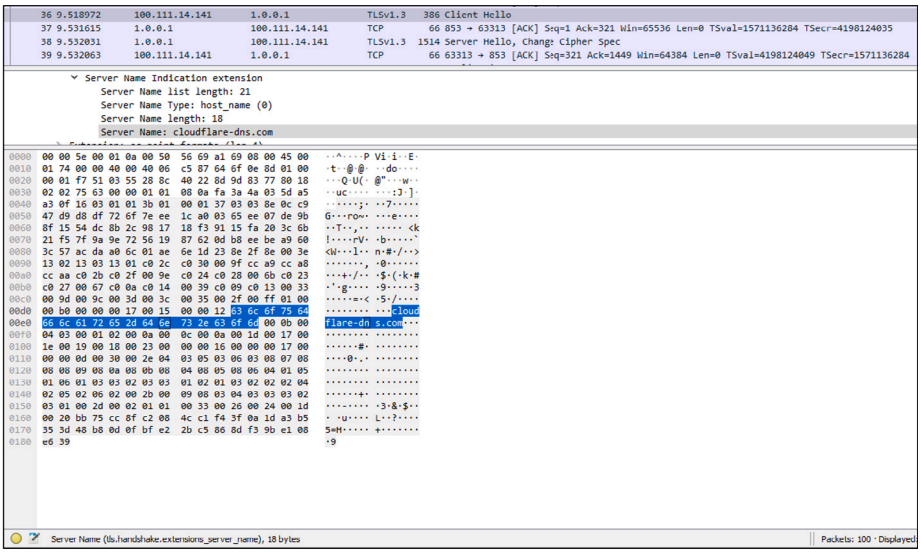

Fig. 1. Example plaintext SNI for cloudflare-dns.com; domain name shown in SNI extension within packet capture of TLS connection.

Internet Security Research Group and is credited with the widespread adoption of TLS over the past five years.

More advanced URL filtering approaches have also been observed. One way censors may disallow undesired HTTPS requests is by pattern matching against fields on the TLS certificate that are passed to the client. These will be transmitted in plaintext (unencrypted), and fields such as subjectAltName (SAN) or Common Name (CN) in the IP packet may contain portions of the URL or domain name (Palo Alto Networks, 2018a). However, this blocking method is prone to error. Certificate authorities differ in implementation as to what certificate fields contain, and shared domains could lead to over-blocking.

In addition to TLS, users in censored countries or filtered corporate environments have used proxies to evade filtering. Research has shown that at least tens of thousands of open HTTP/SOCKS proxies are available on the Internet to which any user may connect (Roberts et al., 2010). Many web browsers and Internet applications allow the manual entry of a proxy server. When users can initiate a connection to a proxy outside of the censor's influence, they may be able to bypass URL filtering; users may chain multiple proxies together to further obfuscate their traffic endpoints. However, these circumvention techniques can easily be thwarted if the censor requires that all connections to external Internet resources be negotiated through the censor's proxies.

A more robust censorship technique involves blocking based on Server Name Indication (SNI). SNI is an extension within the TLS protocol that helps a client to ensure that they are connecting to a web resource using the correct TLS certificate. This is necessary when a client reaches the IP address of a particular server but needs to ensure that it resolves to the correct host, especially on a server that hosts multiple domains. This scenario is commonplace on the modern Internet, with the rise of content delivery networks (CDNs) designed to place content topographically close to users to reduce latency (Gosain et al., 2021). SNI is transmitted in plaintext, and a censor with the capability to detect SNI using Deep Packet Inspection (DPI) can perform filtering based on it (Master and Garman, 2023) (see Fig. 1).

Several attempts have been made to increase the privacy of TLS. For example, in Fall 2018, Cloudflare proposed an extension to TLS named Encrypted Server Name Indication (ESNI). This extension would enable TLS 1.3 sessions to encrypt the SNI with a server's public key before sending it to the target (Ghedini, 2018). The approach caught the attention of some censors, as research revealed that the People's Republic of China had begun blocking all TLS 1.3 connections utilizing ESNI crossing the Great Firewall (Bock et al., 2020a). ESNI was not implemented on many production servers, and Firefox was the only major web browser to support it. In a Mozilla blog post in January 2021, Kevin Jacobs announced that Firefox would no longer support ESNI in favor of a new draft RFC in development for Encrypted ClientHello (ECH) (Jacobs, 2021). ECH would enable clients to encrypt the entire ClientHello of a TLS handshake (not only SNI), thus concealing the destination from an eavesdropping adversary. In 2023, Mozilla released a version of ECH in Firefox 118, and configured it to be on by default in Firefox 119 (Mozilla, 2023). Mozilla's version of ECH relies on DNS over HTTPS (see Section 4.2). This design decision shifts trust of name resolution to third-party providers (e.g., Mozilla, Cloudflare, NextDNS). In 2024, Firefox had less than 5% market share for web browsers globally (Statista, 2024); however, Google Chrome had the largest share in the user market in 2024.[5] Google developers have implemented their own version of ECH into Chromium (the codebase of Chrome) as of version 117 and subsequently turned it on by default for non-enterprise installations (Google, 2023). Despite these advancements, until ECH is ratified as an open standard by the Internet Engineering Task Force (IETF) and adopted by web servers around the world, censors will still be able to use SNI destinations against some users for censorship and allow for mass surveillance of web browsing activities.

4.2. DNS detection, manipulation, and denial

Another method widely used by censors is manipulation of the Domain Name System (DNS). As the "phonebook" of the Internet, the DNS standard (initially defined in RFC 882 and 883, superseded by RFC 1034 and 1035) matches human-readable domain names to IP addresses of web resources. DNS is an application layer protocol. DNS was not originally designed with security or privacy protections; the protocol is the topic of an entire body of literature on the DNS threat landscape, DNS research methods, and entities involved in DNS transactions (Khormali et al., 2021). Siby et al. have stated that "... virtually every connection to an Internet service is preceded by a DNS lookup" (Siby et al., 2020).

DNS requests pose several security and privacy considerations. Internet Service Providers (ISPs) can easily surveil users' Internet activity based on DNS. By default, most DNS requests are transmitted unencrypted. ISPs often provide DNS servers for customers to use and can monitor all requests. Even in cases with manually configured external

[5] https://gs.statcounter.com/browser-market-share#monthly-202401-202412

(a) Korean (b) English translation

Fig. 2. Example blockpage from the Republic of Korea (Retrieved April 01, 2024).

DNS servers, ISPs can "hijack" (Houser et al., 2021) unencrypted DNS requests and return an IP address of their choosing to the client (IVPN Limited, 2023; Preti et al., 2026).

Suppose that a censor is only concerned with monitoring activity. In that case, they may transparently proxy the results of manually configured DNS servers, logging the requests, and passing the results back to the client unaltered. A user may believe they are resolving DNS queries using a server of their choosing when the censor has transparently proxied the request and forwarded it along on the user's behalf. These tactics can facilitate surveillance or censorship based on domain queries. If a censor wants to implement a blocking action based on lists of domains (and the observed DNS requests are not encrypted), the censor has many options available. Requests that match selected material can simply be dropped, resulting in timeouts for the client. The censor can also tamper with the DNS result, inserting an IP address of their choosing and redirecting the client to it (Lowe et al., 2007). This could be used to display a "blocked content warning page" (referred to as a blockpage from this point forward), as some countries have demonstrated (Jones et al., 2014; Verkamp and Gupta, 2012). See Fig. 2 for an example blockpage. A more malicious adversary could use this tactic to redirect the user to download malware or present the user with disinformation or propaganda materials.

One countermeasure to DNS tampering is to manually define the DNS server for domain resolution. Naive censors will only filter requests they receive, and the user will be able to resolve IP addresses successfully. However, censor and filtering technologies have grown in sophistication — manually defined DNS servers are often not enough to avoid censorship. Even low-resource censors can block all DNS traffic except for their resolver, defeating this countermeasure.

Another countermeasure to DNS tampering is tunneling. Using an encrypted proxy (HTTPS or SOCKS) will obfuscate the request while it traverses the censor boundary, and the unencrypted DNS resolution will take place elsewhere on the Internet outside the censor's influence. Virtual Private Networks (VPNs) for personal use have increased in popularity to circumvent censorship and geographic area filtering for media content (Khan et al., 2018; Ramesh et al., 2022). Despite their initial purpose of providing an encrypted connection between two networks across the Internet, commercial providers are increasingly offering paid services to route traffic through their infrastructure. Several censors have taken notice. In particular, the People's Republic of China (PRC) banned non-state-sanctioned VPNs in 2018 (Reuters Staff, 2018), and the Russian Federation banned the use of several VPN services in 2021 (Trevelyan, 2022). VPN connections encrypt traffic between endpoints, allowing users to tunnel their traffic outside the censor's influence. Alternatively, they may use split-tunneling to selectively route only some of their traffic, such as DNS requests. Although VPN users may be able to connect to content they otherwise could not access, they are shifting trust from their ISP to the VPN provider.

Efforts are underway to improve the security and privacy of DNS as a whole. As early as 1997, work began on DNSSEC (Domain Name System Security Extensions) as a means to add authentication to DNS. DNSSEC adds public-key cryptography to the DNS lookup process. DNSSEC-compliant servers digitally sign DNS records and rely on a chain of trust similar to TLS certificate authorities.[6] DNSSEC ensures DNS replies have not been manipulated, which could serve as a countermeasure to DNS cache poisoning. However, it does not provide confidentiality, as the responses are still transmitted in plaintext and are subject to other censorship techniques. In 2013, researchers identified that only 0.15% of the top-level domains of ".com" used DNSSEC (Lian et al., 2013). Rijswijk-Deij et al. demonstrated how sites using DNSSEC could also be susceptible to packet fragmentation or amplification-based DoS attacks on their DNS traffic (van Rijswijk-Deij et al., 2015).

[6] DNSSEC extensions are defined in RFCs 4033, 4034, and 4035, and summarized in RFC 9364, available at https://datatracker.ietf.org/doc/html/rfc9364

Encryption of DNS can address some of the privacy and authenticity problems of the original protocol. Many public DNS services offer DNS over TLS (DoT) and DNS over HTTPS (DoH). Both have been used as countermeasures to DNS tampering. DoT and DoH encrypt DNS requests in transit and bypass the DNS resolvers of the service provider gateways (Siby et al., 2020). Several web browsers support DoH natively. However, there are challenges with implementation. Many Internet of Things (IoT) devices do not support encrypted DNS methods. The backward compatibility issue with many devices, firewalls, and routing equipment currently in production environments will also limit the adoption of encryption for DNS requests. Encrypting DNS also limits the visibility (and potential functionality) of cybersecurity tools that organizations may use to secure their enterprise. Additionally, DoT/DoH server endpoints have been targeted by censors in China, Iran, and Kazakhstan (Basso, 2021). When used in isolation, DoT and DoH do not fully address Internet privacy concerns, as censors can target other vulnerable aspects of a DNS request. However, DoT/DoH may be helpful if a nation-state only implements its censorship regime via domain name blocklisting.

4.3. IP address and port matching, blocking

A common form of Internet censorship is blocking based on Internet Protocol (IP) addresses. Censors can maintain blocklists of IP addresses associated with objectionable endpoints. Censor systems monitor traffic and drop connections when a blocked address is observed crossing the censor's boundary. Third parties can provide blocklists, or the censor can maintain their lists based on other content-matching efforts. IP address blocking can be resource intensive, as blocklists may grow large and become outdated as a result of the ephemeral nature of IP addresses (Xie et al., 2007). With the growth in the adoption of IPv6, these limitations will continue to increase. Despite these constraints, some nation-states choose to censor Internet traffic using IP blocklists — likely because of ease of implementation.

IP address spoofing can serve as a countermeasure to bypass censorship efforts. The IPv4 protocol lacks authenticity mechanisms in that senders (and network address translation nodes along a traffic path) assign the packet source address field (Benson, 2016). If a censor implements blocking based on source IP address, spoofing the address of an allowed endpoint may allow traffic that would otherwise be denied. However, source blocking is seldom used for large-scale censorship; censors often focus on the content to which they wish to deny access and apply blocking against all users within the censor's influence. Accordingly, few deployed anti-censorship tools attempt to implement IP address spoofing.

Censors may also choose to block Internet traffic by ports. Port blocking can be paired with IP address blocking or is done indiscriminately across all traffic. Many applications openly advertise their software's ports and transport protocols, and censors may wish to deny access to those specific applications, such as when the Burmese government blocked access to Skype in 2011 (McHugh, 2011). A more advanced blocking regime in Iran involving port blocking was revealed in 2020 by Bock et al. and the Open Observatory of Network Interference (OONI). Four Iranian ISPs were shown to have blocked port 853, associated with DNS over TLS, to many popular DNS providers (Basso, 2020) (in addition to tampering with TLS handshakes to those providers). Iran had attempted allowlisting particular ports (80, 443, 53 — HTTP, HTTPS, and DNS, respectively) in 2013 while blocking all other ports (Aryan et al., 2013) before abandoning the effort in the same year. In 2020, Bock et al. demonstrated that Iran had reimplemented what they called a "protocol filter" prior to their censorship apparatus. It filtered out all traffic except HTTP, HTTPS, and DNS before filtering based on content or destination (Bock et al., 2020b).

Traditional port blocking is an approach relying on software following common conventions. This is effective against applications that explicitly follow RFC specifications or their own conventions. However, transport layer protocols can easily use non-standard port mappings, and many applications do so. Most censors are unwilling to rely on allowlist filtering, given the large amount of collateral damage that would result in overblocking (Iran being a notable exception).

A 2021 study (Bock et al., 2021b) 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). Bock et al. observed this time-based approach to IP and port blocking in China, Iran, and Kazakhstan. More research is needed to determine if other nation-states are implementing similar functionality in their censorship systems.

Using high-number ports is a simple yet detectable countermeasure against censorship. By altering the listening port of a web application or service, censors that only filter based on static port numbers may be bypassed. This technique does not bypass censors that block/reject all traffic except for particular common ports and those that use allowlisting.

Censors may also use hybrid methods to deny undesirable traffic. By injecting an artificial TCP Reset (TCP-RST), network operators can cause an endpoint to shut down communication upon receipt (Weaver et al., 2009; Nourin et al., 2023a), as defined in RFC 793 and RFC 1122 (DARPA, 1981; Braden, 1989). It is a normal element of TCP/IP functionality for connection timeouts and non-existent TCP endpoints, among other uses. Censors can pair identification techniques (such as those discussed in Section 4.1) with a TCP Reset to obscure the fact that censorship is occurring. Users may attribute a web browser message or software error to poor network service rather than deliberate censorship. TCP Resets have also been misused to orchestrate distributed denial of service (DDoS) attacks[7]; we discuss these in detail in Section 4.8.

The complexity of the Internet has complicated the job of administrators ensuring the availability of systems as well as censors hoping to deny access to particular content. An example is content delivery networks (CDNs), designed to provide access to web resources as close to the user as possible to reduce latency (Gosain et al., 2021). Censors have caused extensive collateral damage in overblocking by denying access to the IP address space of large CDNs (McDonald et al., 2018). A particularly salient example of inadvertent censorship is the PRC's blocking of Google Scholar. Despite it being considered a valid academic resource and legal service by CCP governmental regulators, the Great Firewall filters traffic destined for Google.com based in the U.S. (Lu et al., 2017). Legal frameworks and technical implementations change over time and often conflict.

Tunneling has repeatedly demonstrated its effectiveness in circumventing IP and port blocking. Because the encrypted tunnel obfuscates the metadata of the IP packets, many blocking efforts are thwarted. However, encrypted proxies, VPNs, and anti-censorship tunnels still suffer from the bootstrapping problem (Winter, 2014) — motivated censors will use their resources to prevent the tunnel's initial establishment. These techniques often include simple endpoint IP or port blocking, DNS filtering, and deep packet inspection approaches.

4.4. Deep packet inspection and protocol fingerprinting

In response to the success of early circumvention tactics, some censors sought advanced capabilities to detect undesirable Internet traffic. As the name suggests, deep packet inspection (DPI) allows searching of payload content in data packets (Sherry et al., 2015). In an IP packet, the IP header is followed by the packet's payload. A payload consists of the transport, session, presentation, and application (layers 4–7 of the OSI model) data of the communication (see Fig. 3). DPI is frequently

[7] https://www.akamai.com/glossary/what-is-a-tcp-reset-flood-ddos-attack

used in cybersecurity contexts by system administrators. DPI-enabled network devices can "be programmed to detect certain bit sequences associated with known malicious code" (Green, 2015) from large lists of indicators of compromise (IOCs) provided by security tool vendors, threat intelligence sharing feeds, or freely available online. However, any tool that assists with identifying or classifying traffic can also be used to identify content for censorship.

In the context of censorship, DPI allows for content matching, such as with keywords of prohibited materials. While still applicable for Internet censorship, the large-scale proliferation of encryption across many Internet resources (Let's Encrypt, 2021) has rendered simple content matching obsolete in many protocol exchange scenarios. Additionally, many anti-censorship solutions implement encryption at multiple layers to protect traffic confidentiality and thwart simple content filtering.

DPI is often considered expensive in terms of computing costs, as well as challenging to implement on high-speed network systems (Van Leeuwen et al., 2019). However, the potential of DPI based on heuristic or machine learning techniques remains. Open-source DPI tools are increasing in sophistication and accuracy. The project ntop maintains a software fork of OpenDPI named nDPI, which includes the flow signatures of hundreds of protocols and applications (ntop, 2022). Some commercial firewalls (e.g., Palo Alto, Fortinet FortiGate, Forcepoint) already claim to be able to filter data from applications on a network (Forcepoint, 2023; Fortinet, 2021). Palo Alto has a blog post guide for their customers on all the steps to block Tor using their product (Palo Alto Networks, 2018b). The most aggressive nation-state censors have shown an increased willingness to implement DPI (Master and Garman, 2023).

Some anti-censorship software developers and researchers have implemented countermeasures against deep packet inspection. One approach is to completely randomize the payload to make the traffic "look like nothing" (Dixon et al., 2016). This is the approach taken by "obfs" tools such as Dust (Wiley, 2011) and ScrambleSuit (Winter et al., 2013). These pluggable transports were initially created for integration with Tor or the Tor Browser, allowing some censored users to overcome censor blocks on their first hop. This approach makes inherent assumptions about the adversary in that they only operate against blocklists. If a censor uses an allowlist to define "known good", randomization methods fail.

Other approaches involve mimicking the payloads of other data protocols (dubbed "mimicry" approaches), such as StegoTorus (Weinberg et al., 2012) for HTTP, SkypeMorph (Mohajeri Moghaddam et al., 2012) for Skype, and CensorSpoofer (Wang et al., 2012) for SIP-based Voice over IP. This approach has been criticized by Houmansadr et al. as "fundamentally flawed", as any slight variation not imitated by the spoofing software can allow a determined censor to detect the anomaly and block the traffic (Houmansadr et al., 2013). Balboa works as middleware and attempts to overcome the shortfalls of mimicry approaches by using standard outputs of existing software and injecting traffic into allowed TLS streams (Rosen et al., 2021). Newer approaches, such as format transformation encryption (FTE), claim that observation-based FTE steganography can be used as an undetectable covert channel (Oakley et al., 2020).

Overall, pluggable transports have become important tools supporting bootstrapping of anti-censorship tool connections. Projects other than Tor have begun to integrate pluggable transport compatibility in their software (obfuscation group, 2015).

Advanced censors have taken additional steps to deny access to anti-censorship, VPN, and other encrypted communication methods. Active probing by the Great Firewall of China has been shown to routinely target Tor bridges (Winter and Lindskog, 2012), as well as SSH (Nixon, 2011) and VPN endpoints (Nobori and Shinjo, 2014). Active probing involves the censor masquerading as a user and attempting to connect to the circumvention service. The probe observes how the service responds. If the censor's probe determines that the server is running

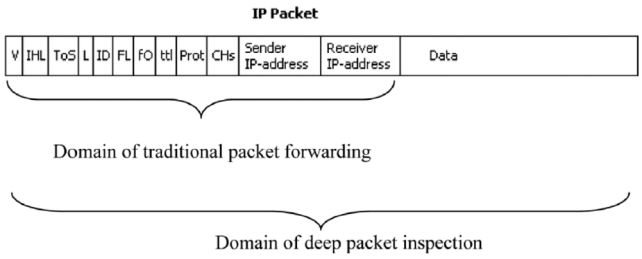

Fig. 3. DPI Diagram from Bendrath and Mueller (Bendrath and Mueller, 2011).

an "undesirable" service, the censor can take a blocking action, such as adding the server to an IP blocklist. The "cat-and-mouse" game has continued, as researchers have studied active probing methods and offered solutions to anti-censorship developers to evade active probing (Frolov et al., 2020; Frolov and Wustrow, 2020).

