

CERIAS Tech Report 2023-2
Modeling and Characterization of Internet Censorship Technologies
by Alexander Master
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

**MODELING AND CHARACTERIZATION OF
INTERNET CENSORSHIP TECHNOLOGIES**

by

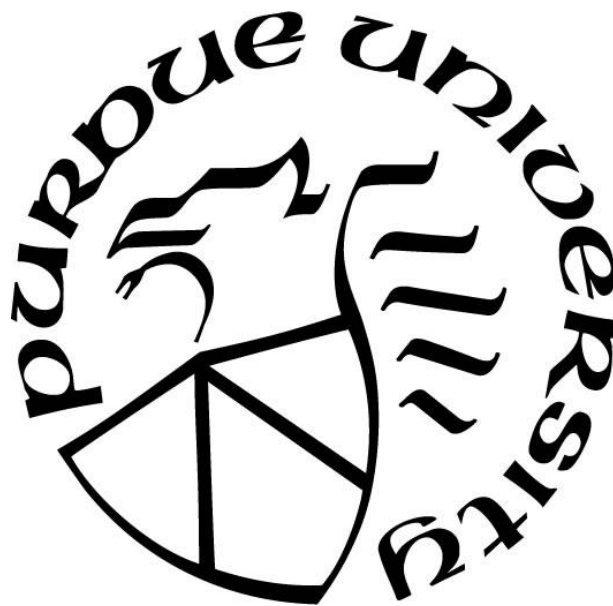
Alexander Master

A Dissertation

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy



Department of Technology

West Lafayette, Indiana

August 2023

**THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL**

Dr. Eugene H. Spafford (Co-Chair)

Department of Computer Science

Dr. J. Eric Dietz (Co-Chair)

Department of Computer and Information Technology

Dr. Christina Garman

Department of Computer Science

Dr. John Springer

Department of Computer and Information Technology

COL Stephen Hamilton, PhD

Director, Army Cyber Institute

Approved by:

Dr. Kathyne Newton

ACKNOWLEDGMENTS

"It takes a village." The studies in this dissertation, and the beginning of my research career would not have been possible without the help, support, and love of many people in my life. First, I would like to thank my family for their love and support over the years — my sisters, in-laws, grandparents, great-grandparents, and cousins — and especially my parents, who always encouraged me to better myself by taking each next leap in higher education. Thank you for always being there for me. Next, I would like to acknowledge the U.S. Army leaders that had a profound effect on shaping the direction of my life and developing me into the leader I am today — people like Nadine Nally, Micah Bushouse, Sarah Crane, William Toft, Jerry Hubbard, Paul Stanton, Mark Klink, and Stephen Hart, among others. Thank you all for the lessons learned, the example you set of what "right looks like," and the "war stories" (literal and metaphorical) we have shared.

The transition from active-duty military to academia was certainly a culture change, and I want to express my deep appreciation to my committee for enabling my success. Professor Spafford (Spaf), thank you for making me aware of the interdisciplinary program at my alma mater and for the many lessons that guided me to become an effective researcher (correct use of the scientific method, "standing on the shoulders of giants," research ethics, not taking oneself too seriously, among many others). Professor Eric Dietz, you and Julie immediately welcomed my family into your home and the local community upon our arrival. Thank you for your mentorship and friendship. The work you and Dave Hankins have done through the Purdue Military Research Institute (PMRI) has made Purdue a top-tier location for defense-related research and directly enabled my success. Professor Christina Garman, thank you for encouraging me to publish my work in competitive peer-reviewed venues, despite my short timeline and occasional lack of self-confidence. You have helped me grow as a scholar, and your seminars in applied cryptography were immensely helpful in meeting my educational goals. Professor John Springer, thank you for always being available as a calm voice of reason. Your insightful questions and observations improved my research project's quantitative aspects, and I appreciate you always being available to talk through a problem set. COL Stephen Hamilton, thank you for supporting my research with funding through the Army Cyber Institute, and for taking a personal interest in

my work by serving on my committee. Without the Army's financial support of tuition, fees, and travel stipends, this research would not have been possible.

I am grateful to the Purdue Center for Education and Research in Information Assurance and Security (CERIAS) staff, the administrative folks at the Computer and Information Technology department, and the researchers at the Purdue Homeland Security Institute (PHSI). Rather than being an interdisciplinary student with no "home," you provided me with many. To my labmates — Nicholas Harrell, George Hamilton, Krassimir Tzvetanov, Manuel Mar Valencia, and Travis Cline — thank you for always being there to bounce ideas off of, air frustrations, or provide much needed distractions from work. I also owe a debt of gratitude to COL(R) Jim Lerums; you imparted your wisdom and unique perspective at many key points along my doctoral journey. Thank you for helping me navigate and positively manipulate university bureaucracy, while also preparing me to become the "Iron Major" my future organizations will need.

Most importantly, I want to thank my wife Stephanie for her tireless support. You put up with all of my shenanigans, and I love you deeply for it. The Army put us through a lot, between constantly moving across the country, deployment, temporary assignments overseas, and lots of late nights, and you were with me through all of it. I appreciate how you helped me structure my time to keep my dissertation studies on track, even if your primary motivation might have been to ensure we had time to play the newest Legend of Zelda release. I'm sorry that you had to be my editor; your thoughtful input immensely improved this manuscript, and my future readers have you to thank.

TABLE OF CONTENTS

TABLE OF CONTENTS.....	5
LIST OF FIGURES	8
LIST OF TABLES.....	9
ABSTRACT.....	10
CHAPTER 1: INTRODUCTION.....	11
1.1 Background and Motivation	11
1.1.1 Historical Context of Censorship.....	11
1.1.2 Internet Censorship.....	15
1.1.3 Internet Surveillance.....	19
1.1.4 Attribution.....	22
1.2 Problem Statement and Research Questions.....	26
1.3 Dissertation Organization	26
1.4 Methods.....	28
1.5 Delineations	28
1.6 Constraints and Disclosures.....	30
CHAPTER 2: RELATED WORK.....	31
2.1 Internet Censorship Studies	31
2.2 Censorship Circumvention.....	33
2.2.1 Research Publications.....	33
2.2.2 Deployed Anti-Censorship Tools	38
2.2.2.1 Access-focused Approaches.....	39
2.2.2.2 Privacy-focused Approaches.....	41
2.2.2.3 Incidental Approaches.....	42
2.3 Nation-state Censorship Overview	44
CHAPTER 3: A REFERENCE MODEL FOR INTERNET CENSORSHIP TECHNOLOGIES.....	50
3.1 Background.....	50
3.2 System Modeling	51
3.2.1 Validity	52
3.3 Reference Model.....	53