Tor Browser uses obfs4 as its default pluggable transport. Previous versions of obfs were vulnerable to active probing by the GFW of China. Every obfs4 server has a per-bridge secret, and a client must prove knowledge of this secret before gaining access to the protocol. This defeats automated methods of active probing as the censor would need the same out-of-band information as a legitimate client to detect a hidden Tor bridge (Fifield and Tsai, 2016). Another pluggable transport approach, Meek, uses a routing method known as domain fronting (Fifield et al., 2015) to direct first-hop traffic under the cover of HTTPS to a CDN provider domain that is unlikely to be filtered. Psiphon and Tor include Meek implementations. However, domain fronting has faced significant challenges; developers who relied on Google or Amazon CDNs for cover traffic no longer function after those companies reconfigured their cloud implementations to prevent domain fronting (Matan Mates, 2022).

Some newer anti-censorship tools leverage techniques to bypass less aggressive censors that only use DPI blocking (and no other combinations of network filtering). Software such as GoodbyeDPI (GoodbyeDPI, 2017) and a related fork named PowerTunnel (PowerTunnel, 2023) allow users to access DPI-blocked content without other privacy protection mechanisms. These tools are sometimes referred to as "serverless" because they do not rely on an external entity for their functionality. The software creates a local proxy server on the client machine and funnels/manipulates HTTP(S) traffic before it is transmitted over a network interface. Several clever manipulations, such as TCP-level fragmentation of first packets, replacing "Host" header values, adding additional spaces in URIs, mixing letter cases of header values, and fake TTL/sequence/acknowledgment numbers have been demonstrated to fool some DPI implementations.

Encryption does not solve all DPI-based censorship problems; many open research problems related to censorship assume an adversary with advanced DPI capabilities. Some advanced DPI systems characterize traffic from particular applications or protocols, even when the traffic is encrypted. These "fingerprints" or signatures can then be used to determine when users are attempting to use a specific piece of software, despite encryption. One identification technique involves examining the initial unencrypted initiation of an encrypted network stream. Protocol header metadata can often reveal the types of encryption implemented or versions of software applications. A comparison of the available DPI systems that perform this analysis is available at Bujlow et al. (2015).

More sophisticated methods of ETA involve identifying particular byte sequences or patterns in overall encrypted traffic streams to allow for the identification of an application or protocol. The methods may rely on statistical models to identify behavioral changes in bitstreams. Other approaches involve training a machine learning (ML) classifier. The algorithm uses a known "baseline" compared to a bitstream

containing a targeted protocol's traffic to observe patterns or identify anomalies. A survey of methods for encrypted traffic classification by Velan et al. is available in Velan et al. (2015).

An example of pattern or behavioral-based blocking is the denial of secure messaging apps such as Signal (Kadak, 2018). Blocking of Signal has been observed in Iran, China, Cuba, and Uzbekistan (Xynou and Filastò, 2021). More commonly, these nations use techniques such as DNS manipulation (Iran, China) or DPI targeting SNI fields in a TLS handshake (Cuba, Uzbekistan), likely because they require fewer resources. In 2021, the Russian Federation demonstrated hybrid censorship approaches using SNI targeting with DPI and bandwidth throttling to achieve censorship goals against Twitter, discussed in detail in Section 4.6.

4.5. BGP attacks and disruption

Border Gateway Protocol (BGP) is one of the critical components that allows the Internet to function as a network of networks. Several protocols operate at layer 3 of the OSI model, allowing connectivity among devices worldwide. At the highest levels, the Internet Assigned Numbers Authority (IANA) assigns blocks of IP addresses to regional Internet registries (RIRs). RIRs allocate blocks to organizations such as Internet Service Providers (ISPs), technology companies, universities, government agencies, and scientific institutions. These large organizations often serve as an Autonomous System (AS) for the purposes of routing Internet traffic. Each AS is assigned an autonomous system number (ASN), which is unique and used by BGP to determine how ASes communicate with one another. For example, AS17 is assigned to Purdue University, which manages the following sets of IPv4 addresses: 128.10.0.0/16, 128.210.0.0/16, 128.211.0.0/16, 128.46.0.0/16, 149.164.0.0/16, 163.245.0.0/16, 192.31.0.0/24, 204.52.32.0/20, 204.52.48.0/20, 205.215.64.0/18, 69.51.160.0/19, and also IPv6 blocks 2001:18e8:800::/44 and 2607:ac80::/32 (Hacker Target, 2022).

There are approximately 64,000 ASNs in use worldwide, with continuous growth (Cloudflare, 2018b), and BGP (versions 4 and 6) are the protocols that allow them to communicate with each other. "DNS tells you where you're going, and BGP tells you how to get there" (Clark, 2021). Although BGP is intended to provide the most efficient routing options available between ASes, there are many associated factors beyond counting the lowest number of router hops between one source IP address and its destination. Factors such as cost of use and physical distance of transport media complicate routing decisions.

In addition to routing complexity, the design choices made when creating BGP have implications for the security and availability of the global Internet. The protocol assumes that advertisements from interconnected networks are truthful about the IP addresses they own. "BGP hijacking" attacks are nearly impossible to prevent (Cloudflare, 2018a). An attacker may choose to advertise a route for a smaller range of IP addresses than other ASes have previously announced. Another attack involves offering a shorter route to particular blocks of IP addresses. Both allow the attacker to divert large swaths of Internet traffic in a direction of their choosing. To conduct a BGP hijack, the attacker must be an AS administrator or take control of an AS system. This limits the scope of who might perform such attacks but does not rule out nation-states or large technology corporations from using these methods to deny access to information.

There have been several BGP-related incidents. In 2004, a Turkish ISP named TTNet (AS9121) inadvertently modified its configuration to include a full table of entries (>100k). This modification effectively advertised AS9121 as the shortest route to most of the Internet's addresses (Underwood, 2005). For several hours, users worldwide could not access some or all websites because of routing errors. In February 2012, a network operator named Dodo announced internal BGP routes to Telstra, a major ISP in Australia. Telstra incorrectly accepted the routes and caused routing bottlenecks throughout the country. This error resulted in most Australians losing online connectivity for 30 min. A similar outage event occurred in August 2012 in Canada, known as the "Bell-Dery" routing leakage incident, after Dery Telecom leaked a full BGP table of routes to Canadian ISP Bell (Benson et al., 2013). In 2021, Facebook (now Meta) suffered a global outage partially caused by BGP route errors. During routine maintenance, an engineer accidentally disconnected Facebook's backbone data centers. Failover systems, unable to communicate with backbone infrastructure, withdrew IP address blocks from their BGP advertisements. As BGP routes propagated and DNS server caches worldwide expired, all of Facebook's subsidiary services — Instagram, WhatsApp, Messenger, Mapillary, and Oculus — were inaccessible (Janardhan, 2021). The company restored services in six to seven hours but at enormous business and advertising costs.

Malicious BGP-related incidents have also occurred. In 2008, Pakistan Telecom (AS17557) allegedly published an unauthorized BGP announcement of the prefix 208.65.153.0/24 to attempt to censor YouTube from its citizens (RIPE NCC, 2008). This effort temporarily hijacked all YouTube traffic on a global scale, denying access to all users for part of the day on 24 February 2008, until appropriate routes were restored. In 2011, the government of Libya used BGP routing to implement an Internet shutdown on most of its country's users in response to a series of uprisings in the region. A single state-operated AS routed most traffic in Libya at the time, allowing it to withdraw routes and disrupt network connectivity (Dainotti et al., 2011). On February 5, 2021, after the Burmese military overthrew the government of Myanmar in a coup d'état, the junta compelled Campana Mythic (AS136168) to announce the 104.244.42.0/24 prefix, which belonged to Twitter. The junta may have intended to blackhole all Twitter traffic within their borders. The route leaked to the global Internet, making AS136168 appear to own the IP address space, disrupting traffic in Singapore and other Southeast Asian nations (Padmanabhan et al., 2021). Other examples have resulted in monetary lossed due to criminal activity. In 2018, Russian AS48693 and AS41995 advertised IP blocks that belonged to Amazon Route53 DNS services from the provider eNet (AS10297) of Columbus, Ohio, USA (Poinsignon, 2018). Criminals forged a fake version of a web-based Ethereum wallet service[8] and stole approximately $152,000 worth of cryptocurrency. In 2022, a sophisticated supply chain attack on a Korean cryptocurrency exchange platform (involving BGP hijacking perpetrated by AS9457) also resulted in the theft of approximately $1.9 million (₩2.37 trillion KRW) (Cimpanu, 2022).

The threat of abuse with BGP manipulation has motivated proposals for security enhancements (Mitseva et al., 2018). However, BGP attacks have not been used in practice as an intentional technique for routine censorship. Instead, other methods with less collateral damage are used. There are few countermeasures against BGP-related disruptions, given the design of the BGP protocol. International economic and political pressure dissuades malicious actors from abusing BGP routing.

4.6. Bandwidth throttling

Bandwidth throttling involves a deliberate slowing of communication speed. In the context of computer networks, throttling can occur at the application software or network management levels. Throttling Internet traffic has been considered for use during periods of high usage. During the global COVID-19 pandemic, governments in Europe and technology companies in the U.S. recommended using bandwidth throttling and traffic shaping techniques to manage the large-scale throughput increases brought on by stay-at-home orders and remote work requirements (Kang et al., 2020). However, throttling often arises in debates surrounding "net neutrality", a network design principle that states that all data packets should be treated equally regardless of their content, sites, and platforms (Wu, 2003). Network neutrality is a

[8] https://www.myetherwallet.com/

contentious topic. It has been interpreted and implemented differently and has faced legal challenges in multiple countries. Proponents of network neutrality claim that traffic on the open Internet should be freely accessible, while opponents claim that prioritizing particular services creates a better user experience.

In the context of censorship, bandwidth throttling has been used to suppress access to information. Throttling provides some deniability on the part of the censor, differentiating it from other methods of Internet censorship. In Iran, the government slowed Internet speeds nationwide in the lead-up to a presidential election in 2009 (Anderson, 2013) and 2013 (Esfandiari, 2013), as well as other periods of political unrest (Center for Human Rights in Iran, 2018). The Russian Federation has deployed selective throttling (Xue et al., 2021). In March 2021, the Russian government started limiting the speed of connections to Twitter. Russia had previously requested that Twitter remove content it deemed illegal or objectionable, and until then Twitter had refused to comply. Roskomnadzor issued a statement confirming that it ordered the throttling of Twitter traffic until the company complied with its approximately 28,000 removal orders (Roskomnadzor, 2021). Xue et al. discovered that Russian ASes used deep packet inspection to detect SNI within TLS connections specifically for Twitter and its subdomains (twitter.com, t.co, *.twimg.com). If detected, connection speeds were reduced to between 130–150 kilobits per second (kbps). Twitter eventually removed 91% of the requested content, and some of the throttling measures were lifted (Xue et al., 2021).

Taye described several techniques that governments use to throttle Internet connectivity (Mühlenmeier, 2020). First, traditional bandwidth management, such as traffic shaping and policing, can slow objectionable traffic. This can be done based on source or destination IP ranges, virtual local area networks (VLANs), or media access control (MAC) addresses. Second, censors can implement quality of service (QoS) restrictions in network traffic. QoS is typically used to prioritize low-latency traffic, such as voice calls. For censorship, QoS can deprioritize particular kinds of undesirable traffic. Third, inline DPI systems can be used to artificially add latency. Finally, censors can manually alter routing paths at their border gateways to limit traffic. They can change routing paths to be longer, adding latency. Or censors can direct specific traffic through lower capacity links, serving as a chokepoint to delay or halt traffic flows.

There is currently little anti-censorship research dedicated to the study of bandwidth throttling. There are no purpose-built tools to counteract this kind of censorship method. Anecdotes online suggest that commercial VPNs may bypass ISP throttling, depending on how the throttling is implemented (FireninjaDD, 2017). Xue et al. offered several countermeasures against Russia's throttling of Twitter, such as TCP-level fragmentation and TLS packet stuffing — or more traditional anti-censorship methods, such as encrypted proxies or VPNs — which defeated Russia's detection method (Xue et al., 2021). More research and development are needed in this emerging area of censorship studies.

4.7. Internet shutdowns

Even as societies around the world increasingly rely on Internet connectivity for economic, financial, and social functions, some governments have increased efforts to deny Internet access to their citizens. 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" (Feldstein, 2021). Authorities have used network disruptions to "quell mass protests, forestall election losses, reinforce military coups, or cut off conflict areas from the outside world. Data from the past few years documented incidents of global shutdowns: 196 documented incidents in 2018, 213 incidents in 2019, and 155 in 2020... [and] Government-instigated internet shutdowns largely took place in relation to five event types: mass demonstrations, military operations and coups, elections, communal violence and religious holidays, and school exams" (Feldstein, 2022). Shutdowns may be implemented for minutes, hours, or more. Authorities may assert that their sovereignty grants them the right to control Internet access as they see fit; others cite the need to counter threats to public order, challenges to national security, or moral degradation of their populace. These justifications are often incongruent with international norms. The United Nations Human Rights Committee has stated that "The right to access and use Internet and other digital technologies for the purposes of peaceful assembly is protected by Article 20 of the Universal Declaration of Human Rights and Article 21 of the International Covenant on Civil and Political Rights" (Human Rights Council, 2021, 2020). Protection of freedoms of expression and association is often cited as obligations within international human rights law. A plurality of nations across the ideological spectrum agree, but not always in practice. Internet shutdowns often lead to unintended consequences for Internet censors and society at large. From an economic perspective, researchers estimated $5.62 billion dollars of financial impact on the global economy in 2021 as a result of Internet shutdowns (Woodhams and Migliano, 2022).

One of the most cited incidents of Internet shutdown efforts occurred from December 2010 through the end of 2012 in western Asia and northern Africa. Known as the "Arab Spring", these events were a series of anti-government protests, uprisings, and armed rebellions in Tunisia, Egypt, Libya, Yemen, Syria, and Bahrain. The overthrow of several heads of state and some governmental reforms occurred as a result. Demonstrations took place in the streets of Algeria, Iraq, Lebanon, Jordan, Kuwait, Morocco, Oman, and Sudan, while minor protests also occurred in Djibouti, Mauritania, Palestine, and Saudi Arabia (Ruthven, 2016). Citizens (often youth or union groups) protested the corruption of political leaders, governmental abuse of power, economic stagnation, extreme poverty, and unemployment. The more authoritarian regimes among these nations took multi-pronged approaches to quell rebellion, including police and military mobilizations against their populations. Social media platforms were cited as a means of mobilizing collective action during Arab Spring protests, and circumventing traditional media and means of communication typically controlled by censoring states (Albany Associates, 2012; Wright, 2011). According to some, the impact of Facebook and Twitter during the uprisings has been overstated by popular media (Bruns et al., 2013). However, several regimes deemed Internet connectivity important enough to the protesters' causes to selectively deny online access to prevent communication or the spread of information (Woodcock, 2011).

In 2013, Shavitt and Zilberman published an analysis of Internet shutdowns during the Arab Spring, specifically in Egypt, Libya, and Syria (Shavitt and Zilberman, 2012). Using combinations of BGP advertisements and altering default IP routing, each country (at different times and to varying degrees) effectively stopped meaningful resolution of TCP/IP connections throughout regions of their country. Attempts to deny all access to Internet endpoints were relatively straightforward, especially in a small nation such as Syria, which had only one autonomous system controlled by the government (Chaabane et al., 2014). The denial of Internet access may have hampered some protestor mobilization efforts while simultaneously fueling the discontent of Arab youth by disrupting their access to Internet content.

Internet shutdowns have occurred in many countries since the Arab Spring events. Censoring nation-states have diverse geopolitical and social systems and widely varying legal systems. However, controlling access to information is increasingly essential to shaping political narratives. India, the largest self-proclaimed democracy, had 132 regional Internet shutdowns in 2020 (Software Freedom Law Centre, 2020). Politicians in India use shutdowns as a tool of governance under the auspices of countering misinformation and disinformation (sometimes termed "fake news"). These leaders cite national campaigns such as "Digital India", intended to use connectivity to promote

prosperity and wealth accrual. Shah argued that their efforts do not stop fake news stating "...as infrastructural tools, they enable state (dis)information and propaganda to spread without resistance and thus become potent tools in curbing protests and rightful critique of authoritarian practices" (Shah, 2021). Shah also argued that given the patchwork nature of ISP infrastructure and implementation, "shutdowns as a way of regulation and governance are both ineffectual and counterproductive" (Shah, 2021).

In 2019, in response to large anti-government demonstrations against rising gasoline prices, Iranians experienced a several-day Internet blackout (Newman, 2019). In November 2020, Myanmar held national elections in which the candidate for the National League for Democracy Party, Win Myint, won the presidency. The Tatmadaw (Burmese military forces) staged a coup d'etat on 01 February 2021, rejecting the election outcome and installing a military junta in place of Myanmar's elected government (Ryng et al., 2022). In addition to violence, search and seizures, arrests of dissidents, and legal changes to quell dissent, the government blocked social media platforms (Facebook, Twitter, and Instagram) to limit access to information and assembly. Restrictions escalated as protests increased, and nightly shutdowns occurred throughout February and March. Censorship efforts culminated in a near-total Internet shutdown on 02 April 2021 (Januta and Funakoshi, 2021). The junta ordered telecommunications companies to disconnect connectivity to mobile and wireless Internet customers, the only services available in the country to access the Internet. Although Internet penetration rates in Myanmar were only 35% in 2020 (The World Bank, 2022), the censorship measures implemented are some of the most draconian observed in this century and have spurred debate about free expression, freedom of assembly, and free access to information (United Nations, 2021).

Researchers have noted that despite the recent increase in Internet shutdown events, many governments have opted to selectively block (or throttle) individual content or platforms (Feldstein, 2022). Rather than total shutdowns, authorities have attempted to avoid a more potent political backlash from their citizens or the international community with selective filtering. More sophisticated censorship methods — as described in previous sections — sometimes offer ambiguity or minimize the likelihood that users will attribute their lack of access to censorship. Network throttling may be blamed on slow or inconsistent ISP connectivity, targeting of a social media platform in short bursts may be viewed as a platform's technical issue, and URL/DNS filtering (that does not present a blockpage but an HTTP error or TCP timeout) might be shrugged off as poor cellular service. Time-based Internet censorship is an important trend for researchers and activists to monitor. As nation-states demonstrate a willingness to use hybrid methods and timing to achieve their goals, anti-censorship software developers (Dingledine et al., 2004; Xue et al., 2024; Pereira, 2024; Lamansky, 2024; Husaini, 2024; Wang et al., 2023; Winter, 2014) remain adaptive in their approaches to circumvent censorship where it occurs.

4.8. Computer network attacks and resource exhaustion

The study of computer network attacks (CNA) and exploitation has been the subject of cybersecurity research over the years. Subtle methods have been used for cyber espionage, in which a nation-state or non-state actor infiltrates an adversary's network to obtain information for economic, military, or political gain. Subtle and overt methods of cyber attack are also used in the conduct of cyberwarfare, in which one actor destroys, denies, disrupts, deceives, degrades, or manipulates (U.S. Strategic Command, 2009) their targets' computing systems in pursuit of their objectives. Private sector actors often focus their efforts on the World Wide Web to address denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. Both are forms of resource exhaustion that deny access to services by overwhelming target servers.