3.4 Reference Model Components.....	56
3.4.1 Censor Assessment.....	57
3.4.2 Decision Enforcement	59
3.4.3 Data Processing	60
3.5 Example Applications of Reference Model.....	62
3.6 Summary	66
CHAPTER 4: A SURVEY OF INTERNET CENSORSHIP METHODS.....	67
4.1 Background.....	67
4.2 Research Goals.....	68
4.3 Systematization Methodology	69
4.4 Internet Censorship Methods.....	72
4.4.1 HTTP/URL Filtering	72
4.4.2 DNS Detection, Manipulation, and Denial.....	76
4.4.3 IP Address and Port Matching.....	81
4.4.4 Deep Packet Inspection and Protocol Fingerprinting.....	83
4.4.5 BGP Attacks and Disruption	88
4.4.6 Bandwidth Throttling.....	90
4.4.7 Internet Shutdowns	92
4.4.8 Computer Network Attacks and Resource Exhaustion	95
4.4.9 Additional Censorship Considerations	100
4.5 A Taxonomy of Internet Censorship Methods.....	104
4.6 Summary	110
CHAPTER 5: A WORLDWIDE VIEW OF NATION-STATE INTERNET CENSORSHIP ..	111
5.1 Background.....	111
5.1.1 Overview.....	111
5.1.2 Introduction.....	111
5.1.3 Nation-state Internet Censorship	113
5.1.4 Summary of Censor Methods	114
5.2 Methodology	115
5.2.1 Data Sources	115
5.2.2 Methods	116

5.2.3 Limitations and Delineations	117
5.3 Results and Analysis	118
5.3.1 The Framework	118
5.3.2 Analysis and Trends	120
5.3.3 Discussion	126
5.4 Summary	128
CHAPTER 6: DISCUSSION AND FUTURE DIRECTIONS	129
6.1 Summary of Contributions	129
6.2 Future Work	130
APPENDIX: DATASETS	133
Open Observatory of Network Interference Data	133
Censored Planet Data	133
Access Now Data	133
Freedom on the Net Data	133
Internet Society Pulse Data	133
REFERENCES	145
VITA	190

LIST OF FIGURES

Figure 1. Ukrainian Tor connections after the 2022 Russian invasion.....	18
Figure 2. Overall research procedures	27
Figure 3. Levels of protection for a message [180]	36
Figure 4. Weaknesses of major types of circumvention systems [310].....	36
Figure 5. Evidence of censorship by nation-states, as of 2006 [105]	46
Figure 6. Blocking techniques by nation-states, as of 2006 [105].....	47
Figure 7. Censored Planet Satellite visualization (August 10, 2020)	48
Figure 8. <i>Freedom on the Net 2021</i> global overview map [396].....	49
Figure 9. Methodology for construction of an empirically grounded reference model [139]	52
Figure 10. Abridged version of the reference model for Internet censorship technologies.....	54
Figure 11. Reference model for Internet censorship technologies	56
Figure 12. Censor Boundary depicted	57
Figure 13. Example use of reference model assessing Tor Browser	63
Figure 14. Example use of reference model assessing GoodbyeDPI	65
Figure 15. A systematic guide to literature review development [325].....	70
Figure 16. Example plaintext SNI for cloudflare-dns.com.....	75
Figure 17. Transparent DNS proxy illustrated [513].....	78
Figure 18. Example blockpage from the Republic of Korea	79
Figure 19. DPI Diagram from Bendrath and Mueller [41]	84
Figure 20. A general scheme of network security protocols [449].....	87
Figure 21. Example law enforcement domain seizure [444] (Retrieved October 2, 2022)	101
Figure 22. Website blocking a user with a European IP address after GDPR enacted [426].....	104
Figure 23. Framework for evidence of Internet censorship methods by country	121
Figure 24. Nation-state censor methods summary.....	123

LIST OF TABLES

Table 1. Examples of attacks utilizing traffic metadata.....	21
Table 2. Internet Censorship Methods Taxonomy.....	106
Table 3. Citations of evidence of Internet censorship methods (by decade)	109
Table 4. Percentage of countries that use each Internet censorship method in the framework ..	122
Table 5. Citations for evidence of Internet censorship methods by country	125

ABSTRACT

The proliferation of Internet access has enabled the rapid and widespread exchange of information globally. The world wide web has become the primary communications platform for many people and has surpassed other traditional media outlets in terms of reach and influence. However, many nation-states impose various levels of censorship on their citizens' Internet communications. There is little consensus about what constitutes “objectionable” online content deserving of censorship. Some people consider the censor activities occurring in many nations to be violations of international human rights (e.g., the rights to freedom of expression and assembly). This multi-study dissertation explores Internet censorship methods and systems. By using combinations of quantitative, qualitative, and systematic literature review methods, this thesis provides an interdisciplinary view of the domain of Internet censorship. The author presents a reference model for Internet censorship technologies: an abstraction to facilitate a conceptual understanding of the ways in which Internet censorship occurs from a system design perspective. The author then characterizes the technical threats to Internet communications, producing a comprehensive taxonomy of Internet censorship methods as a result. Finally, this work provides a novel research framework for revealing how nation-state censors operate based on a globally representative sample. Of the 70 nations analyzed, 62 used at least one Internet censorship method against their citizens. The results reveal worldwide trends in Internet censorship based on historical evidence and Internet measurement data.

Keywords: computer networks, filtering, Internet censorship, managed attribution, modeling, nation-state censorship

CHAPTER 1: INTRODUCTION

1.1 Background and Motivation

1.1.1 Historical Context of Censorship

Censorship is an increasingly important topic of public debate worldwide. The interpretation and implementation of censorship influence abstract ideals such as freedom of expression, advancement of human knowledge, and national security. Differences in how individuals, societies, cultures, and legal frameworks view censorship reflect the underlying values of the people involved.

Meriam Webster defines a censor as “a person who supervises conduct and morals, such as: an official who examines materials (such as publications or films) for objectionable matter, or an official who reads communications (such as letters) and deletes material considered sensitive or harmful.” The second Webster entry is more applicable to the modern era: “to examine in order to suppress or delete anything considered objectionable” [295]. Britannica attributed the first historical use of the term censorship to 443 BCE when Rome established the office of the censor. The office was responsible for conducting the census and regulating citizens’ morals [21]. In the ancient world, citizens concealed the expression of certain beliefs (e.g., agnosticism) because it risked social ostracization and criminal charges. Self-censorship, when an individual holds back opinions or beliefs, also continues to occur today. The impact of censorship on society in modernity has profoundly shifted, alongside opinions about what constitutes a legitimate concern of government.