DDoS attacks have dominated the computer security literature over the past several decades (Loukas and Oke, 2010; Mahjabin et al., 2017; Manavi, 2018; Mirkovic and Reiher, 2004; Tripathi and Hubballi, 2021; Zargar et al., 2013), given the scope and scale of the attacks and their economic impact. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) defines a DoS as an attack that "occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is achieved by flooding the target host or network with traffic until the target cannot respond or crashes, preventing access for legitimate users" (CISA, 2009). DDoS attacks are similar in intent but utilize a distributed system of many computers as the source of the superfluous traffic. This allows the attacker greater anonymity and larger amounts of attack traffic, making a defender's job of mitigating the attack more difficult. Participants in DDoS are often unwitting, as their devices may have been infected with malware that surreptitiously joined the attacker's botnet.

From a technical perspective, DDoS attacks can be broadly classified into network-layer and application-layer attacks. Network-layer attacks generally involve flooding a victim's network bandwidth to exhaust its resources; traffic could be UDP streams, ICMP flooding, DNS traffic flooding, VoIP flooding (Amalou and Mehdi, 2022), or other protocols. Application-layer attacks, higher in the OSI model, are protocol-specific and exploit a bug or particular feature of a protocol implementation to consume resources; TCP SYN flooding, TCP SYN-ACK flooding, ACK & PUSH ACK flooding, or RST-FIN flooding (Zargar et al., 2013) are examples. Reflection-based attacks involve spoofing the source of a message, so not only does the victim interact with the flood of traffic, but also the spoofed source, which is now involved when the victim replies. Amplification-based attacks rely on external services to help create additional traffic, "amplifying the message" (Tripathi and Hubballi, 2021). They may exploit an IP broadcast feature of a network device to reduce the effort an attacker must expend to attack their targets. Reflection and amplification attacks are present in the application layer but occur using protocols such as HTTP or database queries (e.g., SQL). An analysis of application-layer DDoS attacks is available in Tripathi and Hubballi (2021), as is a more general taxonomy of DDoS attacks and defense mitigations in Mirkovic and Reiher (2004).

DDoS attacks have not been observed as a routine method of Internet censorship by nation-states against users. This is likely because of the nature of the attack techniques used. DDoS attacks are effective against large, centralized services and may deny access to the network for all users. Other methods, such as Internet shutdowns, would be used instead for censorship. Zargar et al. characterize the motivations of DDoS attackers into five categories: financial/economic gain, revenge, ideological belief, intellectual challenge, and cyberwarfare (Zargar et al., 2013). Attribution of blame for the conduct of DDoS attacks is also a difficult problem. Nation-states, governmental proxy groups, criminals, and Internet activists (or "hacktivists") (Sauter, 2014) have used DDoS attack techniques to achieve their goals.

There are dozens of examples of DDoS attacks linked to cybercrime or cyberwarfare since the early days of the world wide web. In 2000, a fifteen-year-old using the online handle "Mafiaboy" (he was later revealed to be a Canadian named Michael Calce) compromised computer systems at several universities and used them to conduct DoS attacks. The attack brought down the websites of Yahoo!, CNN, eBay, Dell, Amazon, and E*Trade, and the litigation that followed inspired first-of-their-kind cybercrime laws across several countries (Brenner, 2007; Hersher, 2015).

In April 2007, the national government of Estonia was the victim of a campaign of DDoS attacks targeting government services, banking systems, and media outlets. The attacks roughly coincided with the relocation of a memorial statue, the "Bronze Soldier of Tallinn", which

was perceived by ethnic Russians living in Estonia and Russia as an affront to their sacrifices during World War II (Clarke and Knake, 2012). The economic damage resulting from system downtime and societal disruption was estimated to cost tens of millions of Euros (Watney, 2014). The campaign against Estonia has been cited as the second state-sponsored act of cyber warfare (the first being a series of coordinated cyberspace operations, dubbed Titan Rain, against the U.K. Defense Ministry and U.S. Defense Intelligence Agency (DIA) beginning in 2003 (Council on Foreign Relations, 2005)).

In 2008, coinciding with an armed attack against Georgia by the Russian Federation, large-scale DDoS attacks began against Georgian web pages (Tikk et al., 2008). The targets included the Georgian president's website, government ministry pages, and news agencies. While the Russian government may have benefited from the disruption, evidence suggests that the attack resources were crowdsourced from underground hacker communities sympathetic to the Russian cause (Tikk et al., 2008). There is no published evidence of whether the attackers were encouraged, endorsed, coordinated, or resourced by the state. Other large-scale DDoS incidents were documented in 2013 against Spamhaus (an email spam tracking organization), in 2015 and 2018 against GitHub (an open-source software distribution platform), and in 2016 against Dyn (a major DNS provider) (Cloudflare, 2024). The Mirai botnet targeted Dyn using compromised Internet of Things (IoT) devices to attack its victims, denying Internet access to many users on the east coast of the United States on 12 October 2016.

In 2017, the U.S. government released a report documenting malicious cyber activity performed by the government of North Korea. The report outlined the activities and capabilities of the Lazarus Group (aka HIDDEN COBRA, or APT38 by Mandiant). The organization was the same group responsible for global computer disruption with their release of the WannaCry malware in 2016 (U.S. Army, 2020; Greenberg, 2017). Among the malware analysis and IOCs in the report, a tool called DeltaCharlie was revealed to have been used for DNS, NTP, and carrier-grade NAT DDoS attacks (CISA, 2017). Lazarus Group likely perpetrated DDoS and offensive cyberspace operations campaigns against South Korean media, financial institutions, and critical infrastructure in 2011 and 2013 (Zetter, 2016).

In 2020, Google disclosed that in 2017 its cloud services infrastructure was the target of a 2.54 terabyte per second DDoS attack originating from four Chinese ISPs (Menscher, 2020; Cloudflare, 2024). A series of attacks, including the "Mantis" attacks, were targeted at Google infrastructure (Kiner and Konduru, 2022; Yoachimik, 2022). Another attack against Google cloud services in August 2023 reached a peak of 398 million requests per second, nearly 7.5 times larger than the 2020 campaign (Kiner and April, 2023). Cloudflare reported mitigation of the largest DDoS attack recorded in history in 2024, with a peak of 666 million packets per second (Cloudflare, 2024); the targets of the broader campaign were primarily banking and financial services, most of which were located in China.

The literature has documented several DDoS attacks that appear to represent Internet censorship. These attacks are attributed to governmental entities or proxies of that nation-state and tend to target a particular web page or Internet resource they oppose. Notably, DDoS attacks restrict access to Internet resources for *everyone*, not only users within the censor's sphere of influence. After the Snowden classified document leaks of 2013, media outlets reported that the United Kingdom Government Communications Headquarters (GCHQ) intelligence service had conducted DDoS attacks against servers hosting IRC chat services used by members of the hacktivist group Anonymous in 2011 (Greenwald, 2014). Concern among Western nations arose from the incident as the use of the TCP-SYN flooding capability (dubbed "Rolling Thunder") may have "chilled" the speech of uninvolved users of the same servers.

DDoS-related censorship has often been shown to originate from Chinese ASes. On 16 March 2015, greatfire.org observed via their Amazon CloudFront hosting service that their website was under attack by a DDoS and their hosting costs had increased to $30,000 per day because of the added throughput (Smith, 2015). Later the same month, two GitHub pages affiliated with their project were also targeted. The organizers of greatfire.org offer resources to Chinese nationals looking to circumvent censorship within PRC. Baidu servers were identified as the source of much of the DDoS traffic, although the company denied involvement. Researchers dubbed the attack tool used during the incident the "great cannon" of China and advised that its overt deployment represents an escalation of state-level information control (Marczak et al., 2015b,a). The same paper alleges a capability called QUANTUM, maintained by the U.S. National Security Agency (NSA) and U.K. GCHQ, which similarly abuses plaintext HTTP traffic as a "man-on-the-side" attack for exploitation rather than DDoS.

Another example of politically motivated DDoS attacks happened in Southeast Asia in recent years. On 27 February 2022, CNN Philippines journalists were preparing to cover a presidential candidate debate when their website went down because of a DDoS attack (Gavilan, 2022). Guest writes, "Since June 2021, opposition politicians, independent media, and fact-checking websites in the Philippines have been hit over and over with brute-force cyberattacks known as distributed denial-of-service, or DDoS, attacks. CNN, major news network ABS-CBN, Rappler (the outlet founded by the 2021 Nobel Peace Prize winner Maria Ressa), and VERA Files, a fact-checking organization, have all been targeted, along with the website of Vice President Leni Robredo, who is a staunch critic of the current president, Rodrigo Duterte" (Guest, 2022). A Rappler journalistic investigation noted that a local Filipino hacking group called Pinoy Vendetta claimed credit for some of the attacks. A government report from the US-CERT (United States Computer Emergency Readiness Team) identified source IP addresses affiliated with the Philippine Army associated with DDoS attacks on two independent media sites, AlterMidya and Bulatlat (AlterMidya, 2021). Definitive attribution of DDoS attackers is difficult, and it is unclear whether some attacks denying access to political commentary in the Philippines were carried out by a nation-state actor.

A 2009 book chapter specifically analyzing DoS attacks with political motivations suggests that most DDoS attackers online are non-state actors (Nazario, 2009). A study in 2020 evinced that authoritarian states are increasingly performing attacks on foreign entities during elections and changes of power (Lutscher et al., 2020). However, the ease of access to attack resources coupled with difficulties in attribution often leaves identifying involvement unresolved.

4.9. Additional censorship considerations

The Internet censorship methods described above encompass the technical dimensions of *how* censors deny access to Internet resources. These generally involve identifying "objectionable" content as it traverses a network and then implementing a blocking action. Other methods are more blunt instruments, such as Internet shutdowns, denying access to all users. There are additional considerations for Internet censorship from social and legal perspectives.

One element not yet discussed in this work is compelled disconnection or removal of Internet content. Web servers must physically exist and operate on computer hardware, and law enforcement (LE) entities may seize hardware to take a web page offline. LE may also compel a domain registrar to surrender access to a domain so website users can no longer resolve the IP address of the target server that hosts the now-censored content. See Fig. 4 for an example of a splash page left behind on the Raid Forums website after a coalition of LE agencies seized the domain and associated web servers. Similar techniques have been used in other cybercrime enforcement measures. LE seizures frequently disrupt the online distribution of child sexual abuse material (CSAM), which is nearly universally denounced as criminal and an exception to the norms of free expression (ICMEC, 2021). Web services that host pirated content in violation of the intellectual property laws of certain jurisdictions may also be targeted in a similar manner (Reid, 2019).

Fig. 4. Example law enforcement domain seizure (U.S. Department of Justice, 2022) (Retrieved October 2, 2022).

Determined state censors may also use substitution as censorship. Redirection of web requests is often used to display a blockpage, warning the user why they were denied access (Deibert et al., 2008); a censor could also use redirection to display a website that appears legitimate but contains false information. Although specific instances of disinformation through redirection have not been documented in the literature, state-sponsored actors have been shown to spread false information or links to "fake news" websites on social media platforms (Serabian and Kapellmann Zafra, 2022; Zannettou et al., 2019; Harrell et al., 2025). These efforts may distract or discourage citizens from seeking the information they want, or reduce overall institutional trust among Internet users (Ognyanova et al., 2020). Nation-states may also provide intranets, such as the Iran National Information Network (NIN) built by the IRGC, which aims to normalize among Iranian citizens that they can access the information they want from their government and do not need global Internet access. This normalization allows for creation of "splinternets" with less public outcry or pushback when a censorship apparatus denies access to resources from outside countries.

Another controversial and sometimes ambiguous aspect of Internet censorship deals with content moderation. In addition to heavily censored external connections, China has been shown to delete content on social media networks and news sites within its borders (Hua and Shaw, 2020; Deluca, 2016; Zhu et al., 2013; Aase et al., 2012; King et al., 2013; Bamman et al., 2012). The Chinese government encourages Chinese companies to host alternative services to Western social media (e.g., Weibo as a microblogging service, WeChat as an alternative to messengers such as WhatsApp), which it can compel to remove content as the CCP deems necessary.

In the United States, free speech is protected under the First Amendment to the country's constitution and upheld in the courts under the "state action doctrine". Furthermore, Section 230 of the Communications Decency Act is part of a federal law that protects online services from lawsuits based on user content (Kosseff, 2019). While fostering free expression, issues of speech suppression have arisen because U.S. technology companies have wide latitude in determining what content they remove. Drawing distinctions between protected speech (e.g., radical ideas, controversial opinions, religious beliefs) and harmful rhetoric (e.g., hate speech, calls to enact violence, unlawful discrimination) can be difficult and spurs debate. From a legal perspective, U.S. citizens cannot have their speech suppressed by the government, but private companies hosting forums, blogs, and social media platforms are not beholden to the same standard and can moderate content as they see fit. Europe has demonstrated a desire to push further than the U.S.: rather than leaving companies the option of moderation, the European Union (EU) passed the Digital Services Act. The law requires companies that serve users in EU member states to moderate content for items such as "false information, hate speech, and extremism", and levies substantial fines (up to 6% of annual revenue) for noncompliance (Schroeder, 2022). It is uncertain how European regulations will affect future global corporation moderation practices and impact Internet users' freedom of expression.

Self-censorship is another adjacent issue in discussions of censorship. Humans often decide to withhold or selectively disclose their own discourse (Cook and Heilmann, 2013; Horton, 2011). Rather than deny access to content, a country may create a social or legal environment that encourages users to keep their views to themselves. A regime may allow access to social media platforms but punish journalists or dissidents who express opinions that portray authorities in a negatively (Tanash et al., 2017). In some cases, citizens may feel compelled to feign positive attitudes toward ruling elites (Shen and Truex, 2021).

Another tangential censorship issue is the disruption of information access due to physical attacks. Unlike Internet shutdowns as described above, some nations will attack critical infrastructure that enables Internet connectivity. Instances where European submarine fiber optic lines have been cut have been allegedly attributed to Russia, which "primarily employs deniable disruption and sabotage as part of hybrid warfare, aiming to impose costs on rivals without escalating to open conflict" (Bjartmarsson, 2026). During Russia's invasion of Ukraine, Russian forces made concerted efforts to destroy cellular telephone towers, disrupting Ukrainians' ability to communicate (Bergengruen, 2022). In response, Ukraine leveraged low-earth orbit satellite constellations from Starlink to enable TCP/IP connectivity (Burgess, 2022). While these physical layer attacks are not intended solely for censorship, their consequences are similar to the network, transport, and application layer attacks described throughout our survey.

Recent technological advances in generative artificial intelligence (AI), such as large language models (LLMs), have become a target of censorship. LLMs allow for access to large datasets of information, which users can have "conversations" with software to analyze, summarize, or create text-based content. Nation-states have begun to demonstrate a willingness to deny their citizens access to web-based LLMs (Berger and Shavitt, 2024; Ahmed and Knockel, 2024). Similarly, recent research has revealed that automated censorship is applied to Web-based language translation services (three Chinese, one American) (Ruo et al., 2024).

A final consideration for potential Internet censorship is publisher denial of access. It is common practice for web servers to filter inbound

Table 1
The Internet Censorship Methods Taxonomy.

	Censorship method	Techniques	OSI Model layer
Shallow Packet Inspection	**Internet Shutdowns**	Physical network disconnection Logical denial Routing blackhole[a]	Physical Layer
	Local Network Attacks[b]	ARP poisoning DoS MAC address filtering	Data Link Layer
	IP Address Blocking	IP address blocklist/allowlist IP range blocklist/allowlist Routing manipulation	Network Layer
	Computer Network Attack	Network DDoS	
	Port Blocking	Port blocklist/allowlist TCP/UDP/QUIC manipulation	Transport Layer
	BGP Attacks and Disruption	BGP hijacking AS path forgery BGP collusion attack	
Deep Packet Inspection	**Bandwidth Throttling**	Indiscriminate throttling Routing manipulation/delays[a] DPI latency injection Targeted throttling Traffic shaping/policing Quality of Service (QoS)	Session, Application, and Presentation Layers
	DNS Tampering	DNS blocklist/allowlist DNS cache poisoning DNS protocol manipulation DNS hijacking DNS transparent proxy	
	Protocol/Application Content Filtering	URL blocklist/allowlist Transparent proxy HTTP web content matching Keyword filtering (FTP, SMTP, etc.)	
	TLS-based Filtering	SNI blocklist MITM attack Application targeting	
	Computer Network Attack	Application-layer DDoS Offensive cyberspace operations	
	Protocol/Application Fingerprinting	Protocol manipulation Protocol or application blocking Active probing Encrypted traffic analysis Pattern/heuristic filtering	

[a] Occurs at the network layer
[b] None observed for nation-state censorship

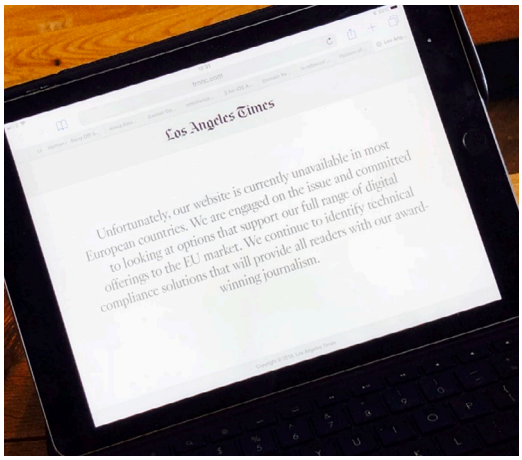

Fig. 5. Website blocking a user with a European IP address after GDPR was enacted (Tinworth, 2018) (May 25, 2018).

traffic. Administrators do this for a variety of security reasons. Subscribing to CTI blocklists or loading indicators of compromise (IOC) lists into an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) may prevent cyber attacks from occurring against their server. Some servers filter IP addresses that are marked as malicious, send spam emails, or host malware. The Internet measurement community has also identified publisher-side censorship trends (Tschantz et al., 2018) in which users who value anonymity are scrutinized. At the time of their study, Khattak et al. found that 3.67% of the top 1000 web pages blocked access to Tor users (Khattak et al., 2016). Some servers naively block all Tor exit nodes. Others use heuristic methods to detect abusive behavior and punish any user who shares the same exit node as a malicious actor (Singh et al., 2017). A Tor user may also receive differential treatment, such as a "paywall" or a CAPTCHA challenge to "prove they are human". Similarly, aggressive filtering is sometimes applied against VPN users (Ramesh et al., 2022; Khan et al., 2018; Earle, 2016; Biazin do Nascimento, 2021). Additionally, publisher-side filtering may occur based on geolocation. Servers in one country may not accept users from another. When the EU enacted the General Data Protection Regulation (GDPR), many web servers worldwide blocked connections from European IP addresses (Tschantz et al., 2018). These decisions likely happened to avoid compliance with GDPR's privacy rules or out of an abundance of caution for liability (see Fig. 5 for an example). Mobile device applications have also been shown to discriminate based on the estimated location where a user resides (Gosain et al., 2024). These kinds of server-side blocking are not necessarily government censorship, but they are relevant to a holistic discussion of what it means to be able to access information freely in the modern, interconnected world.

5. A taxonomy of internet censorship methods

The Internet Censorship Methods Taxonomy, shown in Table 1, is the result of our study. We organized the taxonomy using the OSI model for clarity of presentation. A censorship method is an abstraction of similar techniques used by censors. Examples of techniques that comprise a censorship method are included, but this is not an exhaustive list. Layers 1–4 represent methods that only require "shallow packet inspection" methods (reading of packet headers) and are minimally resource-intensive. Deep packet inspection (DPI) methods analyze contents beyond packet headers. Notably, bandwidth throttling bridges the gap between these methods and can occur network-wide or on an application-layer basis. Distributed denial-of-service attacks also occur at both the network and the application layers.

Moving downwards through the methods categorized as DPI implies increased complexity and use of resources. As an example, consider the observation of patterns (or anomalies) in bitstreams of traffic, including those protected by encryption. Encrypted traffic analysis often uses machine learning or statistical models to create profiles of traffic behavior for particular applications or protocols. Higher layers of OSI (down the taxonomy chart) represent methods of censorship with increasingly complex circumvention analysis and censor implementation. A preliminary version of the taxonomy was presented previously in Master (2023). In Table 2 we show the bibliography of evidence of Internet censorship methods and techniques, sorted chronologically by method and delineated by decade.