The rise of liberalism in the modern world prompted new ideas about the flow of information. The Oxford English Dictionary (OED) defines liberalism as “a political and social philosophy that promotes individual rights, civil liberties, democracy, and free enterprise” [339]. Near the turn of the seventeenth century, liberal philosophy helped inspire revolutions and movements to establish new governance systems as nation-states. These events were a shift away from traditional monarchies and feudal systems. Much of the modern “Western world,” including North America, western Europe, Australia, and South America, consist of governments founded

on liberal ideology. While classical liberals and modern liberals disagree on the size and scope of government [31], they generally maintain similar principles related to liberty (freedom), rights of the individual, consent of the governed, and equality before the law [292]. Individual rights tend to include political freedom, freedom of speech, freedom of religion, and private property — although implementation or codification of rights differs among nations. In a liberal society, an individual may do whatever is not forbidden by law. Habermas, one of the twentieth century's leading European social philosophers, argued that truth is the consensual outcome of reasoned debate, and that unconstrained communications in the “public sphere” are necessary to reach truth statements [464]. In that view, ideal decision-making in a liberal society involves all known facts of an issue being brought to bear to ensure a decision is well-informed.

Liberal societies often prioritize individuality, such as the right to freedom of expression. Allowing each individual to speak their opinion, vote in fair elections, and publicly debate ideas is central to self-governance. Censorship performed by governmental entities could stifle the building blocks of the state; however, it may be tolerated in circumstances when failing to do so would infringe upon the rights of another individual. The United States has its Bill of Rights (the first ten amendments to its Constitution), in which the first enumerated right is: “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances” [511]. Not all liberal nations have codified these ideals into law, however. Citizens in the United Kingdom have a negative right to freedom of expression under the common law [251]. The constitution of South Korea guarantees freedom of speech, press, petition, and assembly for its nationals; however, its national security law allows for criminal prosecution of individuals who publicly support communism or the regime of North Korea. This tension between liberty and security has played out in other liberal nations worldwide.

In contrast, many nations do not share liberal values. Illiberal societies often reject the democratic values of Western countries for many different reasons. Some authoritarian regimes organically formed as monarchies fell. The OED defines authoritarianism as "favorable to or characterized by obedience to authority as opposed to personal liberty; strict, dictatorial" [340].

Some nations formed under a theocracy, such as the Islamic Republics of Iran, Pakistan, and Mauritania — where (to varying extents) religious ideology forms the basis for governance. Other countries have deep-rooted cultural or social elements that shape their worldview differently than that of liberal societies. Some Asian cultures value the community over the individual [363]. Collectivist cultures make decisions considering the good of the whole rather than the protection of individual civil liberties.

Illiberal nation-states have shown that they view censorship differently than Western countries. Rather than allowing the free flow of all information with select exceptions, illiberal countries often view information as a tool of governance. In authoritarian regimes, leaders use censorship to exert control over the information environment to maintain their power and status [432]. In theocracies, government officials use religious law and ideology to guide their decision-making. For them, censorship is a way to protect citizens from ideas or images deemed offensive or detrimental to their faith. Collectivist cultures use censorship and surveillance to control ideas and prevent crime. The PRC's Communist Party of China (CCP) outlined “social harmony” as one of its strategic national policy goals [91].

International organizations promote freedom of expression as a human right and therefore oppose censorship. The United Nations (UN) included an open-ended definition of freedom of expression in its Universal Declaration of Human Rights in 1948. As an intergovernmental organization with nearly all nation-states on Earth as members [440], the UN is uniquely situated as a source of information and policy on a global scale. Article 19 of the UN declaration announced that freedom of expression is a universal human 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." [438]. This universal definition is helpful in unifying research goals on a global scale. While the UN's effectiveness as an international organization has been called into question [36], this support for free expression gives citizens in countries that desire more freedoms a standard to reference as universally applicable. Critics of the UN documents point out that the founding members of the UN after World War II were liberal nations that did not share the values of every country globally [242].

Nation-states across ideologic spectrums and value systems deny access to certain information through legal or technical means. The German penal code prohibits the dissemination of Nazi propaganda and public denial of the Holocaust, both in-person and online [134]. The German government also compels social media companies to moderate and delete hate speech and threats of violence from their platforms, with deadlines as short as 24 hours and financial fines for non-compliance [266]. Over the years, countries in Africa have banned dozens of books containing sexual content, homosexual relationships, racism, and criticism of government actions [154]. Several countries (e.g., Italy, France, Estonia, Iceland) use domain name system (DNS) tampering to block online content considered illegal (e.g., intellectual property theft, gambling, pornography, terrorism, child sexual abuse materials) in their society (see Chapter 5).

There are debates about disinformation and misinformation and whether such content should be permitted on online platforms. There is no consensus within a country's borders, let alone the international community, on whether policing online spaces belongs to governments or the entities that host news and social media platforms. Contention about who in government decides what content is objectionable is vigorously debated, and consensus is rarely reached.

Even some liberal nations have demonstrated a willingness to censor their citizens. In recent years, hundreds of Internet shutdowns coincided with elections and other politically charged events in India — a federal republic with a democratically elected parliament. The Republic of Turkey arrested dozens of journalists and shut down media outlets following an attempted coup in July 2016 [422]. South Korea, a democratic republic, routinely censors print, television, and online content. The country bans pornography, has strong defamation laws with severe criminal penalties, and filters political content critical of elected officials [106,148,172].

In contrast to controversial censorship decisions, there are rare cases in which there is a broad consensus that censorship is appropriate. Globally, countries outlaw child sexual abuse material (CSAM, often referred to as child pornography). Few societies view these materials as allowable or protected, including illiberal nations that do not subscribe to Western values. Very few topics are as straightforward as CSAM — and even then, systems that attempt to detect illicit content in modern communication systems have been scrutinized for violations of user privacy expectations

[470]. In addition to CSAM, the United States actively shuts down web services that violate intellectual property law. Few arguments challenge these shutdowns, aside from the potential for government overreach or in cases where "fair use doctrine" may apply [181]. Censors in many nations target hate speech and violent rhetoric; these topics do not often find sympathy but are sometimes used as a "slippery slope" argument by free speech advocates. There is potential for political targeting of individuals if broad categories of content can be banned and rules are not clearly defined.

Additionally, there are instances of censorship across different societies that are commonplace and protected by law. Militaries exert control over intelligence and information they possess in the name of national security interests. By denying citizens access to military information, a country may prevent the success of other nation-states' espionage activities. It may also limit public transparency and prevent government scandals or inefficiencies from surfacing.

In all, defining what is "objectionable" and deserving of censorship depends on the context, the entities involved, and the dynamic underlying values of the people concerned.

1.1.2 Internet Censorship

The proliferation of Internet access has enabled the rapid and widespread exchange of information around the world. 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." [112]. However, many nation-states impose censorship on their country's Internet communications. As the world wide web rose in prominence, governments of nation-states around the globe began to realize the power and influence of the "information superhighway." Private sector organizations might also implement censorship measures on their Internet users [293] or be compelled by their governments to do so [184].

Internet censorship is a relatively new phenomenon in the human experience. 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. Initial Internet-like capabilities, such as the Advanced Research Projects Agency Network (ARPANET), were only available to

governmental entities and researchers at select institutions. Upon the advent of the world wide web in the early-1990s, along with decreasing costs of computing devices and software, Internet technologies became available to average citizens in some nations around the globe. The proliferation of Internet-connected devices continues to accelerate today, allowing more people to communicate worldwide in near real-time over various mediums and protocols. As stated by Warf, the Internet shifts the production of meaning from the few to the many, and "unfettered electronic communication allows truth to be uncoupled from power" [464].

Aceto and Pescapé defined Internet censorship as "the intentional impairing or blocking of access to online resources and services," regardless of the intent, scope, or legitimacy of the actions [6]. The technical means by which Internet censors implement censorship vary widely but are generally constrained by standardized protocols that allow the Internet to function as a network of networks. Some Internet censors block web pages with "objectionable" content and inform users that their request was denied. Others simply drop the connection or manipulate the traffic so the connection appears to fail. Others will degrade the connectivity of a user when undesirable activity is detected, rendering the communication unusable. Applications that allow for unmonitored communications will often be blocklisted, denied based on ports used by the application's software or signatures of its data packets. In addition to blocking communication, Internet surveillance is closely tied to censorship activities. Detection of objectionable content (or anti-censorship tunnels) is generally the first and most important step toward implementing a blocking action. More aggressive nation-state censors will also completely disconnect Internet connectivity during perceived critical events, such as elections or periods of civil unrest.

Countless examples of Internet censorship have occurred over the last three decades. Social movements, such as the "Arab Spring" in the early 2010s, were accelerated by the use of technology to organize protests and garner support and became a target for censorship. Authoritarian leaders have demonstrated a willingness to selectively censor information they deem dangerous to maintaining power, sometimes disconnecting Internet connectivity completely during tumultuous periods [188] (see §4.4.7 for further discussion).

Many studies have observed how the now famous "great firewall of China" (GFW) has been employed to enable domestic censorship and surveillance in the People's Republic of China (PRC) and is considered by many to be the most sophisticated and aggressive state censor [337,203,253,467,56,316,505,50,374,14,450,269,252,128,127,250,249,35,486,335,105,268,87,212,279,508]. 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" [98]. In July 2021, Cubans took to the streets to protest the government's handling of the COVID-19 pandemic response. During the demonstrations, government officials restricted access to Facebook and WhatsApp. Many Cuban users turned to the US-based anti-censorship tool Psiphon for open communications access [103].

In February 2022, metrics of total Tor network usage showed an over 300% increase in connections originating from Ukraine immediately following Russia's invasion of the country [427]; usage rapidly fell after February 24th, possibly because of Russian forces destroying cellular tower infrastructure or overall displacement of civilians (see Figure 1). Ukrainians continued to rely on virtual private networks (VPNs) and anti-censorship technologies throughout the conflict, as the Russian Federation diverted Internet traffic from parts of Ukraine through Russian service providers [384] to censor information sources and conduct surveillance operations. Domestically, Roskomnadzor — the federal executive agency responsible for monitoring, controlling, and censoring Russian mass media — ordered the blocking of popular apps such as Telegram and the filtering of traffic from media sources such as the British Broadcasting Company (BBC), Deutsche Welle, Radio Free Europe/Radio Liberty, and Voice of America, among other news sites [367].

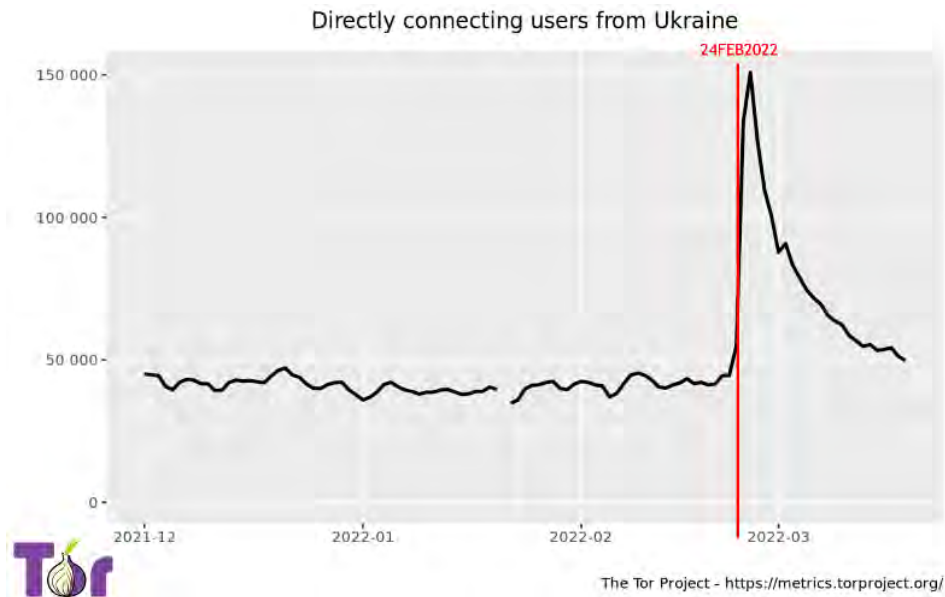


Figure 1. Ukrainian Tor connections after the 2022 Russian invasion

Censorship is a broad issue encompassing numerous aspects of modern societies. Some censorship is mandated by law in particular countries for various reasons, ranging from morality to political manipulation and control of the information environment. This work does not seek to make value judgments on the reasons for Internet-based censorship nor encourage the violation of laws. Instead, this study recognizes the paradigm that international expectations and norms are being violated in some places around the globe. In Article 19 of the universal declaration of human rights, the United Nations 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" [438]. 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.