5.1. The impact of technological changes

Foundational improvements in Internet architecture can reduce the ability of censors on a broad scale. For example, a primary means of TLS-based blocking occurs when a censor targets the hostname of a website within the unencrypted SNI extension of a TLS header. When Cloudflare attempted to deploy encrypted SNI (ESNI), China blocked all TLS 1.3 traffic that had ESNI (Bock et al., 2020a). The IETF has a draft RFC for an Encrypted ClientHello (ECH) to be implemented in the TLS standard (Rescorla et al., 2022). If ratified and installed on the majority of web servers across the Internet, ECH has the potential to eliminate much of an entire class of censor methods. If ECH becomes the global standard for TLS connections, censors will eventually have to abandon many of their TLS-based censorship methods.

Censorship circumvention has been characterized as an arms race or "cat-and-mouse" game: developers of anti-censorship software discover novel ways to evade censor methods, and motivated censors respond with countermeasures to thwart circumvention efforts. Manual discovery may take months or years, but recent efforts have been made to automate the discovery of evasion strategies (Bock and Levin, 2020). However, many censors have constraints on resources or political will. A country may be willing to implement a censorship regime knowing that it will not deter determined users but be content in knowing that the majority of the population will not have access to denied content. Some researchers have questioned the assumption of an arms race situation, in favor of developing software that can be fully known by the censor (Fifield, 2024), as censors are limited by the fundamental protocols that allow the Internet to operate. The Internet Censorship Methods Taxonomy scopes the problem space for anti-censorship software developers by characterizing what methods and techniques are possible. Future work may involve assigning metrics to a tool's ability to counter particular censor methods. This would allow for an objective comparison of the capabilities of anti-censorship software.

6. Conclusion

The Internet has surpassed television, print media, and radio in terms of media influence and has become one of "the irreplaceable elements of our lives since the 2000s" (Dolunay et al., 2017). Consequently, a growing number of authorities in many jurisdictions apply censorship to online communications. Understanding how censors implement content filtering, throttling of connections, or Internet shutdowns is important for researchers, policymakers, and practitioners.

This work presents a taxonomy of Internet censorship methods derived from a systematic review of the literature and analysis of Internet technologies. The survey systematizes the technical means that censors implement, outlined by the legal and social circumstances in which they have occurred over the past three decades. We contend that this taxonomy has pedagogical and research value. This work lays the groundwork for future research endeavors in Internet design, Internet measurement studies, and online censorship circumvention.

Table 2
Evidence of Internet censorship methods.

Censorship method	1990–1999	2000–2009	2010–2019	2020–2025
Internet Shutdowns	-	Wang and Nagaraja (2007)	Tschantz et al. (2016), Hasan et al. (2013), Shavitt and Zilberman (2012), Dainotti et al. (2011)	Bischof et al. (2023), Feldstein (2022), Woodhams and Migliano (2022), Ryng et al. (2022), Padmanabhan et al. (2021), Gregorio (2020), Shah (2021), Mangino and Bou-Harb (2021)
IP Address Blocking	-	OpenNet Initiative (2009), Deibert et al. (2008), Xie et al. (2007), Clayton (2006), Dornseif (2003)	Nisar et al. (2018), McDonald et al. (2018), Singh et al. (2017), Wang et al. (2017), Tschantz et al. (2016), Fifield and Tsai (2016), Aceto and Pescapé (2015), Chaabane et al. (2014), Verkamp and Gupta (2012), Sfakianakis et al. (2011)	Padmanabhan et al. (2021), Bhaskar and Pearce (2022), Xue et al. (2022a), Elmenhorst et al. (2021), Xynou and Filastò (2021), Niaki et al. (2020), Ramesh et al. (2020), Alharbi et al. (2020), Sundara Raman et al. (2020)
Port Blocking	-	-	Tschantz et al. (2016), Aceto and Pescapé (2015), Technical Working Group, BITAG (2013)	Bhaskar and Pearce (2022), Elmenhorst et al. (2021), Niaki et al. (2020)
Computer Network Attacks	-	Clayton et al. (2006), Mirkovic and Reiher (2004), CISA (2009)	Tschantz et al. (2016), Marczak et al. (2015b), Aceto and Pescapé (2015), Deibert et al. (2012, 2010), Dainotti et al. (2011), Bailey and Labovitz (2011), Loukas and Oke (2010)	Kawerau et al. (2023), Bock et al. (2021a,b), Tripathi and Hubballi (2021), Lutscher et al. (2020)
BGP Attacks and Disruption	-	RIPE NCC (2008), Underwood (2005)	Mitseva et al. (2018), Aceto and Pescapé (2015), Benson et al. (2013)	Ramesh et al. (2023), Cloudflare (2018a), Padmanabhan et al. (2021), Janardhan (2021), Mangino and Bou-Harb (2021)
Bandwidth Throttling	-	-	Tschantz et al. (2016), Aryan et al. (2013), Anderson (2013)	Xue et al. (2021), Zhu et al. (2020)
DNS Tampering	-	OpenNet Initiative (2009), Deibert et al. (2008), Lowe et al. (2007), Clayton (2006), Wolfgarten (2006), Dornseif (2003)	Nisar et al. (2018), Yadav et al. (2018), Pearce et al. (2017), Wang et al. (2017), Jermyn and Weaver (2017), Ververis et al. (2017), Farnan et al. (2016), Scott et al. (2016), Tschantz et al. (2016), Aceto et al. (2016), Jones and Feamster (2015), Ververis et al. (2015), Gill et al. (2015), Chaabane et al. (2014), Khattak et al. (2014), Anderson et al. (2014), Anonymous (2014), Aryan et al. (2013), Nabi (2013), AFNIC (2013), Verkamp and Gupta (2012), Anonymous (2012), Duan et al. (2012), Filastò and Appelbaum (2012), Wright (2012), Xu et al. (2011), Sfakianakis et al. (2011)	Tai et al. (2025), Sheffey et al. (2025), Calle et al. (2024), Tsai et al. (2024), Ramesh et al. (2023), Brown et al. (2023), Nourin et al. (2023b), Katira et al. (2023), Cheng et al. (2022), Bhaskar and Pearce (2022), Harrity et al. (2022), Hoang et al. (2022), Hall et al. (2022), Jin et al. (2021), Houser et al. (2021), Padmanabhan et al. (2021), Kwan et al. (2021), Basso (2021), Xynou and Filastò (2021), Singh et al. (2020), Niaki et al. (2020), Bock et al. (2020c), Ramesh et al. (2020), Alharbi et al. (2020), Anonymous et al. (2020), Bock et al. (2020b), Sundara Raman et al. (2020)
Protocol/Application Content Filtering	Ding et al. (1999)	Deibert et al. (2008), Crandall et al. (2007), Clayton et al. (2006), Clayton (2006), Wolfgarten (2006), Dornseif (2003)	VanderSloot et al. (2018), Nisar et al. (2018), Yadav et al. (2018), Darer et al. (2017), Li et al. (2017), Wang et al. (2017), Jermyn and Weaver (2017), Weinberg et al. (2017), Tschantz et al. (2016), Aceto et al. (2016), Ververis et al. (2015), Gill et al. (2015), Aceto and Pescapé (2015), Chaabane et al. (2014), Khattak et al. (2014), Dalek et al. (2013), Aryan et al. (2013), Nabi (2013), Verkamp and Gupta (2012), Filastò and Appelbaum (2012), Xu et al. (2011), Sfakianakis et al. (2011), Park and Crandall (2010)	Zohaib et al. (2025), Tai et al. (2025), Wang et al. (2024), Hoang et al. (2024), Tsai et al. (2024), Müller et al. (2024), Ortwein et al. (2023), Nourin et al. (2023b), Ramesh et al. (2023), Katira et al. (2023), Sundara Raman et al. (2023), Harrity et al. (2022), Raman et al. (2022), Hall et al. (2022), Jin et al. (2021), Bock et al. (2021b), Weinberg et al. (2021), Knockel and Ruan (2021), Singh et al. (2020), Niaki et al. (2020), Bock et al. (2020c), Wang et al. (2020), Raman et al. (2020b), Ramesh et al. (2020), Alharbi et al. (2020), Bock et al. (2020b), Sundara Raman et al. (2020), Wang et al. (2020), Xiong and Knockel (2019)
TLS-based Filtering	-	-	Frolov and Wustrow (2019), Chai et al. (2019), VanderSloot et al. (2018), Nisar et al. (2018), Palo Alto Networks (2018b), Tschantz et al. (2016), Aceto and Pescapé (2015), Karapanos and Capkun (2014), Aryan et al. (2013), Winter and Lindskog (2012)	Niere et al. (2025a,b), Zohaib et al. (2025), Katira et al. (2023), Sundara Raman et al. (2023), Hoang et al. (2022), Xue et al. (2022a), Raman et al. (2022), Hall et al. (2022), Bock et al. (2021b), Weinberg et al. (2021), Jin et al. (2021), Xue et al. (2021), Elmenhorst et al. (2021), Bock et al. (2021c), Satija and Chatterjee (2021), Xynou and Filastò (2021), Bock et al. (2020a), Singh et al. (2020), Raman et al. (2020a), Alharbi et al. (2020), Sundara Raman et al. (2020), Basso (2020)
Protocol/Application Fingerprinting	-	-	Wang et al. (2017), Dunna et al. (2018), Tschantz et al. (2016), Fifield and Tsai (2016), Ensafi et al. (2015a), Wang et al. (2015), Ensafi et al. (2015b), Houmansadr et al. (2013), Aryan et al. (2013), Winter and Lindskog (2012), Palo Alto Networks (2018a), Kadak (2018)	Xue et al. (2025), Almutairi et al. (2024), Wu et al. (2023), Harrity et al. (2022), Xue et al. (2022b), Xynou and Filastò (2021), Bock et al. (2020b), Alice et al. (2020)

CRediT authorship contribution statement

Alexander Master: Writing – review & editing, Writing – original draft, Visualization, Methodology, Investigation, Data curation, Conceptualization. **Eugene H. Spafford:** Writing – review & editing, Writing – original draft, Supervision, Methodology, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

Aase, Nicholas, Crandall, Jedidiah R., Díaz, Álvaro, Knockel, Jeffrey, Molinero, Jorge Ocaña, Saia, Jared, Wallach, Dan, Zhu, Tao, 2012. Whiskey, weed, and wukan on the world wide web: on measuring censors' resources and motivations. In: Free and Open Communications on the Internet. USENIX, Bellevue, WA, p. 7, URL https://www.usenix.org/system/files/conference/foci12/foci12-final17.pdf.

Access Now, 2026. Internet shutdowns. https://www.accessnow.org/issue/internet-shutdowns/.

Aceto, Giuseppe, Botta, Alessio, Pescapè, Antonio, Awan, M. Faheem, Ahmad, Tahir, Qaisar, Saad, 2016. Analyzing internet censorship in Pakistan. In: Research and Technologies for Society and Industry. IEEE, Bologna, Italy, p. 6. http://dx.doi.org/10.1109/RTSI.2016.7740626.

Aceto, Giuseppe, Pescapé, Antonio, 2015. Internet censorship detection: A survey. Comput. Netw. 83, 381–421. http://dx.doi.org/10.1016/j.comnet.2015.03.008, URL https://linkinghub.elsevier.com/retrieve/pii/S1389128615000948.

AFNIC, 2013. Report of the AFNIC Scientific Council: Consequences of DNS-based Internet Filtering. Technical Report, AFNIC Scientific Council, URL https://www.afnic.fr/wp-media/uploads/2021/01/SC-consequences-of-DNS-based-Internet-filtering.pdf.

Ahmed, Mohamed, Knockel, Jeffrey, 2024. Extended abstract: The impact of online censorship on LLMs. In: Free and Open Communications on the Internet. Proceedings on Privacy Enhancing Technologies, Bristol, UK, p. 9, URL https://www.petsymposium.org/foci/2024/foci-2024-0006.pdf.

Albany Associates, 2012. The Arab spring and the impact of social media. URL https://web.archive.org/web/20130512021954/http://www.albanyassociates.com/notebook/2012/03/the-arab-spring-and-the-impact-of-social-media/.

Alharbi, Fatemah, Faloutsos, Michalis, Abu-Ghazaleh, Nael, 2020. Opening digital borders cautiously yet decisively: Digital filtering in Saudi Arabia. In: FOCI Workshop. USENIX, Virtual Event, USA, p. 7, URL https://www.usenix.org/system/files/foci20-paper-alharbi_0.pdf.

Alice, Bob, Carol, Beznazwy, Jan, Houmansadr, Amir, 2020. How China detects and blocks shadowsocks. In: Internet Measurement Conference. ACM, Virtual Event, USA, p. 14. http://dx.doi.org/10.1145/3419394.3423644, URL https://dl.acm.org/doi/10.1145/3419394.3423644.

Almutairi, Sultan, Neumann, Yogev, Harfoush, Khaled, 2024. Fingerprinting VPNs with custom router firmware: A new censorship threat model. In: Conference Proceedings of the CCNC. IEEE, Las Vegas, NV, USA, p. 5. http://dx.doi.org/10.1109/CCNC51664.2024.10454833.

AlterMidya, 2021. Joint statement by bulatlat and altermidya: Hold the Philippine Army accountable for cyberattacks against PH media websites. URL https://www.altermidya.net/joint-statement-by-bulatlat-and-altermidya-hold-the-philippine-army-accountable-for-cyberattacks-against-ph-media-websites/.

Amalou, Warda, Mehdi, Merouane, 2022. An approach to mitigate DDoS attacks on SIP based VoIP. In: ICCEIS 2021. MDPI, Virtual Event, USA, p. 6. http://dx.doi.org/10.3390/engproc2022014006, URL https://www.mdpi.com/2673-4591/14/1/6.

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

Anderson, Collin, Winter, Philipp, Roya, 2014. Global network interference detection over the RIPE atlas network. In: Free and Open Communications on the Internet. USENIX, San Diego, CA, p. 8, URL https://www.usenix.org/system/files/conference/foci14/foci14-anderson.pdf.

Anonymous, 2012. The collateral damage of internet censorship by DNS injection. ACM SIGCOMM Comput. Commun. Rev. 42 (3), 21–27. http://dx.doi.org/10.1145/2317307.2317311, URL https://dl.acm.org/doi/10.1145/2317307.2317311.

Anonymous, 2014. Towards a comprehensive picture of the great firewall's DNS censorship. In: Free and Open Communications on the Internet. USENIX, San Diego, CA, p. 7, URL https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf.

Anonymous, Niaki, Arian Akhavan, Hoang, Nguyen Phong, Gill, Phillipa, Houmansadr, Amir, 2020. Triplet censors: Demystifying great firewall's DNS censorship behavior. In: Free and Open Communications on the Internet. USENIX, Virtual Event, USA, p. 7, URL https://www.usenix.org/system/files/foci20-paper-anonymous_0.pdf.

Aryan, Simurgh, Aryan, Homa, Halderman, J. Alex, 2013. Internet censorship in Iran: A first look. In: Free and Open Communications on the Internet. USENIX, Washington, D.C., p. 8, URL https://www.usenix.org/system/files/conference/foci13/foci13-aryan.pdf.

Bailey, Michael, Labovitz, Craig, 2011. Censorship and Co-option of the Internet Infrastructure. Technical Report, University of Michigan, Ann Arbor, MI, p. 7, URL https://faculty.cc.gatech.edu/~mbailey/publications/CSE-TR-572-11.pdf.

Bamman, David, O'Connor, Brendan, Smith, Noah, 2012. Censorship and deletion practices in Chinese social media. First Monday 17 (3), 16. http://dx.doi.org/10.5210/fm.v17i3.3943.

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

Basso, Simone, 2021. Measuring DoT/DoH blocking using OONI probe: A preliminary study. In: Network and Distributed System Security (NDSS) Symposium. NDSS, Virtual Event, USA, p. 10, URL https://www.ndss-symposium.org/wp-content/uploads/dnspriv21-02-paper.pdf.

Bendrath, Ralf, Mueller, Milton, 2011. The end of the net as we know it? deep packet inspection and internet governance. New Media Soc. 13 (7), 1142–1160. http://dx.doi.org/10.1177/1461444811398031, URL http://journals.sagepub.com/doi/10.1177/1461444811398031.

Benson, Karyn, 2016. Leveraging Internet Background Radiation for Opportunistic Network Analysis (Ph.D. thesis). University of California, San Diego, URL https://www.proquest.com/dissertations-theses/leveraging-internet-background-radiation/docview/1828386151/se-2.

Benson, Karyn, Dainotti, Alberto, Claffy, K.C., Aben, Emile, 2013. Gaining insight into AS-level outages through analysis of internet background radiation. In: IEEE Conference on Computer Communications Workshops. IEEE, Turin, Italy, p. 6, URL https://cseweb.ucsd.edu/~kbenson/papers/tma13.pdf.

Bergengruen, Vera, 2022. The Battle for Control Over Ukraine's Internet. TIME, URL https://time.com/6222111/ukraine-internet-russia-reclaimed-territory/.

Berger, Harel, Shavitt, Yuval, 2024. Measuring DNS Censorship of Generative AI Platforms. Technical Report, ArXiv, p. 14. http://dx.doi.org/10.48550/arXiv.2412.14286.

Bhaskar, Abhishek, Pearce, Paul, 2022. Many roads lead to Rome: how packet headers influence DNS censorship measurement. In: USENIX Security Symposium. USENIX, Boston, MA, USA, p. 17, URL https://www.usenix.org/system/files/sec22-bhaskar.pdf.

Biazin do Nascimento, Francine, 2021. Measuring the Accessibility of Popular Websites While Using Mullvad VPN (Ph.D. thesis). Delft University of Technology, URL http://resolver.tudelft.nl/uuid:190ac398-50a0-4a47-9ec4-5514d5b22e25.

Bischof, Zachary S., Pitcher, Kennedy, Carisimo, Esteban, Meng, Amanda, Bezerra Nunes, Rafael, Padmanabhan, Ramakrishna, Roberts, Margaret E., Snoeren, Alex C., Dainotti, Alberto, 2023. Destination unreachable: Characterizing internet outages and shutdowns. In: Proceedings of the ACM SIGCOMM 2023 Conference. ACM, New York NY USA, p. 14. http://dx.doi.org/10.1145/3603269.3604883, URL https://dl.acm.org/doi/10.1145/3603269.3604883.

Bjartmarsson, Bergur, 2026. Beneath the Surface: Understanding Russian and Chinese Actions in Submarine Cable Context: A Comparative Analysis. University of Iceland, Reykjavík, Iceland, URL https://hdl.handle.net/1946/51989.

Bock, Kevin, Alaraj, Abdulrahman, Fax, Yair, Hurley, Kyle, Wustrow, Eric, Levin, Dave, 2021a. Weaponizing middleboxes for TCP reflected amplification. In: USENIX Security Symposium. USENIX, Virtual Event, USA, p. 18, URL https://www.usenix.org/system/files/sec21-bock.pdf.

Bock, Kevin, Anonymous, Merino, Louis-Henri, Fifield, David, Houmansadr, Amir, Levin, Dave, 2020a. Exposing and circumventing China's censorship of ESNI. URL https://gfw.report/blog/gfw_esni_blocking/en/.

Bock, Kevin, Bharadwaj, Pranav, Singh, Jasraj, Levin, Dave, 2021b. Your censor is my censor: Weaponizing censorship infrastructure for availability attacks. In: 2021 IEEE Security and Privacy Workshops. SPW, IEEE, San Francisco, CA, USA, pp. 398–409. http://dx.doi.org/10.1109/SPW53761.2021.00059.

Bock, Kevin, Fax, Yair, Reese, Kyle, Singh, Jasraj, Levin, Dave, 2020b. Detecting and evading censorship-in-depth: A case study of Iran's protocol filter. In: Free and Open Communications on the Internet. USENIX, Virtual Event, USA, p. 7, URL https://www.usenix.org/system/files/foci20-paper-bock.pdf.

Bock, Kevin, Hughey, George, Merino, Louis-Henri, Arya, Tania, Liscinsky, Daniel, Pogosian, Regina, Levin, Dave, 2020c. Come as you are: Helping unmodified clients bypass censorship with server-side evasion. In: ACM SIGCOMM. ACM, Virtual Event, USA, p. 13.