Given concerns about open access to Internet information, software developers have created tools designed to circumvent censorship in places where it exists. These groups are primarily (but not exclusively) located in North America and western Europe, often in nations that encounter minimal censorship. Anti-censorship tools generally allow individuals to access content and information that would otherwise be unavailable to them. These tools often provide a

capability to protect the identity of journalists, whistleblowers, political dissidents, activists, censored citizens, and others as they attempt to use Internet-based communication mechanisms. Some providers repurpose existing protocols to enable censorship circumvention and provide privacy protections to users, while other software developers create tools specifically to bypass censor restrictions. Many approaches have been undertaken, which are discussed in detail in Chapter 2.

For focus and clarity of study, this dissertation will primarily concern itself with censorship that occurs within the technical elements of Internet communications. Example protocols that allow Internet functionality include Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), QUIC¹, and Border Gateway Protocol (BGP). Historical censor examples will be illustrated with the technology in use at the time of the incident, while the modeling presented in this study will demonstrate abstract functionality for the purposes of generalization.

1.1.3 Internet Surveillance

Surveillance has often been viewed as a controversial phenomenon among different societies. To surveil is to watch, listen, or record an individual's activities [407]. Technology has allowed for new methods of tracking individuals. Businesses and residential homes use cameras to deter crime; Law Enforcement (LE) officials track identification numbers of people crossing international borders to prevent terrorism; during the COVID-19 coronavirus pandemic, countries and institutions used surveillance testing strategies to track and contain the spread of disease [290,230]. System administrators monitor computer network traffic and logs for signs of intrusion on their systems.

When conducted with malicious intent, surveillance becomes a privacy problem. Before the age of electronic communications, surveillance only included visually observing or listening to someone and was somewhat limited in scope. New technologic innovations have brought further opportunities to enter people's personal space. Telephones brought about the idea of listening in on someone's conversation from afar and the concept of wiretapping. The introduction of audio

¹ According to RFC 9000 [271], QUIC is the name of the transport protocol, and is not an acronym.

recording devices allowed for exchanges to be captured and shared with others outside of the initial context of the conversation. Computer-based communications have brought forward entirely new categories of storable data about people. Log files can show the activity performed on a computer, email metadata can show who a person corresponds with, and online advertisers use cookies to track browsing habits and cater personalized ads without a user necessarily understanding the data collected about them. Smartphone users are often unaware of the amount of telemetry and usage data technology that corporations collect from their devices at any given time [262].

As with censorship, the proliferation of Internet communications has significantly increased the ability to conduct surveillance activities on individuals and groups. Internet surveillance is the act of monitoring Internet-based communications. Data packets may be viewed in real-time or stored and analyzed after the communication occurs. Internet surveillance is closely related to Internet censorship because they are frequently interdependent. Surveillance monitoring is often a prerequisite to identifying objectionable user behavior and developing signatures to stop communication. Monitoring techniques have been used to identify offending users and punish them instead of denying their communications.

From an anti-censorship perspective, "surveillance is extremely difficult to detect technically if it has been properly implemented. However, the results of surveillance (arrests or warnings) are often made visible in order to deter future infringement of the rules" [105]. Circumvention methods bring about normative challenges for societies. As Spafford and Antón observed, "for anonymous participation to succeed in those cases where it is most needed, such as under threat of financial or political retribution, the anonymity needs to be so strongly protected as to be effectively inviolable. However, because we cannot know a priori whether such communication is lawful or harmful, there is a basic conflict — do we support mechanisms that allow for true anonymity to anyone seeking it, or do we force all participants to have some form of (eventually) verifiable identity?" [410]. Anonymity is discussed in further detail in §1.1.4. Creating tools that circumvent technical controls may enable free and open communication among some participants; criminals may also use them to cause harm.

Traffic analysis is one of the central elements involved in the conduct of digital surveillance on modern communication mediums. Traffic analysis refers to a category of methods for deducing information from patterns in communication without necessarily knowing its contents. In the context of computer security and Internet traffic, traffic analysis attacks generally involve metadata of network packets or insights inferred by side-channel information about the packets. Security researchers generally categorize traffic analysis attacks as passive or active. Passive attacks involve collection, aggregation, and analysis of traffic without the interference of the communication in real-time. Active attacks include creating, altering, or deleting packets to observe changes and link flows. Attacks vary dramatically in sophistication, from network flow data confirming "who talks to whom," timing and frequency statistical analyses, or active manipulation of live network traffic.

Table 1. Examples of attacks utilizing traffic metadata

Traffic confirmation attack	[197,305,376]
Timing attack	[137]
Frequency attack	[298,412]
Man-in-the-middle attack	[66,237]
Website Fingerprinting	[63]
Browser Fingerprinting	[121,259]
Protocol Fingerprinting	[111]

Internet privacy became a concern even in the early days of the world wide web. Web servers served mostly unencrypted HTTP data, easily observed by an ISP or passive observer on a network. Even with SSL encryption, administrators' server logs easily identified unique users. IP addresses, authentication data, and sizes of file transfers all served to fingerprint connections [200].

In the years following the Snowden leaks of 2013, discussions of mass Internet surveillance capabilities by Western nation intelligence agencies sparked public interest and dialog [170]. In 2014 at a now-famous Johns Hopkins University debate, when pressed about bulk surveillance programs, retired General Michael Hayden (former NSA Director) admitted that the U.S. Government uses metadata to target and kill individuals with drone strikes in some

circumstances [227]. Mr. Hayden assured the audience that U.S. persons were not analyzed in those datasets unless internal rules, processes, checklists, and FISA warrants were acquired. These assurances offer little comfort to the rest of the international community, whose data may or may not be aggregated into the intelligence systems discussed by the panel and are not subject to U.S. civil liberty protections. The implied confidence in the intelligence based on metadata to enable a kinetic strike on a terrorist or enemy combatant likely gives pause to someone concerned about revealing their identity through their Internet communications. Moreover, the existence of such a bulk surveillance program (or intelligence-sharing agreements between nations) lends credibility to the possibility of a passive global adversary, often described in theoretical threat models in academic literature but often assumed to be impractical. In a separate interview in 2017, Mr. Hayden said that "Anything that is worth anything now is being encrypted" [341] and that signals intelligence (SIGINT) organizations must adapt to deriving usable information from data that is encrypted by default.

1.1.4 Attribution

Managing Attribution

Attribution is an important component of any discussion involving communication. Attribution is defined as "the ascribing of a work... to a particular author" [296]. On the Internet, the answer to "who does what" is often found in Internet communications metadata. Attribution can take the form of IP addresses, ports, domain names, Autonomous Systems (ASes), social media personas, organizations, governments, or even the individual identities of Internet users. Attribution provides context to the communication. In the case of using anti-censorship software, appropriately managing or manipulating attribution values can be a critical aspect of avoiding consequences from censors. The use of web proxies in obfuscating the origin of Internet traffic is an obvious example.

One example of the institutional use of managed attribution is found in the United States military. The U.S. Army's field manual (FM) 3-12 *Cyberspace and Electronic Warfare Operations* 2017 edition references "non-attributed" networks as elements of cyberspace operations [443] (references were removed in newer editions of the publication). Little is known about the specifics of many of these operations by the general public. The intelligence "sources and

methods" used to drive these missions are often classified as Secret or Top Secret. Given the sensitive nature of geopolitical competition below the threshold of armed conflict, it is apparent why managing the attribution of cyber operations and espionage activities would be desirable.

Other examples of managed attribution can be found in the commercial sector. Companies use penetration testing to simulate adversary activity and find vulnerabilities or unauthorized access vectors in their network. Penetration testers often use a combination of proxies, VPNs, anti-censorship tools, or cloud infrastructure to emulate an attack from a network perspective during an authorized engagement. These techniques allow them to bypass naive intrusion detection/prevention systems (IDS/IPS) that block malicious activity based on IP address source, as attackers can easily rotate their traffic sources. Different companies (e.g., data brokers) may desire to scrape Internet sites for information. These firms use managed attribution tactics for automated collection, so their behavior is unhindered when a website blocks their traffic.

It must be acknowledged that criminals and malicious cyber actors can use managed attribution techniques in the pursuit of their goals. The balance between providing privacy and free access to information for censored users will always be at odds with potentially providing tools to those who would abuse them.

Anonymity

"Anonymity is the state of being not identifiable within a set of subjects, the anonymity set" [350]. In the context of Internet privacy, full anonymity is a difficult (and often impractical) threshold to meet. Users hoping to achieve relative anonymity must be diligent in the disclosure of their information, given the unsecure design of some of the fundamental protocols of the Internet. Computer data can be uniquely attributed to particular users or devices in many ways. Users must also be cognizant of how computing systems truly function to avoid accidental exposure. Technology that enables anonymous communication is only one of the considerations a user must consider. Poor operational security (OPSEC) practices may defeat the purpose of the person's efforts to disassociate their activity from their identity: for example, logging into a service that knows a person's true identity over an anonymized communication channel.

From a legal perspective, there is a wide variety of judicial precedents and lawful protection (or prohibition) of anonymous communications. Further complexities involve the interpretation of what anonymity enables. Kosseff argued that the United States primarily interprets anonymity in terms of free speech and expression, while European laws typically view anonymity in terms of an individual right to privacy [255]. In 2014 the Supreme Court of Canada struck down the warrantless procurement of anonymous user online identifiers (such as IP address), acknowledging a place for anonymity in section 8 of the Canadian Charter of Rights and Freedoms [213]. In 2012 the Constitutional Court of the Republic of Korea struck down laws that required users of certain web pages to register with their state-issued identification, promoting anonymous expression [79]. The United Nations published reports promoting anonymity as beneficial in some circumstances, such as "the important role it plays in safeguarding and advancing privacy, free expression, political accountability, public participation, and debate" [241]. In the "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," the UN outlined the following recommendations for nation-state policy: "States should revise or establish, as appropriate, national laws and regulations to promote and protect the rights to privacy and freedom of opinion and expression. With respect to encryption and anonymity, States should adopt policies of nonrestriction or comprehensive protection, only adopt restrictions on a case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective, require court orders for any specific limitation, and promote security and privacy online through public education." [241].

However, many nation-states do oppose the use of anonymity by their citizens. Brazil prohibited anonymous speech outright in its constitution "in the context of freedom of expression" [92]. Brazil also required users to register their names when subscribing to cellular telephone service subscriptions. Iran forced citizens to register their IP address to their identity with their ISP [241]. In 2014, the Russian Federation passed a law requiring any blogger with over 3,000 readers to register with Roskomnadzor, the nation's media oversight agency [375].

Given concerns about censorship and surveillance, software developers have developed different approaches to provide varying degrees of anonymity online. Early tools to obscure the source of

web traffic, such as Crowds from 1999, operationalized the axiom "anonymity loves company" [364]. The software relied on a large number of users to participate so that web requests are mixed and performed by other users, ensuring that web servers cannot distinguish unique identifiers of the originating user. Earlier approaches used mixnets to batch and mix packets to provide "untraceable" electronic email [74,222]. The Tor network is the most widely used privacy-enhancing technology today that promotes anonymity as a design goal on a low latency connection (discussed in detail in §2.2.2).

Pseudonymity

Pseudonymity involves distancing actions from a true identity by using a persistent identifier. There is a linking connection between a pseudonym and an identity. An example from United States history would be the publication of the Federalist Papers: a collection of essays published in newspapers in the 1770s under the fictitious name "Publius." Three authors, Alexander Hamilton, James Madison, and John Jay shared the pseudonym. Using a pseudonym allowed the authors to communicate their views of federalism and promote the ratification of the U.S. Constitution among the public while minimizing the fear of reprisal and avoiding *ad hominem* critiques against their ideas. Moreover, pseudonymous anti-federalist essays were published in response under pen names such as "The Federal Farmer," "Brutus," and "Cato." These authors advocated for the addition of a bill of rights to protect individual liberties against the powers of a new federal government or even opposed ratification of the new constitution entirely. They used pseudonyms for the same reason, and to this day, the true author identities of many anti-federalist essays of the time are disputed among historians [503]. When utilizing pseudonymity, caution must be exercised as there is no forward secrecy if the identities are linked. For example, the cryptocurrency Bitcoin uses pseudonymous cryptographic public key addresses as wallets. A wallet has no distinguishing characteristics or metadata linking to a user's identity. However, transactions made on the blockchain are immutable and cannot be changed once they are accepted and appended to the public blockchain ledger [308]. Suppose the true identity of the user of a pseudonym (wallet public key) is revealed by an out-of-band method. Anyone with access to the public blockchain could view every transaction the exposed user has ever made.

1.2 Problem Statement and Research Questions

No model previously existed to characterize Internet censorship technologies. Researchers, policymakers, anti-censorship software developers, and educators will benefit from a research framework to describe censorship and anti-censorship systems.

The research in this dissertation provides insight into the following questions:

R1: What are the technical threats to Internet-based communications? This question is primarily addressed in Chapter 4.

R2: What factors characterize Internet censor activities, in practice? This question is primarily answered in Chapter 5.

1.3 Dissertation Organization

The research in this dissertation followed the steps illustrated in Figure 2.