Bock, Kevin, Levin, Dave, 2020. Automating the censorship arms race. XRDS: Crossroads ACM Mag. Stud. 27 (2), 30–35, URL https://dl.acm.org/doi/10.1145/3437410.

Bock, Kevin, Naval, Gabriel, Reese, Kyle, Levin, Dave, 2021c. Even censors have a backup: Examining China's double HTTPS censorship middleboxes. In: Free and Open Communications on the Internet. ACM, Virtual Event, USA, p. 7.

Braden, Robert, 1989. RFC 1122 - requirements for internet hosts - communication layers. URL https://datatracker.ietf.org/doc/html/rfc1122,

Brenner, Susan W., 2007. At light speed: Attribution and response to cybercrime/terrorism/warfare. J. Crim. Law Criminol. 97, 379–475, URL https://www.proquest.com/docview/218442098.

Brown, Jacob, Jiang, Xi, Tran, Van, Bhagoji, Arjun Nitin, Hoang, Nguyen Phong, Feamster, Nick, Mittal, Prateek, Yegneswaran, Vinod, 2023. Augmenting rule-based DNS censorship detection at scale with machine learning. In: Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. ACM, Long Beach CA USA, p. 13. http://dx.doi.org/10.1145/3580305.3599775, URL https://dl.acm.org/doi/10.1145/3580305.3599775.

Bruns, Axel, Highfield, Tim, Burgess, Jean, 2013. The Arab spring and social media audiences: English and Arabic Twitter users and their networks. Am. Behav. Sci. 57 (7), 871–898. http://dx.doi.org/10.1177/0002764213479374, URL http://journals.sagepub.com/doi/10.1177/0002764213479374.

Bujlow, Tomasz, Carela-Español, Valentín, Barlet-Ros, Pere, 2015. Independent comparison of popular DPI tools for traffic classification. Comput. Netw. 76, 75–89. http://dx.doi.org/10.1016/j.comnet.2014.11.001, URL https://linkinghub.elsevier.com/retrieve/pii/S1389128614003909.

Burgess, Matt, 2022. How Starlink Scrambled to Keep Ukraine Online. WIRED, URL https://www.wired.com/story/starlink-ukraine-internet/.

Burgess, Matt, Newman, Lily Hay, 2026. Internet starts to return in Iran after 3-month blackout. URL https://www.wired.com/story/internet-in-iran-starts-to-return-after-3-month-blackout/.

Calle, Paola, Savitsky, Larissa, Bhagoji, Arjun Nitin, Hoang, Nguyen Phong, Cho, Shinyoung, 2024. Toward automated DNS tampering detection using machine learning. In: Free and Open Communications on the Internet. Proceedings on Privacy Enhancing Technologies, Bristol, UK, p. 9, URL https://www.petsymposium.org/foci/2024/foci-2024-0008.pdf.

Center for Human Rights in Iran, 2018. Iran's severely disrupted internet during protests: "websites hardly open". URL https://iranhumanrights.org/2018/01/irans-severely-disrupted-internet-during-protests-websites-hardly-open/.

Chaabane, Abdelberi, Chen, Terence, Cunche, Mathieu, Cristofaro, Emiliano De, Friedman, Arik, Kaafar, Mohamed Ali, 2014. Censorship in the wild: analyzing internet filtering in Syria. In: Internet Measurement Conference. ACM, Vancouver, BC, Canada, p. 14. http://dx.doi.org/10.1145/2663716.2663720, URL https://dl.acm.org/doi/10.1145/2663716.2663720.

Chai, Zimo, Ghafari, Amirhossein, Houmansadr, Amir, 2019. On the importance of encrypted-SNI (ESNI) to censorship circumvention. In: Free and Open Communications on the Internet. USENIX, Santa Clara, CA, USA, p. 8, URL https://www.usenix.org/system/files/foci19-paper_chai_update.pdf.

Chandel, Sonali, Jingji, Zang, Yunnan, Yu, Jingyao, Sun, Zhipeng, Zhang, 2019. The golden shield project of China: A decade later—An in-depth study of the great firewall. In: 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. CyberC, IEEE, Guilin, China, pp. 111–119. http://dx.doi.org/10.1109/CyberC.2019.00027, URL https://ieeexplore.ieee.org/document/8945933/.

Chen, Mo, Grossklags, Jens, 2022. Social control in the digital transformation of society: A case study of the Chinese social credit system. Soc. Sci. 11 (6), 23. http://dx.doi.org/10.3390/socsci11060229.

Cheng, Yanan, Liu, Yali, Li, Chao, Zhang, Zhaoxin, Li, Ning, Du, Yuejin, 2022. In-depth evaluation of the impact of national-level DNS filtering on DNS resolvers over space and time. Electronics 11 (8), 1276. http://dx.doi.org/10.3390/electronics11081276, URL https://www.mdpi.com/2079-9292/11/8/1276.

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

CISA, 2009. Understanding Denial-of-Service Attacks. Technical Report ST04-015, U.S. Cybersecurity and Infrastructure Agency, URL https://www.cisa.gov/uscert/ncas/tips/ST04-015.

CISA, 2017. HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure. Technical Report TA17-164A, U.S. Cybersecurity and Infrastructure Agency, URL https://www.cisa.gov/uscert/ncas/alerts/TA17-164A.

Clark, Mitchell, 2021. What is BGP, and what role did it play in Facebook's massive outage. URL https://www.theverge.com/2021/10/4/22709260/what-is-bgp-border-gateway-protocol-explainer-internet-facebook-outage.

Clarke, Richard A., Knake, Robert K., 2012. Cyber War: The next Threat to National Security and What to Do about It, first ed. Ecco, New York.

Clayton, Richard, 2006. Failures in a hybrid content blocking system. In: Privacy Enhancing Technologies. Springer, Cambridge, UK, pp. 78–92, URL https://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf.

Clayton, Richard, Murdoch, Steven J., Watson, Robert N.M., 2006. Ignoring the great firewall of China. In: Privacy Enhancing Technologies, vol. 4258, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 20–35. http://dx.doi.org/10.1007/11957454_2, URL http://link.springer.com/10.1007/11957454_2.

Cloudflare, 2018a. Bgp hijacking. URL https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/.

Cloudflare, 2018b. What is BGP? | BGP routing explained. URL https://www.cloudflare.com/learning/security/glossary/what-is-bgp/.

Cloudflare, 2024. Famous DDoS attacks | the largest DDoS attacks of all time. URL https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/.

Cook, Philip, Heilmann, Conrad, 2013. Two types of self-censorship: Public and private. Political Stud. 61 (1), 178–196. http://dx.doi.org/10.1111/j.1467-9248.2012.00957.x, URL http://journals.sagepub.com/doi/10.1111/j.1467-9248.2012.00957.x.

Council on Foreign Relations, 2005. Titan rain. URL https://www.cfr.org/cyber-operations/titan-rain.

Crandall, Jedidiah R., Zinn, Daniel, Byrd, Michael, Barr, Earl, East, Rich, 2007. ConceptDoppler: A weather tracker for internet censorship. In: Computer and Communications Security. ACM, Alexandria, VA, USA, p. 14, URL http://www.csd.uoc.gr/~hy558/papers/conceptdoppler.pdf.

Dahir, Abdi Latif, 2019. After a record 16-month ban, this president has unblocked social media access. URL https://qz.com/africa/1667263/chads-idriss-deby-unblocks-social-media-after-record-shutdown.

Dainotti, Alberto, Squarcella, Claudio, Aben, Emile, Claffy, Kimberly, Chiesa, Marco, Russo, Michele, Pescapè, Antonio, 2011. Analysis of country-wide internet outages caused by censorship. ACM IMC 2011 1, 18. http://dx.doi.org/10.1145/2068816.2068818.

Dalek, Jakub, Haselton, Bennett, Noman, Helmi, Senft, Adam, Crete-Nishihata, Masashi, Gill, Phillipa, Deibert, Ronald, 2013. A method for identifying and confirming the use of URL filtering products for censorship. In: Proceedings of the ACM IMC 2013. ACM, Barcelona Spain, pp. 23–30. http://dx.doi.org/10.1145/2504730.2504763.

Dalek, Jakub, Senfit, Adam, 2011. Behind blue coat: investigations of commercial filtering in Syria and Burma. URL https://citizenlab.ca/2011/11/behind-blue-coat/.

Darer, Alexander, Farnan, Oliver, Wright, Joss, 2017. FilteredWeb: A framework for the automated search-based discovery of blocked URLs. In: Network Traffic Measurement and Analysis. IFIP, Dublin, Ireland, p. 9, URL http://tma.ifip.org/wordpress/wp-content/uploads/2017/06/tma2017_paper32.pdf.

DARPA, 1981. RFC 793 - transmission control protocol (TCP). URL https://datatracker.ietf.org/doc/html/rfc793.

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

Dawn, 2010. 5,000 internet porn users held in China last year. URL https://www.dawn.com/news/825971/5-000-internet-porn-users-held-in-china-last-year.

Day, J.D., Zimmermann, H., 1983. The OSI reference model. Proc. IEEE 71 (12), 16. http://dx.doi.org/10.1109/PROC.1983.12775.

Deibert, Ronald, Palfrey, John, Rohozinski, Rafal, Zittrain, Jonathan, Initiative, OpenNet (Eds.), 2010. Access controlled: The shaping of power, rights, and rule in cyberspace. In: Information Revolution and Global Politics, MIT Press, Cambridge, MA.

Deibert, Ronald, Palfrey, John, Rohozinski, Rafal, Zittrain, Jonathan, Stein, Janice, 2008. Access denied: The practice and policy of global internet filtering. In: Project MUSE: Information Revolution and Global Politics, The MIT Press, Cambridge, MA, URL https://muse.jhu.edu/book/60844.

Deibert, Ronald, Zittrain, Jonathan, Rohozinski, Rafal, Palfrey, John (Eds.), 2012. Access contested: Security, identity, and resistance in Asian cyberspace information revolution and global politics. In: Information Revolution and Global Politics, MIT Press, Cambridge, MA.

Deluca, Kevin Michael, 2016. Weibo, wechat, and the transformative events of environmental activism on China's wild public screens. Int. J. Commun. 10, 19.

Ding, Chen, Chi, Chi-Hung, Deng, Jing, Dong, Chun-Lei, 1999. Centralized content-based web filtering and blocking: How far can it go? In: Conference Proceedings, vol. 2, IEEE, Tokyo, Japan, pp. 115–119. http://dx.doi.org/10.1109/ICSMC.1999.825218.

Dingledine, Roger, Mathewson, Nick, Syverson, Paul, 2004. Tor: The second-generation onion router. 13th USENIX Security Symposium, 13th USENIX Security Symposium, vol. 1, 18.URL http://usenix.org/publications/library/proceedings/sec04/tech/full_papers/dingledine/dingledine.pdf,

Dixon, Lucas, Ristenpart, Thomas, Shrimpton, Thomas, 2016. Network traffic obfuscation and automated internet censorship. IEEE Secur. Priv. 14 (6), 43–53. http://dx.doi.org/10.1109/MSP.2016.121, URL http://ieeexplore.ieee.org/document/7782699/.

Dolunay, Ayhan, Kasap, Fevzi, Keçeci, Gökçe, 2017. Freedom of mass communication in the digital age in the case of the internet: "freedom house" and the USA example. Sustainability 9 (10), 1739. http://dx.doi.org/10.3390/su9101739, URL http://www.mdpi.com/2071-1050/9/10/1739.

Dornseif, Maximillian, 2003. Government mandated blocking of foreign web content. In: DFN-Arbeitstagung Über Kommunikationsnetze. Gesellschaft für Informatik, Trier, Germany, pp. 617–647, URL https://censorbib.nymity.ch/pdf/Dornseif2003a.pdf.

Duan, Haixin, Weaver, Nicholas, Zhao, Zongxu, Hu, Meng, Liang, Jinjin, Jiang, Jian, Li, Kang, Paxson, Vern, 2012. Hold-on: protecting against on-path DNS poisoning. In: Securing and Trusting Internet Names. National Physical Laboratory, UK, p. 7, URL http://www.cs.albany.edu/~mariya/courses/csi516F19/papers/holdon.pdf.

Dunna, Arun, O'Brien, Ciarán, Gill, Phillipa, 2018. Analyzing China's blocking of unpublished tor bridges. In: Free and Open Communications on the Internet. USENIX, Baltimore, MD, USA, p. 7, URL https://www.usenix.org/system/files/conference/foci18/foci18-paper-dunna.pdf.

Dykstra, Josiah, Gordon, Lawrence A., Loeb, Martin P., Zhou, Lei, 2022. The economics of sharing unclassified cyber threat intelligence by government agencies and departments. J. Inf. Secur. 13 (03), 85–100. http://dx.doi.org/10.4236/jis.2022.133006.

Earle, Sabrina, 2016. The battle against geo-blocking: The consumer strikes back. Richmond J. Glob. Law Bus. 15, 20, URL https://scholarship.richmond.edu/global/vol15/iss1/2.

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

Ensafi, Roya, Fifield, David, Winter, Philipp, Feamster, Nick, Weaver, Nicholas, Paxson, Vern, 2015a. Examining how the great firewall discovers hidden circumvention servers. In: Proceedings of the 2015 Internet Measurement Conference. ACM, Tokyo Japan, pp. 445–458. http://dx.doi.org/10.1145/2815675.2815690, URL https://dl.acm.org/doi/10.1145/2815675.2815690.

Ensafi, Roya, Winter, Philipp, Mueen, Abdullah, Crandall, Jedidiah R., 2015b. Analyzing the great firewall of China over space and time. Proc. Priv. Enhanc. Technol. 2015 (1), 61–76. http://dx.doi.org/10.1515/popets-2015-0005, URL https://www.sciendo.com/article/10.1515/popets-2015-0005.

Esfandiari, Golnaz, 2013. Iran admits throttling internet to 'preserve calm' during election. URL https://www.rferl.org/a/iran-internet-disruptions-election/25028696.html.

Fallows, James, 2008. The connection has been reset. URL https://www.theatlantic.com/magazine/archive/2008/03/the-connection-has-been-reset/306650/.

Farnan, Oliver, Darer, Alexander, Wright, Joss, 2016. Poisoning the well – exploring the great firewall's poisoned DNS responses. In: Workshop on Privacy in the Electronic Society. ACM, Vienna, Austria, p. 4. http://dx.doi.org/10.1145/2994620.2994636, URL https://dl.acm.org/authorize?N25517.

FCC, 2000. Children's internet protection act (CIPA). URL https://www.fcc.gov/consumers/guides/childrens-internet-protection-act.

Feldstein, Steven, 2021. The rise of digital repression: How technology is reshaping power, politics, and resistance. In: Carnegie Endowment for International Peace, Oxford Press, New York, NY.

Feldstein, Steven, 2022. Internet shutdowns are changing. how should citizens and democracies respond? URL https://carnegieendowment.org/2022/03/31/government-internet-shutdowns-are-changing.-how-should-citizens-and-democracies-respond-pub-86687.

Fifield, David, 2024. Against the "arms race". URL https://bamsoftware.com/talks/arms-race-foci-2024/.

Fifield, David, Lan, Chang, Hynes, Rod, Wegmann, Percy, Paxson, Vern, 2015. Blocking-resistant communication through domain fronting. Proc. Priv. Enhanc. Technol. 2015 (2), 46–64. http://dx.doi.org/10.1515/popets-2015-0009, URL https://www.sciendo.com/article/10.1515/popets-2015-0009.

Fifield, David, Tsai, Lynn, 2016. Censors' delay in blocking circumvention proxies. In: Free and Open Communications on the Internet. USENIX, Austin, TX, p. 7, URL https://www.usenix.org/system/files/conference/foci16/foci16-paper-fifield.pdf.

Filastò, Arturo, Appelbaum, Jacob, 2012. OONI: open observatory of network interference. In: Free and Open Communications on the Internet. USENIX, Bellevue, WA, p. 8, URL https://www.usenix.org/system/files/conference/foci12/foci12-final12.pdf.

Fink, Arlene, 2005. Conducting Research Literature Reviews: From the Internet to Paper, second ed. Sage Publications, Thousand Oaks, CA.

FireninjaDD, 2017. Will using a VPN prevent ISP throttling due to the removal of net neutrality? URL https://www.reddit.com/r/technology/comments/6c1kck/will_using_a_vpn_prevent_isp_throttling_due_to/.

Forcepoint, 2023. Protocol agents on NGFW engines. URL https://help.forcepoint.com/ngfw/en-us/7.0.0/GUID-8A8FD672-D113-4D47-945A-46298F96C0F9.html.

Fortinet, 2021. Fortios 7.0.1 administration guide. URL https://docs.fortinet.com/document/fortigate/7.0.1/administration-guide/233445/blocking-applications-with-custom-signatures.

Freedom House, 2026. Freedom on the Net 2025 Report. Technical Report, Freedom House, Washington, D.C., p. 43, URL https://freedomhouse.org/sites/default/files/2025-12/FOTN%202025_final_digital_120525.pdf.

Frolov, Sergey, Wampler, Jack, Wustrow, Eric, 2020. Detecting probe-resistant proxies. In: Network and Distributed System Security. The Internet Society, San Diego, California, p. 17. http://dx.doi.org/10.14722/ndss.2020.23087, URL https://www.ndss-symposium.org/wp-content/uploads/2020/02/23087.pdf.

Frolov, Sergey, Wustrow, Eric, 2019. The use of TLS in censorship circumvention. In: Network and Distributed System Security. The Internet Society, San Diego, CA, p. 15, URL https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_03B-2-1_Frolov_paper.pdf.

Frolov, Sergey, Wustrow, Eric, 2020. HTTPT: A probe-resistant proxy. In: Free and Open Communications on the Internet, vol. 1, USENIX, Virtual Event, USA, p. 8, URL https://www.usenix.org/system/files/foci20-paper-frolov.pdf.

FTC, 1998. Children's online privacy protection rule ("COPPA"). URL https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

Garcia, Raphael, 2019. Internet censorship is part of South Korea's democracy package. URL https://international.thenewslens.com/article/122579.

Gardner, Frank, 2000. Saudis 'defeating' internet porn. URL http://news.bbc.co.uk/2/hi/middle_east/742798.stm.

Gavilan, Jodesz, 2022. Cyberattack hits CNN Philippines on day of presidential debate. URL https://www.rappler.com/nation/cyberattack-hits-cnn-philippines-presidential-debate-february-27-2022/.

Ghedini, Alessandro, 2018. Encrypt it or lose it: How encrypted SNI works. URL https://blog.cloudflare.com/encrypted-sni/.

Gill, Phillipa, Crete-Nishihata, Masashi, Dalek, Jakub, Goldberg, Sharon, Senft, Adam, Wiseman, Greg, 2015. Characterizing web censorship worldwide: Another look at the OpenNet initiative data. ACM Trans. Web 9 (1), 29. http://dx.doi.org/10.1145/2700339, URL https://censorbib.nymity.ch/pdf/Gill2015a.pdf.

GoodbyeDPI, 2017. GoodbyeDPI — deep packet inspection circumvention utility. URL https://github.com/ValdikSS/GoodbyeDPI.

Google, 2017. HTTPS encryption on the web. URL https://transparencyreport.google.com/https/overview.

Google, 2023. Feature: TLS encrypted client hello (ECH). URL https://chromestatus.com/feature/6196703843581952.

Gosain, Devashish, Agarwal, Anshika, Shekhawat, Sahil, Acharya, H.B., Chakravarty, S., 2018. Mending wall: On the implementation of censorship in India. 1, p. 20. http://dx.doi.org/10.48550/arXiv.1806.06518, arXiv.

Gosain, Devashish, Mohindra, Mayank, Chakravarty, Sambuddho, 2021. Too close for comfort: Morasses of (anti-) censorship in the era of CDNs. Proc. Priv. Enhanc. Technol. 2021 (2), 173–193. http://dx.doi.org/10.2478/popets-2021-0023, URL https://www.sciendo.com/article/10.2478/popets-2021-0023.