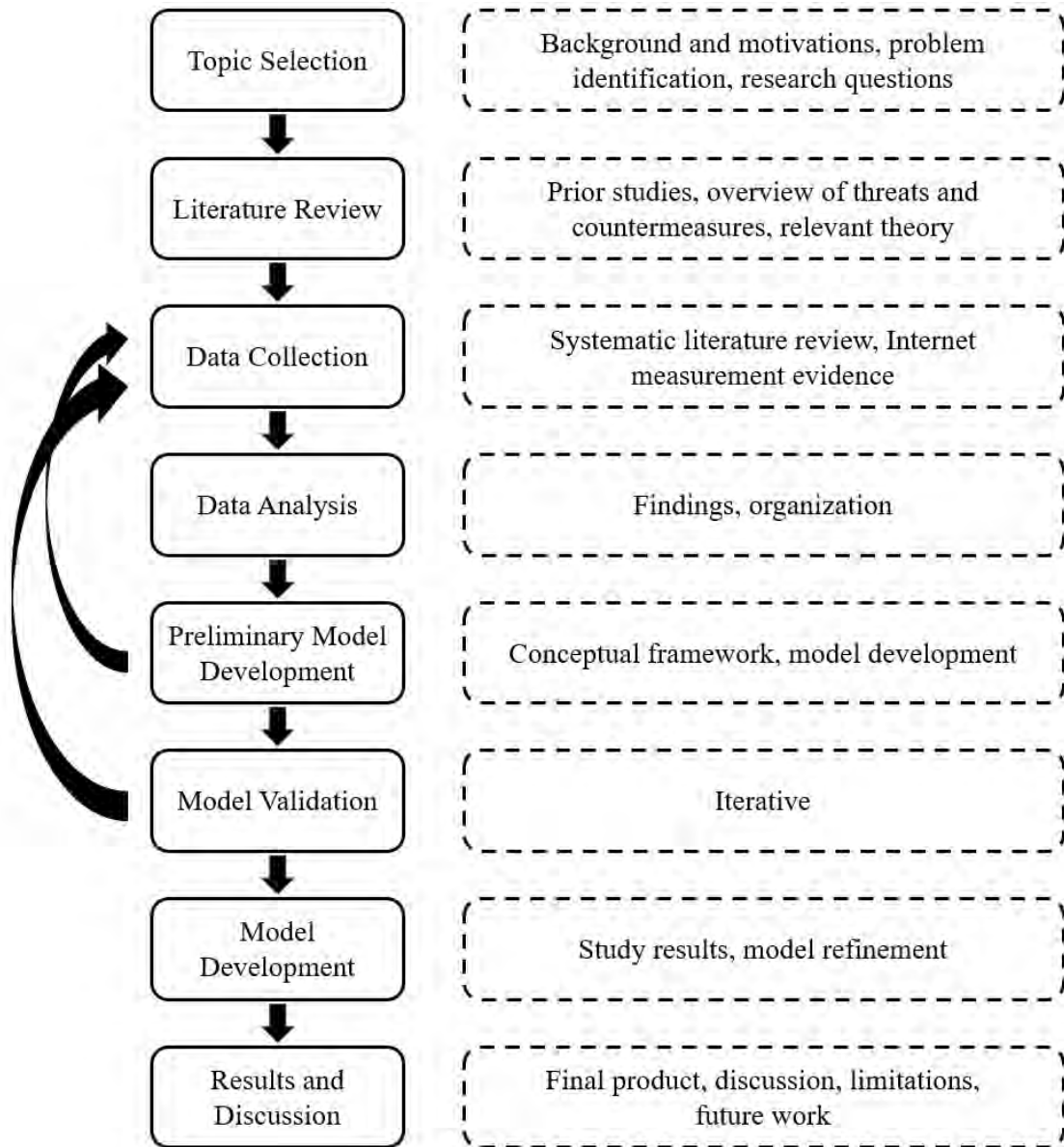


Figure 2. Overall research procedures

As shown in Figure 2, the studies in this dissertation began with topic selection, covered in Chapter 1. Next was a review of relevant literature, covered in Chapter 2. Data collection through model validation was an iterative process involving multiple research methods to formulate and validate the model. Chapter 3 introduces the reference model for Internet censorship technologies. Chapter 4 presents a taxonomy of Internet censorship methods derived from a systematic literature review (SLR). Chapter 5 presents a research framework for

discovering instances of nation-state Internet censorship on a global scale. The author finalized the model based on the results of these supporting studies and discussed the overall contributions and future work in Chapter 6.

1.4 Methods

The individual chapters of this multi-study dissertation utilize different research methods. Chapter 4 uses a systematic literature review (SLR) methodology over a defined timeframe to develop a taxonomy of Internet censorship methods. Chapter 5 uses a mixed methods (quantitative and qualitative) approach to develop a research framework for investigating worldwide occurrences of Internet censorship. The author first performed a cross-sectional study of 70 countries during a one-year period with quantitative measurement data, illuminating current online censorship trends. Second, the author systematically studied prior work to illustrate if and how those same countries performed censorship over the past two decades. The research contributions of Chapter 5 are three-fold: (1) a snapshot of current and emerging Internet censorship methods around the globe, (2) a holistic view of changes in censorship trends over the past two decades as the Internet has become a primary means of human communication, and (3) a novel research framework to allow for ease of continual analysis.

1.5 Delineations

While important to a holistic discussion of online censorship, this dissertation does not address the following topics directly:

- Domain seizures by law enforcement entities
- Outlawed encryption or technologies
- Social media deplatforming
- Content moderation
- Corporate censorship in the workplace

The data collected and used in this study provides evidence of nation-state Internet censorship methods. The data are network focused and provide insight into the transmission and delivery (or

its denial) of messages over Internet networks. Therefore, compelled removal of content and denial of access to private data on segmented networks that do not interact with the broader Internet are not within the scope of this study. Additionally, some countries use legal means to ban particular encryption algorithms or the use of specific technologies, such as VPNs. The framework and model in this dissertation describe how systems operate on networks but do not make value judgments about whether or not an activity or tool ought to be permissible.

Domain seizures affect all Internet users globally, not only those impacted by censors (see Figure 21 for an example). Issues of censorship on social media pages involve the legitimate owner of a web resource moderating or removing content — which cannot be impacted by the communications between the client and server. Discussions of what constitutes free expression and where society defines "public spaces" online are important topics but are not covered in this work. Hidden services such as those found on the Tor network [209], I2P [93], and (proposed) censorship-resistant publishing systems such as Free Haven [108] and Publius [458] are outside the scope of this study. While these approaches are relevant to an overall discussion of online censorship, this dissertation focuses on protocols and applications that are widely used across the Internet. Rather than focusing on niche interest groups or systems that have never been implemented in practice, the author sought to characterize the censor activities and systems that impact millions of people on a daily basis.