Gosain, Devashish, Singh, Kartikey, Sharma, Rishi, Suresh Babu, Jithin, Chakravaty, Sambuddho, 2024. Out in the open: On the implementation of mobile app filtering in India. In: Richter, Philipp, Bajpai, Vaibhav, Carisimo, Esteban (Eds.), In: Passive and Active Measurement, vol. 14538, Springer Nature Switzerland, Cham, pp. 19–36. http://dx.doi.org/10.1007/978-3-031-56252-5_2, URL https://link.springer.com/10.1007/978-3-031-56252-5_2.

Green, James A. (Ed.), 2015. Cyber warfare: A multidisciplinary analysis. In: Routledge Studies in Conflict, Security and Technology, Routledge, Abingdon, Oxon ; New York, NY.

Greenberg, Andy, 2017. The WannaCry ransomware has a link to suspected north Korean hackers. URL https://www.wired.com/2017/05/wannacry-ransomware-link-suspected-north-korean-hackers/.

Greenwald, Glenn, 2014. Exclusive: Snowden docs show UK spies attacked anonymous, hackers. URL https://www.nbcnews.com/feature/edward-snowdeninterview/exclusive-snowden-docs-show-uk-spies-attackedanonymous-hackers-n21361.

Gregorio, Giovanni De, 2020. Internet shutdowns and the limits of law. Int. J. Commun. 1, 20, URL https://ijoc.org/index.php/ijoc/article/view/13752/3183.

Grover, Rohan, Jang, Kyooeun, Su, Li Wen, 2024. Beyond digital protection(ism). J. Inf. Policy 14, 32. http://dx.doi.org/10.5325/jinfopoli.14.2024.0005.

Guest, Peter, 2022. "It's like being under siege": How DDoS became a censorship tool. URL https://restofworld.org/2022/blackouts-ddos/.

Hacker Target, 2022. WHOIS ASN IP lookup tool. URL https://hackertarget.com/as-ip-lookup/.

Hall, et al., 2022. A survey of worldwide censorship techniques (draft in progress). URL https://datatracker.ietf.org/doc/draft-irtf-pearg-censorship/08/.

Hancock, Alexis, 2021. HTTPS is actually everywhere. URL https://www.eff.org/deeplinks/2021/09/https-actually-everywhere.

Harrell, Nicholas, Master, Alexander, Starck, Nicolas, Eerhart, Daniel, 2025. Tactics and techniques of information operations: gaps in us response to counter malign influence. ICCWS 1, 10. http://dx.doi.org/10.34190/iccws.20.1.3271.

Harrity, Michael, Bock, Kevin, Sell, Frederick, Levin, Dave, 2022. GET /out: Automated discovery of application-layer censorship evasion strategies. In: USENIX Security Symposium. USENIX, Boston, MA, USA, p. 19, URL https://www.usenix.org/system/files/sec22-harrity.pdf.

Hasan, Shaddi, Ben-David, Yahel, Fanti, Giulia, Brewer, Eric, Shenker, Scott, 2013. Building dissent networks: Towards effective countermeasures against large-scale communications blackouts. In: Free and Open Communications on the Internet. USENIX, San Jose, CA, USA, p. 8, URL https://censorbib.nymity.ch/pdf/Hasan2013a.pdf.

Hersher, Rebecca, 2015. Meet mafiaboy, the 'bratty kid' who took down the internet. URL https://www.npr.org/sections/alltechconsidered/2015/02/07/384567322/meet-mafiaboy-the-bratty-kid-who-took-down-the-internet.

Hoang, Nguyen Phong, Dalek, Jakub, Crete-Nishihata, Masashi, Christin, Nicolas, Yegneswaran, Vinod, Polychronakis, Michalis, Feamster, Nick, 2024. GFWeb: Measuring the great firewall's web censorship at scale. In: USENIX Security Symposium. USENIX, Philadelphia, PA, p. 17, URL https://www.usenix.org/system/files/sec24fall-prepub-310-hoang.pdf.

Hoang, Nguyen Phong, Polychronakis, Michalis, Gill, Phillipa, 2022. Measuring the accessibility of domain name encryption and its impact on internet filtering. In: Passive and Active Measurement Conference. Springer, Virtual Event, p. 17. http://dx.doi.org/10.1007/978-3-030-98785-5_23, URL https://www3.cs.stonybrook.edu/~mikepo/papers/dneye.pam22.pdf.

Horton, John, 2011. Self-censorship. Res Publica 17 (1), 91–106. http://dx.doi.org/10.1007/s11158-011-9145-3, URL http://link.springer.com/10.1007/s11158-011-9145-3.

Houmansadr, A., Brubaker, C., Shmatikov, V., 2013. The parrot is dead: Observing unobservable network communications. In: 2013 IEEE Symposium on Security and Privacy. IEEE, Berkeley, CA, pp. 65–79. http://dx.doi.org/10.1109/SP.2013.14, URL http://ieeexplore.ieee.org/document/6547102/.

Houser, Rebekah, Hao, Shuai, Li, Zhou, Liu, Daiping, Cotton, Chase, Wang, Haining, 2021. A comprehensive measurement-based investigation of DNS hijacking. In: Symposium on Reliable Distributed Systems. IEEE, Virtual Event, USA, p. 11. http://dx.doi.org/10.1109/SRDS53918.2021.00029.

Howard, Philip N., Agarwal, Sheetal D., Hussain, Muzammil M., 2015. The hermit kingdom in cyberspace: Unveiling the north Korean internet. Inf. Commun. Soc. 18 (3), 252–267. http://dx.doi.org/10.1080/1369118X.2014.940363.

HTTP Archive, 2024. HTTP - the web almanac 2024. URL https://almanac.httparchive.org/en/2024/http.

Hua, Jinling, Shaw, Rajib, 2020. Corona virus (COVID-19) "infodemic" and emerging issues through a data lens: The Case of China. Int. J. Environ. Res. Public Health 17 (7), 2309. http://dx.doi.org/10.3390/ijerph17072309, URL https://www.mdpi.com/1660-4601/17/7/2309.

Human Rights Council, 2020. General Comment No. 37 (2020) on the Right of Peaceful Assembly (Article 21). Technical Report CCPR/C/GC/37, United Nations, United Nations, URL https://digitallibrary.un.org/record/3884725?ln=en.

Human Rights Council, 2021. Ending Internet Shutdowns: A Path Forward. Technical Report A/HRC/47/24/Add.2, United Nations, United Nations, URL https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/149/66/PDF/G2114966.pdf?OpenElement.

Hunt, Troy, Helme, Scott, 2021. Why no HTTPS? URL https://whynohttps.com/.

Husaini, Saro, 2024. Circumventing Internet Censorship (Ph.D. thesis). University of South-Eastern Norway, URL https://openarchive.usn.no/usn-xmlui/handle/11250/3135775.

ICMEC, 2021. The growing global threat of child sexual abuse material (CSAM). URL https://icmec.org.au/blog/the-growing-global-threat-of-child-sexual-abuse-material-csam/.

Internet Security Research Group, 2023. Let's encrypt. URL https://letsencrypt.org/.

Internet Society Pulse, 2021. Internet Shutdown in Jammu and Kashmir, India. Internet Society, URL https://pulse.internetsociety.org/en/shutdowns/india-110/.

IVPN Limited, 2023. Transparent DNS proxy, dnsleaktest.com. URL https://dnsleaktest.com/what-is-transparent-dns-proxy.html.

Jacobs, Kevin, 2021. Encrypted client hello: The future of ESNI in firefox. URL https://blog.mozilla.org/security/2021/01/07/encrypted-client-hello-the-future-of-esni-in-firefox/.

Janardhan, Santosh, 2021. More details about the October 4 outage. URL https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/.

Januta, Andrea, Funakoshi, Minami, 2021. Myanmar's internet suppression. URL https://www.reuters.com/graphics/MYANMAR-POLITICS/INTERNET-RESTRICTION/rlgpdbreepo/.

Jermyn, Jill, Weaver, Nicholas, 2017. Autosonda: Discovering rules and triggers of censorship devices. In: Free and Open Communications on the Internet. USENIX, Vancouver, BC, Canada, p. 9, URL https://www.usenix.org/system/files/conference/foci17/foci17-paper-jermyn.pdf.

Jin, Lin, Hao, Shuai, Wang, Haining, Cotton, Chase, 2021. Understanding the practices of global censorship through accurate, end-to-end measurements. Proc. ACM Meas. Anal. Comput. Syst. 5 (3), 1–25. http://dx.doi.org/10.1145/3491055, URL https://dl.acm.org/doi/10.1145/3491055.

Jones, Ben, Feamster, Nick, 2015. Can censorship measurements be safe(r)? In: HotNets '15. ACM, Philadelphia, PA, p. 7, URL http://conferences.sigcomm.org/hotnets/2015/papers/jones.pdf.

Jones, Ben, Lee, Tzu-Wen, Feamster, Nick, Gill, Phillipa, 2014. Automated detection and fingerprinting of censorship block pages. In: Proceedings of the Internet Measurement Conference 2014. ACM, Vancouver BC Canada, pp. 299–304. http://dx.doi.org/10.1145/2663716.2663722, URL https://dl.acm.org/doi/10.1145/2663716.2663722.

Kadak, 2018. How to block traffic based on application filters with an exception. URL https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClXfCAK.

Kang, Cecilia, Alba, Davey, Satariano, Adam, 2020. Surging traffic is slowing down our internet. URL https://www.nytimes.com/2020/03/26/business/coronavirus-internet-traffic-speed.html,

Karapanos, Nikolaos, Capkun, Srdjan, 2014. On the effective prevention of TLS man-in-the-middle attacks in web applications. In: USENIX Security Symposium. USENIX, San Diego, CA, p. 17, URL https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-karapanos.pdf.

Katira, Divyank, Grover, Gurshabad, Singh, Kushagra, Bansal, Varun, 2023. CensorWatch: On the implementation of online censorship in India. In: Free and Open Communications on the Internet. Proceedings on Privacy Enhancing Technologies, Lausanne, Switzerland, p. 12.

Kawerau, Lukas, Weidmann, Nils B., Dainotti, Alberto, 2023. Attack or block? repertoires of digital censorship in autocracies. J. Inf. Technol. Politics 20 (1), 60–73. http://dx.doi.org/10.1080/19331681.2022.2037118, URL https://www.tandfonline.com/doi/full/10.1080/19331681.2022.2037118.

Khan, Mohammad Taha, DeBlasio, Joe, Voelker, Geoffrey M., Snoeren, Alex C., Kanich, Chris, Vallina-Rodriguez, Narseo, 2018. An empirical analysis of the commercial VPN ecosystem. In: Proceedings of the Internet Measurement Conference 2018. ACM, Boston, MA, USA, pp. 443–456.

Khattak, Sheharbano, Fifield, David, Afroz, Sadia, Javed, Mobin, Sundaresan, Srikanth, Paxson, Vern, Murdoch, Steven J., McCoy, Damon, 2016. Do you see what I see? differential treatment of anonymous users. In: Proceedings 2016 Network and Distributed System Security Symposium. Internet Society, San Diego, CA, p. 15. http://dx.doi.org/10.14722/ndss.2016.23342, URL https://www.ndss-symposium.org/wp-content/uploads/2017/09/do-you-see-what-i-see-differential-treatment-anonymous-users.pdf.

Khattak, Sheharbano, Javed, Mobin, Khayam, Syed Ali, Uzmi, Zartash Afzal, Paxson, Vern, 2014. A look at the consequences of internet censorship through an ISP lens. In: Internet Measurement Conference. ACM, Barcelona, Spain, p. 13, URL http://conferences2.sigcomm.org/imc/2014/papers/p271.pdf.

Khormali, Aminollah, Park, Jeman, Alasmary, Hisham, Anwar, Afsah, Saad, Muhammad, Mohaisen, David, 2021. Domain name system security and privacy: A contemporary survey. Comput. Netw. 185, 107699. http://dx.doi.org/10.1016/j.comnet.2020.107699, URL https://linkinghub.elsevier.com/retrieve/pii/S1389128620313001.

Kiner, Emil, April, Tim, 2023. Google mitigated the largest DDoS attack to date, peaking above 398 million rps. URL https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps.

Kiner, Emil, Konduru, Satya, 2022. How Google Cloud blocked the largest layer 7 DDoS attack at 46 million rps. URL https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps.

King, Gary, Pan, Jennifer, Roberts, Margaret E., 2013. How censorship in China allows government criticism but silences collective expression. Am. Political Sci. Rev. 1, 18, URL https://gking.harvard.edu/files/censored.pdf.

Knockel, Jeffrey, Ruan, Lotus, 2021. Measuring QQMail's automated email censorship in China. In: Free and Open Communications on the Internet. ACM, Virtual Event, p. 8.

Kosseff, Jeff, 2019. The Twenty-Six Words That Created the Internet. Cornell University Press, Ithaca, New York.

Kwan, Carmen, Janiszewski, Paul, Qiu, Shela, Wang, Cathy, Bocovich, Cecylia, 2021. Exploring simple detection techniques for DNS-over-https tunnels. In: Free and Open Communications on the Internet. ACM, Virtual Event, USA, p. 6. http://dx.doi.org/10.1145/3473604.3474563.

Lamansky, Yumi, 2024. TCP Segmentation to Evade NIDS (Ph.D. thesis). Arizona State University, URL https://keep.lib.asu.edu/items/198214.

Let's Encrypt, 2021. Let's encrypt statistics. URL https://letsencrypt.org/stats/.

Li, Fangfan, Razaghpanah, Abbas, Kakhki, Arash Molavi, Niaki, Arian Akhavan, Choffnes, David, Gill, Phillipa, Mislove, Alan, 2017. Lib•erate, (n): A library for exposing (traffic-classification) rules and avoiding them efficiently. In: Proceedings of the 2017 Internet Measurement Conference. ACM, London, United Kingdom, pp. 128–141. http://dx.doi.org/10.1145/3131365.3131376, URL https://dl.acm.org/doi/10.1145/3131365.3131376.

Lian, Wilson, Rescorla, Eric, Shacham, Hovav, Savage, Stefan, 2013. Measuring the practical impact of DNSSEC deployment. USENIX Secur. Symp. 1, 16, URL https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_lian.pdf.

Loukas, G., Oke, G., 2010. Protection against denial of service attacks. Comput. J. 53, 17. http://dx.doi.org/10.1093/comjnl/bxp078.

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

Lu, Zhen, Li, Zhenhua, Yang, Jian, Xu, Tianyin, Zhai, Ennan, Liu, Yao, Wilson, Christo, 2017. Accessing Google Scholar under extreme internet censorship: A legal avenue. In: Middleware. ACM, Las Vegas, NV, p. 7, URL https://censorbib.nymity.ch/pdf/Lu2017a.pdf.

Lutscher, Philipp M., Weidmann, Nils B., Roberts, Margaret E., Jonker, Mattijs, King, Alistair, Dainotti, Alberto, 2020. At home and abroad: The Use of denial-of-service attacks during elections in nondemocratic regimes. J. Confl. Resolut. 64 (2–3), 373–401. http://dx.doi.org/10.1177/0022002719861676.

Luxmoore, Matthew, Czerny, Milan, 2026. Russia Shuts Off Internet in Moscow as It Tests Nationwide Censorship System. The Wall Street Journal, URL https://www.wsj.com/world/russia/russia-shuts-off-internet-in-moscow-as-it-tests-nationwide-censorship-system-3b44c0af.

Lyengar, J., Thomson, M., 2021. RFC 9000: A UDP-based multiplexed and secure transport. URL https://doi.org/10.17487/RFC9000.

Madiega, Tambiama, Luca, Stefano De, 2023. Collapse of the internet. In: Future Shocks 2023: Anticipating and Weathering the Next Storms. European Parliament, EU, pp. 34–39. http://dx.doi.org/10.2861/88235, URL https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751428/EPRS_STU(2023)751428_EN.pdf.

Mahjabin, Tasnuva, Xiao, Yang, Sun, Guang, Jiang, Wangdong, 2017. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. Int. J. Distrib. Sens. Networks 13 (12), 155014771774146. http://dx.doi.org/10.1177/1550147717741463, URL http://journals.sagepub.com/doi/10.1177/1550147717741463.

Manavi, Mousa Taghizadeh, 2018. Defense mechanisms against distributed denial of service attacks : A survey. Comput. Electr. Eng. 72, 26–38. http://dx.doi.org/10.1016/j.compeleceng.2018.09.001, URL https://linkinghub.elsevier.com/retrieve/pii/S0045790616307029.

Mangino, Antonio, Bou-Harb, Elias, 2021. A multidimensional network forensics investigation of a state-sanctioned internet outage. In: IWCMC 2021. IEEE, Harbin City, China, pp. 813–818. http://dx.doi.org/10.1109/IWCMC51323.2021.9498743, URL https://ieeexplore.ieee.org/document/9498743/.

Marczak, Bill, Weaver, Nicholas, Dalek, Jakub, Ensafi, Roya, Fifield, David, McKune, Sarah, Rey, Arn, Scott-Railton, John, Deibert, Ron, Paxson, Vern, 2015a. China's Great Cannon. Citizen Lab, Munk School of Global Affairs, University of Toronto, URL https://citizenlab.ca/research/chinas-great-cannon/.

Marczak, Bill, Weaver, Nicholas, Dalek, Jakub, Ensafi, Roya, Fifield, David, McKune, Sarah, Rey, Arn, Scott-Railton, John, Deibert, Ron, Paxson, Vern, 2015b. An analysis of China's "great cannon". In: Free and Open Communications on the Internet. USENIX, Washington, D.C., p. 11, URL https://www.usenix.org/system/files/conference/foci15/foci15-paper-marczak.pdf.

Marrow, Alexander, Antonov, Dmitry, 2021. Russia Disconnected from Global Internet in Tests: RBC Daily. Reuters, URL https://www.reuters.com/technology/russia-disconnected-global-internet-tests-rbc-daily-2021-07-22/.

Masinter, L., McCahill, M., 1994. RFC 1738: Uniform resource locators (URL). URL https://datatracker.ietf.org/doc/html/rfc1738.

Master, Alexander, 2023. Modeling and Characterization of Internet Censorship Technologies (Ph.D. thesis). Purdue University, p. 190. http://dx.doi.org/10.25394/PGS.23666784,

Master, Alexander, Garman, Christina, 2023. A worldwide view of nation-state internet censorship. In: Free and Open Communications on the Internet. Proceedings on Privacy Enhancing Technologies, Lausanne, Switzerland, p. 22, URL https://www.petsymposium.org/foci/2023/foci-2023-0008.pdf.

Master, Alexander, Gomber, Kendall, 2026. The PRC and cyberspace: Internet censorship, the social credit system, and Chinese cyberspace operations. In: De Gruyter Handbook of Cyber Conflict and Warfare. De Gruyter, DE, http://dx.doi.org/10.1515/9783111613031-016.

Matan Mates, 2022. Tor, Meek & The Rise And Fall Of Domain Fronting. Sentinel One, URL https://www.sentinelone.com/blog/privacy-2019-tor-meek-rise-fall-domain-fronting/. Updated October 27, 2022.

McDonald, Allison, Bernhard, Matthew, Valenta, Luke, VanderSloot, Benjamin, Scott, Will, Sullivan, Nick, Halderman, J. Alex, Ensafi, Roya, 2018. 403 forbidden: a global view of CDN geoblocking. In: Internet Measurement Conference, vol. 1, ACM, Boston, MA, USA, p. 13.

McHugh, Molly, 2011. Burma bans Skype, severing global communication. URL https://www.digitaltrends.com/computing/burma-bans-skype-severing-global-communication/.

Menscher, Damian, 2020. Exponential growth in DDoS attack volumes. URL https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks.

Mirkovic, Jelena, Reiher, Peter, 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Comput. Commun. Rev. 34 (2), 39–53. http://dx.doi.org/10.1145/997150.997156, URL https://dl.acm.org/doi/10.1145/997150.997156.

Mitseva, Asya, Panchenko, Andriy, Engel, Thomas, 2018. The state of affairs in BGP security: A survey of attacks and defenses. Comput. Commun. 124, 45–60. http://dx.doi.org/10.1016/j.comcom.2018.04.013, URL https://linkinghub.elsevier.com/retrieve/pii/S014036641731068X.

Mohajeri Moghaddam, Hooman, Li, Baiyu, Derakhshani, Mohammad, Goldberg, Ian, 2012. SkypeMorph: Protocol obfuscation for Tor bridges. In: ACM CCS 2012. ACM Press, Raleigh, NC, p. 97. http://dx.doi.org/10.1145/2382196.2382210.

Moher, David, Liberati, Alessandro, Tetzlaff, Jennifer, Altman, Douglas G., The PRISMA Group, 2009. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLoS Med. 6 (7), e1000097. http://dx.doi.org/10.1371/journal.pmed.1000097, URL https://dx.plos.org/10.1371/journal.pmed.1000097.

Mozilla, 2023. Encrypted client hello (ECH) - frequently asked questions. URL https://support.mozilla.org/en-US/kb/faq-encrypted-client-hello.

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

Müller, Philipp, Niere, Niklas, Lange, Felix, Somorovsky, Juraj, 2024. Turning attacks into advantages: Evading HTTP censorship with HTTP request smuggling. In: Free and Open Communications on the Internet. Proceedings on Privacy Enhancing Technologies, Bristol, UK, p. 12, URL https://www.petsymposium.org/foci/2024/foci-2024-0012.pdf.

Nabi, Zubair, 2013. The anatomy of web censorship in Pakistan. In: Free and Open Communications on the Internet. USENIX, Washington, D.C., p. 7, URL https://www.usenix.org/system/files/conference/foci13/foci13-nabi.pdf.

Nazario, Jose, 2009. Politically motivated denial of service attacks. In: Virtual Battlefield: Perspectives on Cyber Warfare, vol. 3, IOS Press, Ebook, p. 20.

Newman, Lily Hay, 2019. How the Iranian government shut off the internet. URL https://www.wired.com/story/iran-internet-shutoff/.

Niaki, Arian Akhavan, Cho, Shinyoung, Weinberg, Zachary, Hoang, Nguyen Phong, Razaghpanah, Abbas, Christin, Nicolas, Gill, Phillipa, 2020. ICLab: A global, longitudinal internet censorship measurement platform. In: 2020 IEEE Symposium on Security and Privacy. SP, IEEE, San Francisco, CA, USA, pp. 135–151. http://dx.doi.org/10.1109/SP40000.2020.00014, URL https://ieeexplore.ieee.org/document/9152784/.

Niere, Niklas, Lange, Felix, Heitmann, Nico, Somorovsky, Juraj, 2025a. Encrypted client hello (ECH) in censorship circumvention. In: Free and Open Communications on the Internet. FOCI, Washington D.C., p. 10, URL https://petsymposium.org/foci/2025/foci-2025-0016.pdf.

Niere, Niklas, Lange, Felix, Merget, Robert, Somorovsky, Juraj, 2025b. Transport layer obscurity: Circumventing SNI censorship on the TLS layer. In: Symposium on Security & Privacy. IEEE, San Francisco, USA, p. 18, URL https://www.computer.org/csdl/pds/api/csdl/proceedings/download-article/26hiUekZ19S/pdf.

Nisar, Aqib, Kashaf, Aqsa, Qazi, Ihsan Ayyub, Uzmi, Zartash Afzal, 2018. Incentivizing censorship measurements via circumvention. In: SIGCOMM. ACM, Budapest, Hungary, p. 14. http://dx.doi.org/10.1145/3230543.3230568, URL https://dl.acm.org/authorize?N666961.

Nixon, Leif, 2011. Some observations on the great firewall of China. URL https://www.nsc.liu.se/~nixon/sshprobes.html.

Nobori, Daiyuu, Shinjo, Yasushi, 2014. VPN gate: A volunteer-organized public VPN relay system with blocking resistance for bypassing government censorship firewalls. In: Networked Systems Design and Implementation. USENIX, Philadelphia, PA, p. 14, URL https://www.usenix.org/system/files/conference/nsdi14/nsdi14-paper-nobori.pdf.

Nourin, Sadia, Bock, Kevin, Hoang, Nguyen Phong, Levin, Dave, 2023a. Detecting network interference without endpoint participation. In: Free and Open Communications on the Internet. Proceedings on Privacy Enhancing Technologies, Lausanne, Switzerland, p. 5, URL https://www.petsymposium.org/foci/2023/foci-2023-0010.pdf.

Nourin, Sadia, Tran, Van, Jiang, Xi, Bock, Kevin, Feamster, Nick, Hoang, Nguyen Phong, Levin, Dave, 2023b. Measuring and evading Turkmenistan's internet censorship: A case study in large-scale measurements of a low-penetration country. In: Proceedings of the ACM Web Conference 2023. ACM, Austin TX USA, p. 11. http://dx.doi.org/10.1145/3543507.3583189, URL https://dl.acm.org/doi/10.1145/3543507.3583189.

ntop, 2022. nDPI - open and extensible LGPLv3 deep packet inspection library. URL https://www.ntop.org/products/deep-packet-inspection/ndpi/.

Oakley, Jonathan, Yu, Lu, Zhong, Xingsi, Venayagamoorthy, Ganesh Kumar, Brooks, Richard, 2020. Protocol proxy: An FTE-based covert channel. Comput. Secur. 92, 11, URL https://censorbib.nymity.ch/pdf/Oakley2020a.pdf.

obfuscation group, 2015. Pluggable transports. URL https://obfuscation.github.io/.

Ognyanova, Katherine, Lazer, David, Robertson, Ronald, Wilson, Christo, 2020. Misinformation in action: Fake news exposure is linked to lower trust in media, higher trust in government when your side is in power. Harv. Kennedy Sch. Misinformation Rev. 1 (4), 12. http://dx.doi.org/10.37016/mr-2020-024.

Okoli, Chitu, Schabram, Kira, 2010. A guide to conducting a systematic literature review of information systems research. SSRN Electron. J. 1, 51. http://dx.doi.org/10.2139/ssrn.1954824, URL http://www.ssrn.com/abstract=1954824.

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

Ortiz Freuler, Juan, 2022. The weaponization of private corporate infrastructure: Internet fragmentation and coercive diplomacy in the 21st century. Glob. Media China 1, 18. http://dx.doi.org/10.1177/20594364221139729, URL http://journals.sagepub.com/doi/10.1177/20594364221139729.

Ortwein, Aaron, Bock, Kevin, Levin, Dave, 2023. Towards a comprehensive understanding of Russian transit censorship. In: Free and Open Communications on the Internet. PoPETS, Lausanne, Switzerland, p. 7, URL https://www.petsymposium.org/foci/2023/foci-2023-0012.pdf.

Padmanabhan, Ramakrishna, Filastò, Arturo, Xynou, Maria, Raman, Ram Sundara, Middleton, Kennedy, Zhang, Mingwei, Madory, Doug, Roberts, Molly, Dainotti, Alberto, 2021. A multi-perspective view of internet censorship in Myanmar. In: Free and Open Communications on the Internet. ACM, Virtual Event, USA, p. 10. http://dx.doi.org/10.1145/3473604.3474562, URL https://dl.acm.org/doi/10.1145/3473604.3474562.

Palo Alto Networks, 2018a. How to block a specific HTTPS site with URL filtering. URL https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClIPCA0.

Palo Alto Networks, 2018b. How to block tor. URL https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRtCAK.

Park, Jong Chun, Crandall, Jedidiah R., 2010. Empirical study of a national-scale distributed intrusion detection system: Backbone-Level Filtering of HTML responses in China. In: Distributed Computing Systems. IEEE, Genoa, Italy, p. 12, URL https://www.cs.unm.edu/~crandall/icdcs2010.pdf.

Pearce, Paul, Jones, Ben, Li, Frank, Ensafi, Roya, Feamster, Nick, Weaver, Nick, Paxson, Vern, 2017. Global measurement of DNS manipulation. In: USENIX Security. USENIX, Vancouver, Canada, p. 19, URL https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-pearce.pdf.

Pereira, Hugo Gamaliel Dos Santos, 2024. MIRACE: Multi-Path Integrated Routing Architecture for Censorship Evasion (Ph.D. thesis). Universidade Nova De Lisboa, URL https://run.unl.pt/bitstream/10362/178441/1/Pereira_2024.pdf.

Peters, Jay, 2024. Signal has been blocked by Venezuela and Russia. URL https://www.theverge.com/2024/8/9/24217008/signal-blocked-venezuela-russia.

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

PowerTunnel, 2023. PowerTunnel - powerful and extensible proxy server. URL https://github.com/krlvm/PowerTunnel.

Preti, Christian, Harrell, Nicholas, Master, Alexander, 2026. Privacy under pressure: assessing online commercial surveillance countermeasures and gaps. In: The Proceedings of the 25th European Conference on Cyber Warfare & Security (ECCWS 2026). 25, (1), http://dx.doi.org/10.34190/eccws.25.1.4688.

Raman, Ram Sundara, Evdokimov, Leonid, Wurstrow, Eric, Halderman, J. Alex, Ensafi, Roya, 2020a. Investigating large scale HTTPS interception in Kazakhstan. In: Proceedings of the ACM Internet Measurement Conference. ACM, Virtual Event, USA, pp. 125–132. http://dx.doi.org/10.1145/3419394.3423665, URL https://dl.acm.org/doi/10.1145/3419394.3423665.

Raman, Ram Sundara, Stoll, Adrian, Dalek, Jakub, Ramesh, Reethika, Scott, Will, Ensafi, Roya, 2020b. Measuring the deployment of network censorship filters at global scale. In: Proceedings of 2020 NDSS. NDSS, San Diego, CA, p. 16. http://dx.doi.org/10.14722/ndss.2020.23099.

Raman, Ram Sundara, Wang, Mona, Dalek, Jakub, Mayer, Jonathan, Ensafi, Roya, 2022. Network measurement methods for locating and examining censorship devices. In: Emerging Networking Experiments and Technologies. ACM, Roma, Italy, p. 17. http://dx.doi.org/10.1145/3555050.3569133, URL https://dl.acm.org/doi/pdf/10.1145/3555050.3569133.

Ramesh, Reethika, Evdokimov, Leonid, Xue, Diwen, Ensafi, Roya, 2022. VPNalyzer: Systematic Investigation of the VPN ecosystem. In: Proceedings 2022 Network and Distributed System Security Symposium. Internet Society, San Diego, CA, USA, p. 16. http://dx.doi.org/10.14722/ndss.2022.24285, URL https://www.ndss-symposium.org/wp-content/uploads/2022-285-paper.pdf.

Ramesh, Reethika, Raman, Ram Sundara, Bernhard, Matthew, Ongkowijaya, Victor, Evdokimov, Leonid, Edmundson, Anne, Sprecher, Steven, Ikram, Muhammad, Ensafi, Roya, 2020. Decentralized control: A case study of Russia. In: Proceedings 2020 Network and Distributed System Security Symposium. Internet Society, San Diego, CA, p. 18. http://dx.doi.org/10.14722/ndss.2020.23098, URL https://www.ndss-symposium.org/wp-content/uploads/2020/02/23098.pdf.

Ramesh, Reethika, Raman, Ram Sundara, Virkud, Apurva, Dirksen, Alexandra, Huremagic, Armin, Fifield, David, Rodenburg, Dirk, Hynes, Rod, Madory, Doug, Ensafi, Roya, 2023. Network responses to Russia's invasion of Ukraine in 2022: A cautionary tale for internet freedom. In: USENIX Security Symposium. USENIX, Anaheim, CA, USA, p. 19, URL https://censoredplanet.org/assets/russia-ukraine-invasion.pdf.

Reid, Amanda, 2019. Considering fair use: DMCA's take down & repeat infringers policies. Commun. Law Policy 24 (1), 101–141. http://dx.doi.org/10.1080/10811680.2018.1551036, URL https://www.tandfonline.com/doi/full/10.1080/10811680.2018.1551036.

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

Reuters, 2022. Russia blocks access to BBC and voice of America websites. URL https://www.reuters.com/business/media-telecom/russia-restricts-access-bbc-russian-service-radio-liberty-ria-2022-03-04/.

Reuters Staff, 2018. Businesses, consumers uncertain ahead of China VPN ban. URL https://www.reuters.com/article/us-china-vpns/businesses-consumers-uncertain-ahead-of-china-vpn-ban-idUSKBN1H612F,

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

Roberts, Margaret E., 2018. Blocked: How Control of China's Internet and Social Media Allows the State to Dictate the Narrative. Cambridge University Press, Cambridge, http://dx.doi.org/10.1017/9781108551502.

Roberts, Margaret E., 2020. Censored: Distraction and Diversion inside China's Great Firewall. Princeton University Press, Princeton.

Roberts, Hal, Zuckerman, Ethan, York, Jillian, Faris, Robert, Palfrey, John, 2010. 2010 circumvention tool usage report. Berkman Cent. Res. Publ. No. 2010 1, 13, URL https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf.

Rosen, Marc B., Parker, James, Malozemoff, Alex J., 2021. Balboa: Bobbing and weaving around network censorship. In: USENIX Security Symposium. USENIX, Virtual Event, USA, p. 16, URL https://www.usenix.org/system/files/sec21-rosen.pdf.

Roskomnadzor, 2021. Roskomnadzor takes measures to protect Russian citizens from the influence of illegal content. URL https://rkn.gov.ru/news/rsoc/news73464.htm.

Ruo, Samuel, Knockel, Jeffrey, Reichert, Zoë, 2024. Lost in translation: Characterizing automated censorship in online translation services. In: Free and Open Communications on the Internet. Proceedings on Privacy Enhancing Technologies, Bristol, UK, p. 9.

Ruthven, Malise, 2016. How to understand ISIS. URL https://www.nybooks.com/articles/2016/06/23/how-to-understand-isis/.

Ryng, Julia, Guicherd, Guillemette, Saman, Judy Al, Choudhury, Priyanka, Kellett, Angharad, 2022. Internet shutdowns: A human rights issue. RUSI J. 167 (4–5), 50–63. http://dx.doi.org/10.1080/03071847.2022.2156234, URL https://www.tandfonline.com/doi/full/10.1080/03071847.2022.2156234.

Sambaluk, Nicholas Michael, Spafford, Eugene, 2020. Myths and Realities of Cyber Warfare: Conflict in the Digital Realm. Praeger Security International, Santa Barbara, CA.

Satariano, Adam, 2022. How Russia took over Ukraine's internet in occupied territories. URL https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html.

Satija, Sambhav, Chatterjee, Rahul, 2021. BlindTLS: Circumventing TLS-Based HTTPS Censorship. In: Free and Open Communications on the Internet. ACM, Virtual Event, USA, p. 7. http://dx.doi.org/10.1145/3473604.3474564.

Sauter, Molly, 2014. The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet, first ed. Bloomsbury Publishing Inc, New York, NY, http://dx.doi.org/10.5040/9781628926705, URL https://www.bloomsburycollections.com/book/the-coming-swarm-ddos-actions-hacktivism-and-civil-disobedience-on-the-internet.

Schroeder, Jared, 2022. Meet the EU law that could reshape online speech in the U.S.. URL https://slate.com/technology/2022/10/digital-services-act-european-union-content-moderation.html.

Scott, Will, Anderson, Thomas, Kohno, Tadayoshi, Krishnamurthy, Arvind, 2016. Satellite: Joint analysis of CDNs and network-level interference. In: Proceedings of 2016 USENIX Conference. USENIX, Austin, TX, p. 15, URL https://www.usenix.org/system/files/conference/atc16/atc16_paper-scott.pdf.

Serabian, Ryan, Kapellmann Zafra, Daniel, 2022. Pro-PRC "HaiEnergy" information operations campaign leverages infrastructure from public relations firm to disseminate content on inauthentic news sites. URL https://www.mandiant.com/resources/blog/pro-prc-information-operations-campaign-haienergy.

Sfakianakis, Andreas, Athanasopoulos, Elias, Ioannidis, Sotiris, 2011. CensMon: A Web Censorship Monitor. In: Free and Open Communications on the Internet. USENIX, Bellevue, WA, p. 6, URL https://www.usenix.org/legacy/events/foci11/tech/final_files/Sfakianakis.pdf.

Shah, Nishant, 2021. (Dis)information blackouts: Politics and practices of internet shutdowns. Int. J. Commun. 15, 17.

Shavitt, Y., Zilberman, N., 2012. Arabian nights: Measuring the Arab internet during the 2011 events. IEEE Netw. 26 (6), 75–80. http://dx.doi.org/10.1109/MNET.2012.6375897, URL http://ieeexplore.ieee.org/document/6375897/.

Sheffey, Jade, Zohaib, Ali, Kang, Dayeon, Durumeric, Zakir, Houmansadr, Amir, Wu, Qiang, 2025. Extended abstract: I'll shake your hand: What happens after DNS poisoning. In: Free and Open Communications on the Internet. FOCI, Washington D.C., p. 4, URL https://petsymposium.org/foci/2025/foci-2025-0015.pdf.

Shen, Xiaoxiao, Truex, Rory, 2021. In search of self-censorship. Br. J. Political Sci. 51 (4), 1672–1684. http://dx.doi.org/10.1017/S0007123419000735, URL https://www.cambridge.org/core/product/identifier/S0007123419000735/type/journal_article.

Sherry, Justine, Lan, Chang, Popa, Raluca, Ratnasamy, Sylvia, 2015. BlindBox: Deep packet inspection over encrypted traffic. In: Proceedings of 2015 ACM Conference on Special Interest Group on Data Communication. ACM, London, UK, p. 13. http://dx.doi.org/10.1145/2785956.2787502.

Siby, Sandra, Juarez, Marc, Diaz, Claudia, Vallina-Rodriguez, Narseo, Troncoso, Carmela, 2020. Encrypted DNS –> privacy? a traffic analysis perspective. In: Proceedings of 2020 NDSS. Internet Society, San Diego, CA, p. 19. http://dx.doi.org/10.14722/ndss.2020.24301, URL https://www.ndss-symposium.org/wp-content/uploads/2020/02/24301.pdf.

Singh, Kushagra, Grover, Gurshabad, Bansal, Varun, 2020. How India censors the web. In: 12th ACM Conference on Web Science. ACM, Southampton United Kingdom, pp. 21–28. http://dx.doi.org/10.1145/3394231.3397891, URL https://dl.acm.org/doi/10.1145/3394231.3397891.

Singh, Rachee, Nithyanand, Rishab, Afroz, Sadia, Pearce, Paul, Tschantz, Michael, Gill, Phillipa, Paxson, Vern, 2017. Characterizing the nature and dynamics of tor exit blocking. In: USENIX Security Symposium. USENIX, Vancouver, Canada, p. 19, URL https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-singh.pdf.

Smith, Charlie, 2015. We are under attack. URL https://en.greatfire.org/blog/2015/mar/we-are-under-attack.

Software Freedom Law Centre, 2020. Internet shutdowns. URL https://internetshutdowns.in/.

Soldatov, Andrei, Borogan, Irina, 2015. The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries. PublicAffairs, New York, NY.

Statista, 2024. Global market share held by leading internet browsers from January 2012 to August 2024. URL https://www.statista.com/statistics/268254/market-share-of-internet-browsers-worldwide-since-2009/.

Sundara Raman, Ram, Merino, Louis-Henri, Bock, Kevin, Fayed, Marwan, Levin, Dave, Sullivan, Nick, Valenta, Luke, 2023. Global, passive detection of connection tampering. In: Proceedings of the ACM SIGCOMM. ACM, New York, NY, pp. 622–636. http://dx.doi.org/10.1145/3603269.3604875.

Sundara Raman, Ram, Shenoy, Prerana, Kohls, Katharina, Ensafi, Roya, 2020. Censored planet: An Internet-wide, longitudinal censorship observatory. In: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. ACM, Virtual Event, USA, pp. 49–66. http://dx.doi.org/10.1145/3372297.3417883, URL https://dl.acm.org/doi/10.1145/3372297.3417883.

Tai, Jonas, Sengottuvelavan, Karthik Nishanth, Whiting, Peter, Hoang, Nguyen Phong, 2025. IRBlock: A large-scale measurement study of the great firewall of Iran. In: USENIX Security Symposium. USENIX, Seattle, USA, p. 19, URL https://www.usenix.org/system/files/usenixsecurity25-tai.pdf.

Tanash, Rima, Chen, Zhouhan, Wallach, Dan, Marschall, Melissa, 2017. 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, Vancouver, BC, Canada, p. 7, URL https://www.usenix.org/system/files/conference/foci17/foci17-paper-tanash.pdf.

Technical Working Group, BITAG, 2013. Port Blocking. Technical Report, BITAG, Virtual, p. 34, URL http://www.ssrn.com/abstract=2701485.

The World Bank, 2022. % of population using the internet - Myanmar. URL https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=MM.

Tikk, Eneken, Kaska, Kadri, Rünnimeri, Kristel, Kert, Mari, Talihärm, Anna-Maria, Vihul, Liis, 2008. Cyber Attacks Against Georgia: Legal Lessons Identified. Technical Report, Cooperative Cyber Defense Center of Excellence, Tallinn, Estonia, p. 46, URL http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

Tinworth, Adam, 2018. Happy GDPR day!. URL https://twitter.com/adders/status/999976701089189890/photo/1.

Tor, 2022. Tor usage statistics during invasion of Ukraine 2022. URL https://web.archive.org/web/20230105232136/https://web.ics.purdue.edu/~amaster/anticensorship/Tor_usage_Ukraine_invasion.png.

Trevelyan, Mark, 2022. Russians' demand for VPNs skyrockets after Meta block. URL https://www.reuters.com/technology/russians-demand-vpns-skyrockets-after-meta-block-2022-03-14/.

Tripathi, Nikhil, Hubballi, Neminath, 2021. Application layer denial-of-service attacks and defense mechanisms: A Survey. ACM Comput. Surv. 54 (4), 1–33. http://dx.doi.org/10.1145/3448291, URL https://dl.acm.org/doi/10.1145/3448291.

Tsai, Elisa, Raman, Ram Sundara, Prakash, Atul, Ensafi, Roya, 2024. Modeling and detecting internet censorship events. In: Network and Distributed System Security. NDSS, San Diego, CA, USA, p. 17, URL https://www.ndss-symposium.org/wp-content/uploads/2024-409-paper.pdf.

Tschantz, Michael Carl, Afroz, Sadia, Anonymous, Paxson, Vern, 2016. SoK: Towards grounding censorship circumvention in empiricism. In: 2016 IEEE Symposium on Security and Privacy. SP, IEEE, San Jose, CA, pp. 914–933. http://dx.doi.org/10.1109/SP.2016.59, URL http://ieeexplore.ieee.org/document/7546542/.

Tschantz, Michael Carl, Afroz, Sadia, Sajid, Shaarif, Qazi, Shoaib Asif, Javed, Mobin, Paxson, Vern, 2018. A bestiary of blocking: The Motivations and modes behind website unavailability. In: Free and Open Communications on the Internet. USENIX, Baltimore, MD, USA, p. 9, URL https://www.usenix.org/system/files/conference/foci18/foci18-paper-tschantz.pdf.

Underwood, Todd, 2005. Internet-wide catastrophe - last year. URL https://web.archive.org/web/20080228131639/http://www.renesys.com/blog/2005/12/internetwide_nearcatastrophela.shtml.

United Nations, 1948. Universal declaration of human rights: Article 19. URL https://www.un.org/en/about-us/universal-declaration-of-human-rights.

United Nations, 2021. Right to freedom of expression in Myanmar must be guaranteed, UN expert urges military coup leader. URL https://news.un.org/en/story/2021/04/1090742.

U.S. Army, 2020. ATP 7-100.2 North Korean Tactics. Army Techniques Publication, U.S. Army.

U.S. Department of Justice, 2022. Press release: United States leads seizure of one of the world's largest hacker forums and arrests administrator. URL https://www.justice.gov/opa/pr/united-states-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator.

U.S. Strategic Command, 2009. The Cyber Warfare Lexicon. Technical Report, USSTRATCOM, URL https://info.publicintelligence.net/USSTRATCOM-CyberWarfareLexicon.pdf.

Van Leeuwen, Brian, Gao, Jason, Yin, Haikuo, Anthony, Benjamin, Urias, Vincent, 2019. 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, http://dx.doi.org/10.2172/1863848, SAND2019–13774, 1863848, 705224. URL https://www.osti.gov/servlets/purl/1863848/.

van Rijswijk-Deij, Roland, Sperotto, Anna, Pras, Aiko, 2015. Making the case for elliptic curves in DNSSEC. ACM SIGCOMM Comput. Commun. Rev. 45 (5), 13–19. http://dx.doi.org/10.1145/2831347.2831350, URL https://dl.acm.org/doi/10.1145/2831347.2831350.

VanderSloot, Benjamin, McDonald, Allison, Scott, Will, Halderman, J Alex, Ensafi, Roya, 2018. Quack: Scalable Remote Measurement of application-layer censorship. In: USENIX Security Symposium. USENIX, Baltimore, MD, USA, p. 16.

Velan, Petr, Čermák, Milan, Čeleda, Pavel, Drašar, Martin, 2015. A survey of methods for encrypted traffic classification and analysis. Int. J. Netw. Manage. 25 (5), 355–374. http://dx.doi.org/10.1002/nem.1901, URL https://onlinelibrary.wiley.com/doi/10.1002/nem.1901.

Velghe, Pieter, 2019. "Reading China": The Internet of things, surveillance, and social management in the PRC. China Perspect. 2019 (1), 85–89. http://dx.doi.org/10.4000/chinaperspectives.8874, URL http://journals.openedition.org/chinaperspectives/8874.

Verkamp, John-Paul, Gupta, Minaxi, 2012. Inferring mechanics of web censorship around the world. In: Free and Open Communications on the Internet. USENIX, Bellevue, WA, p. 7, URL https://www.usenix.org/conference/foci12/workshop-program/presentation/Verkamp.

Ververis, Vasilis, Isaakidis, Marios, Loizidou, Chrystalleni, Fabian, Benjamin, 2017. Internet censorship capabilities in cyprus: An Investigation of online gambling blocklisting. In: Katsikas, Sokratis K., Zorkadis, Vasilios (Eds.), In: E-Democracy – Privacy-Preserving, Secure, Intelligent E-Government Services, vol. 792, Springer International Publishing, Cham, pp. 136–149. http://dx.doi.org/10.1007/978-3-319-71117-1_10, URL http://link.springer.com/10.1007/978-3-319-71117-1_10.

Ververis, Vasilis, Kargiotakis, George, Filastò, Arturo, Fabian, Benjamin, Alexandros, Afentoulis, 2015. Understanding internet censorship policy: The Case of Greece. In: Free and Open Communications on the Internet. USENIX, Washington, D.C., p. 11.

Wang, Zhongjie, Cao, Yue, Qian, Zhiyun, Song, Chengyu, Krishnamurthy, Srikanth V., 2017. Your state is not mine: A Closer Look at evading stateful internet censorship. In: Internet Measurement Conference. ACM, London United Kingdom, p. 14. http://dx.doi.org/10.1145/3131365.3131374, URL http://www.cs.ucr.edu/~krish/imc17.pdf.

Wang, Liang, Dyer, Kevin P., Akella, Aditya, Ristenpart, Thomas, Shrimpton, Thomas, 2015. Seeing through network-protocol obfuscation. In: Computer and Communications Security. ACM, Denver, CO, USA, p. 13, URL http://pages.cs.wisc.edu/~liangw/pub/ccsfp653-wangA.pdf.

Wang, Qiyan, Gong, Xun, Nguyen, Giang T.K., Houmansadr, Amir, Borisov, Nikita, 2012. CensorSpoofer: Asymmetric communication using IP spoofing for censorship-resistant web browsing. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security - CCS '12. ACM Press, Raleigh, North Carolina, USA, p. 121. http://dx.doi.org/10.1145/2382196.2382212, URL http://dl.acm.org/citation.cfm?doid=2382196.2382212.

Wang, Stephanie, Nagaraja, Shishir, 2007. A Technical Review of the Internet Shutdown in Burma. Technical Report, ONI, OpenNet Initiative, p. 14, URL https://web.archive.org/web/20210701131103/https://opennet.net/sites/opennet.net/files/ONI_Bulletin_Burma_2007.pdf.

Wang, Gaukas, Sippe, Jackson, Anonymous, Chi, Hai, Wustrow, Eric, 2023. Chasing shadows: A security analysis of the shadowtls proxy. In: Free and Open Communications on the Internet. Proceedings on Privacy Enhancing Technologies, Lausanne, Switzerland, p. 7, URL https://petsymposium.org/foci/2023/foci-2023-0002.pdf.

Wang, Chenxu, Yin, Jiangyi, Li, Zhao, Xu, Hongbo, Zhang, Zhongyi, Liu, Qingyun, 2024. Identifying VPN servers through graph-represented behaviors. In: Proceedings of the ACM Web Conference 2024. ACM, Singapore Singapore, p. 10. http://dx.doi.org/10.1145/3589334.3645552, URL https://dl.acm.org/doi/10.1145/3589334.3645552.

Wang, Zhongjie, Zhu, Shitong, Cao, Yue, Qian, Zhiyun, Song, Chengyu, Krishnamurthy, Srikanth V., Chan, Kevin S., Braun, Tracy D., 2020. SymTCP: eluding stateful deep packet inspection with automated discrepancy discovery. In: Proceedings 2020 Network and Distributed System Security Symposium. Internet Society, San Diego, CA, p. 17. http://dx.doi.org/10.14722/ndss.2020.24083, URL https://www.ndss-symposium.org/wp-content/uploads/2020/02/24083.pdf.

Watney, Murdoch, 2014. Determining when conduct in cyberspace constitutes cyber warfare in terms of the international law and tallinn manual on the international law applicable to cyber warfare: A Synopsis. In: International Conference on Digital Forensics and Cyber Crime, vol. 132, Institute for Computer Sciences, Johannesburg, South Africa, pp. 130–143. http://dx.doi.org/10.1007/978-3-319-14289-0_10.

Weaver, Nicholas, Sommer, Robin, Paxson, Vern, 2009. Detecting forged TCP reset packets. In: NDSS. NDSS, San Diego, CA, USA, p. 14, URL https://www.ndss-symposium.org/wp-content/uploads/2017/09/weav.pdf.

Weinberg, Zachary, Barradas, Diogo, Christin, Nicolas, 2021. Chinese wall or Swiss cheese? keyword filtering in the great firewall of China. In: Proceedings of the Web Conference 2021. ACM, Ljubljana Slovenia, pp. 472–483. http://dx.doi.org/10.1145/3442381.3450076, URL https://dl.acm.org/doi/10.1145/3442381.3450076.

Weinberg, Zachary, Sharif, Mahmood, Szurdi, Janos, Christin, Nicolas, 2017. Topics of controversy: An Empirical Analysis of web censorship lists. Priv. Enhanc. Technol. 2017 (1), 42–61, URL https://petsymposium.org/2017/papers/issue1/paper06-2017-1-source.pdf.

Weinberg, Zachary, Wang, Jeffrey, Yegneswaran, Vinod, Briesemeister, Linda, Cheung, Steven, Wang, Frank, Boneh, Dan, 2012. StegoTorus: A camouflage proxy for the Tor anonymity system. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security - CCS '12. ACM Press, Raleigh, North Carolina, USA, p. 109. http://dx.doi.org/10.1145/2382196.2382211, URL http://dl.acm.org/citation.cfm?doid=2382196.2382211.

Wendzel, Steffen, Volpert, Simon, Zillien, Sebastian, Lenz, Julia, Runz, Philip, Caviglione, Luca, 2025. A survey of internet censorship and its measurement: Methodology, trends, and challenges. URL https://arxiv.org/abs/2502.14945.

Wiley, Brandon, 2011. Dust: A Blocking-Resistant Internet Transport Protocol. Technical Report, School of Information, University of Texas at Austin, University of Texas, Austin, p. 12, URL https://www.freehaven.net/anonbib/cache/wileydust.pdf.

Winter, Philipp, 2014. Measuring and Circumventing Internet Censorship (Ph.D. thesis). Karlstad University, URL https://www.diva-portal.org/smash/get/diva2:758124/FULLTEXT01.pdf.

Winter, Philipp, 2023. NullHypothesis / censorbib. URL https://github.com/NullHypothesis/censorbib.

Winter, Philipp, Lindskog, Stefan, 2012. How the great firewall of China is blocking tor. In: Free and Open Communications on the Internet. USENIX, Bellevue, WA, p. 7, URL https://www.usenix.org/system/files/conference/foci12/foci12-final2.pdf.

Winter, Philipp, Pulls, Tobias, Fuss, Juergen, 2013. ScrambleSuit: A polymorphic network protocol to circumvent censorship. In: Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society. ACM, Berlin Germany, pp. 213–224. http://dx.doi.org/10.1145/2517840.2517856, URL https://dl.acm.org/doi/10.1145/2517840.2517856.

Wolfgarten, Sebastian, 2006. Investigating Large-Scale Internet Content Filtering. Technical Report, Dublin City University, Dublin, Ireland, URL http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.133.5778&rep=rep1&type=pdf.

Woodcock, Bill, 2011. Overview of the Egyptian internet shutdown. URL https://web.archive.org/web/20120125051846/http://www.pch.net/resources/misc/Egypt-PCH-Overview.pdf.

Woodhams, Samuel, Migliano, Simon, 2022. Cost of internet shutdowns report 2021. URL https://www.top10vpn.com/research/cost-of-internet-shutdowns/2021/.

Wright, Robin B., 2011. Rock the Casbah: Rage and Rebellion across the Islamic World, first ed. Simon & Schuster, New York.

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

Wu, Tim, 2003. Network neutrality, broadband discrimination. J. Telecommun. High Technol. Law 2 (1), 36.

Wu, Mingshi, Sippe, Jackson, Sivakumar, Danesh, Burg, Jack, Anderson, Peter, Wang, Xiaokang, Bock, Kevin, Houmansadr, Amir, Levin, Dave, Wustrow, Eric, 2023. How the great firewall of China detects and blocks fully encrypted traffic. In: USENIX Security Symposium. USENIX, Anaheim, CA, USA, p. 12, URL https://www.usenix.org/system/files/sec23fall-prepub-234-wu-mingshi.pdf.

Wu, Mingshi, Zohaib, Ali, Durumeric, Zakir, Houmansadr, Amir, Wustrow, Eric, 2025. A wall behind a wall: Emerging regional censorship in China. In: Symposium on Security & Privacy. IEEE, San Fransisco, USA, p. 18, URL https://gfw.report/publications/sp25/data/paper/paper.pdf.

Xie, Yinglian, Yu, Fang, Achan, Kannan, Gillum, Eliot, Goldszmidt, Moises, Wobber, Ted, 2007. How dynamic are IP addresses? In: Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. ACM, Kyoto Japan, pp. 301–312. http://dx.doi.org/10.1145/1282380.1282415, URL https://dl.acm.org/doi/10.1145/1282380.1282415.

Xiong, Ruohan, Knockel, Jeffrey, 2019. An efficient method to determine which combination of keywords triggered automatic filtering of a message. In: FOCI Workshop. USENIX, Santa Clara, CA, USA, p. 9, URL https://www.usenix.org/system/files/foci19-paper_xiong.pdf.

Xu, Xueyang, Mao, Z. Morley, Halderman, J., 2011. Internet censorship in China: Where Does the filtering occur? In: Spring, Neil, Riley, George F. (Eds.), In: Passive and Active Measurement, vol. 6579, Springer, Berlin, Heidelberg, pp. 133–142. http://dx.doi.org/10.1007/978-3-642-19260-9_14, URL http://link.springer.com/10.1007/978-3-642-19260-9_14.

Xue, Diwen, Ablove, Anna, Ramesh, Reethika, Danciu, Grace, Ensafi, Roya, 2024. Bridging barriers: A survey of challenges and priorities in the censorship circumvention landscape. In: USENIX Security Symposium. USENIX, Philadelphia, PA, p. 19, URL https://www.usenix.org/system/files/usenixsecurity24-xue-bridging.pdf.

Xue, Diwen, Mixon-Baca, Benjamin, Ablove, Anna, Kujath, Beau, Crandall, Jedidiah, Ensafi, Roya, 2022a. TSPU: Russia's decentralized censorship system. In: Proceedings of the 22nd ACM Internet Measurement Conference. ACM, Nice France, pp. 179–194. http://dx.doi.org/10.1145/3517745.3561461, URL https://dl.acm.org/doi/10.1145/3517745.3561461.

Xue, Diwen, Ramesh, Reethika, Jain, Arham, Kallitsis, Michalis, Halderman, J. Alex, Crandall, Jedidiah R., Ensafi, Roya, 2022b. OpenVPN is open to VPN fingerprinting. In: USENIX Security Symposium. USENIX, Boston, MA, USA, p. 19, URL https://www.usenix.org/system/files/sec22-xue-diwen.pdf.

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

Xue, Diwen, Stanley, Robert, Kumar, Piyush, Ensafi, Roya, 2025. The discriminative power of cross-layer RTTs in fingerprinting proxy traffic. In: Network and Distributed System Security. The Internet Society, San Diego, USA, p. 18, URL https://www.ndss-symposium.org/wp-content/uploads/2025-966-paper.pdf.

Xynou, Maria, Filastò, Arturo, 2021. How countries attempt to block signal private messenger app around the world. URL https://ooni.org/post/2021-how-signal-private-messenger-blocked-around-the-world/.

Yadav, Tarun Kumar, Sinha, Akshat, Gosain, Devashish, Sharma, Piyush, Chakravarty, Sambuddho, 2018. Where the light gets in: Analyzing Web Censorship Mechanisms in India. In: Internet Measurement Conference. ACM, Boston, USA, p. 13. http://dx.doi.org/10.1145/3278532.3278555.

Yang, Stephanie, 2021. China appears to block popular encrypted messaging app signal. URL https://www.wsj.com/articles/china-appears-to-block-signal-one-of-last-popular-encrypted-messaging-apps-11615883434.

Yoachimik, Omer, 2022. Cloudflare mitigates 26 million request per second DDoS attack. URL https://blog.cloudflare.com/26m-rps-ddos/.

Zannettou, Savvas, Caulfield, Tristan, De Cristofaro, Emiliano, Sirivianos, Michael, Stringhini, Gianluca, Blackburn, Jeremy, 2019. Disinformation warfare: Understanding State-Sponsored Trolls on Twitter and their influence on the web. In: Companion Proceedings of the 2019 World Wide Web Conference. ACM, San Francisco USA, pp. 218–226. http://dx.doi.org/10.1145/3308560.3316495, URL https://dl.acm.org/doi/10.1145/3308560.3316495.

Zargar, Saman Taghavi, Joshi, James, Tipper, David, 2013. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Commun. Surv. Tutor. 15 (4), 2046–2069. http://dx.doi.org/10.1109/SURV.2013.031413.00127, URL http://ieeexplore.ieee.org/document/6489876/.

Zetter, Kim, 2016. The sony hackers were causing mayhem years before they hit the company. URL https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company/.

Zhu, Pengxiong, Man, Keyu, Wang, Zhongjie, Qian, Zhiyun, Ensafi, Roya, Halderman, J., Duan, Haixin, 2020. Characterizing transnational internet performance and the great bottleneck of China. Meas. Anal. Comput. Syst. 4, 23. http://dx.doi.org/10.1145/3379479.

Zhu, Tao, Phipps, David, Pridgen, Adam, Crandall, Jedidiah R., Wallach, Dan S., 2013. The velocity of censorship: High-Fidelity Detection of microblog post deletions. In: USENIX Security Symposium. USENIX, Washington, D.C., p. 14, URL https://www.cs.unm.edu/~crandall/usenix13.pdf.

Zohaib, Ali, Zao, Qiang, Sippe, Jackson, Alaraj, Abdulrahman, Houmansadr, Amir, Durumeric, Zakir, Wustrow, Eric, 2025. Exposing and circumventing SNI-based QUIC censorship of the great firewall of China. In: USENIX Security Symposium. USENIX, Seattle, USA, p. 20, URL https://gfw.report/publications/usenixsecurity25/data/paper/quic-sni.pdf.