Some organizations may use custom, proprietary protocols to exchange information. These protocols are often found in high-security environments, restricted to a local area network (LAN), and potentially “air-gapped” from the public Internet. These implementations are not Internet-routable traffic and are also out of scope. Additionally, while all of the above are relevant to censorship issues at large, a software developer of an anti-censorship tool cannot solve problems outside of their scope of influence. Finally, censorship in the workplace is a different field of inquiry. Employers often filter traffic within their enterprise for security reasons or in the name of productivity. Employees often sign user agreements, notifying them of workplace expectations for what they may access during work hours. These practices vary across legal jurisdictions. Workplace censorship is different from a governmental authority dictating what information may or may not be accessed from personal or public devices.

1.6 Constraints and Disclosures

This study attempts to offer a global view of the issues related to Internet censorship and the anti-censorship software that allows people access to openly available information. While the definition and operationalization of freedom of expression are derived from an international organization (the United Nations), the author acknowledges that this work is influenced by Western philosophy because it originates from the United States. This work is also limited to scholarly sources available in the English language.

Censorship is a broad issue encompassing numerous aspects of modern societies. Some censorship is mandated by law in particular countries for various reasons, ranging from morality to political manipulation and control of the information environment. Even an ardent free speech advocate may encourage censorship of certain information in particular contexts. This work does not seek to make value judgments on the reasons for Internet-based censorship nor encourage violation of laws.

Censorship occurs in printed media, audio recordings, journalistic endeavors, television broadcasts, and many other aspects of daily life. For the purposes of this dissertation, censorship refers specifically to censorship experienced by Internet users online unless specified otherwise. Internet censorship is the impairment or denial of access to information or communication resources available via the Internet and its associated protocols. Further, this study defines anti-censorship software as code or computer programs that allow a user's Internet communications to bypass the denial of access imposed by an Internet censor. This narrow definition excludes important open research problems discussed and delineated in detail in Chapter 2. However, limiting the scope of censorship and anti-censorship enables this study to illuminate and contribute to a particularly salient issue in the body of literature.

Disclaimer:

The facts and analysis presented in this document are attributable exclusively to the author. They do not represent the views of Purdue University nor imply or constitute endorsement by the U.S. Department of Defense.

CHAPTER 2: RELATED WORK

2.1 Internet Censorship Studies

In 2008, Deibert et al. published their seminal report *Access Denied* [105], offering the first global view of Internet censorship. The study data from 2006 covered 40 countries and categorized censor methods into four categories: IP blocking, DNS tampering, Blockpage, and Keyword. The authors concluded that nation-states that practiced state-mandated filtering were predominately clustered into three regions: east Asia, the Middle East/North Africa, and central Asia. Internet routing has increasingly grown in complexity since Deibert et al.'s report, and the geopolitical landscapes within which censorship regimes exist have also changed. Some censors use more sophisticated, targeted, and subtle methods, while others use blunt tactics such as Internet shutdowns to achieve their goals. Researchers have also documented online censorship in self-proclaimed liberal democracies, which espouse freedom of speech and expression as values; these nations were not covered in the *Access Denied* reporting. Deibert et al. had to perform all their measurements using their infrastructure, vantage points, and OpenNet's methodology. They did not have access to the Internet measurement datasets available today (see §5.2.1). This work's author draws inspiration from their approach and provides a broader view of Internet censorship with deeper technical detail. In Chapter 5, the author surveys a globally representative list of countries, using diverse datasets for overlapping coverage, and utilizes the latest research in censor methods (as described in Chapter 4).

Aceto and Pescapé wrote a survey of censorship detection systems in 2015 [6]. Their work covered academic detection architectures as well as deployed Internet measurement platforms. The study relied on the design goals of the detection system's authors for their characterizations, while Chapter 4 of this dissertation focuses on the evidence of censorship occurrences. Gill et al. performed a study similar to Chapter 5 in 2015 but only used OpenNet Initiative data [179] and focused on DNS and HTTP filtering of web URLs.

Khattak et al. conducted a systematization of knowledge 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 comprehensively surveyed 73 such systems and offered an abstract censor attack model [245]. Khattak et al. focused on the goals of CRS designers, not necessarily on censor abilities directly.

Tschantz et al. did a study related to Chapter 5 of this dissertation in 2016 [433] as part of a larger systematization of knowledge (SoK) to survey the evaluation criteria of CRSs. They compare the evaluation criteria elements from the literature to observed "real-world" censor behavior derived from field reports and bug tickets, revealing frequent incongruencies. Their goals were to enumerate evaluation criteria and identify trends rather than systematization of the censor behavior, as accomplished in Chapter 4 of this dissertation. In section 4 of their study, Tschantz et al. outline "censorship as practiced," in which they examined 31 measurement studies to attribute censor capabilities to several high-profile censoring nations. Some of the capabilities were technology-specific (e.g., Netsweeper, BlueCoat, SmartFilter), and the countries were not globally representative, as this work's author strove to accomplish in Chapter 5.

Many studies have attempted to provide coverage of Internet censorship through measurement platforms [229,413,316,289,466,447,349,509,232,24], the use of literature surveys [283,193,6,48,464], or crowdsourced data collection [217,143,3]. Measurement platforms have various advantages and limitations. The author drew from several measurement platform datasets to promote overlapping coverage. Surveys provide historical context to the analysis. Prior work also has dozens of individual country censorship case studies, providing historical data on evidence of censor methods.

Internet measurement communities have faced ethical concerns about the data they have collected [96,231]. Institutional Review Boards (IRBs) at universities have been dismissive of measurement researchers because they are not measuring "human subjects" directly, causing controversy for journals to decide if technical research was conducted ethically [62]. For example, an analysis of the "Encore" research submitted to ACM SIGCOMM 2015 determined that the researchers did not break any U.S. laws and that their research did not rise to the standard definition of having human subjects [309]. Still, lingering questions remain about how

to answer research questions that may involve users' data from around the world. In some nations, citizens may incur harm based on the content they access online. The author of this dissertation strove only to use Internet measurement datasets with no ethical research concerns.

2.2 Censorship Circumvention

2.2.1 Research Publications

There are hundreds of studies in the literature related to anti-censorship software. Authors from the censorship and privacy-enhancing technologies communities in academia have proposed dozens of new anti-censorship systems over the past 20 years. A handful of these papers have been successfully implemented to varying degrees [110], but most have not seen real-world use. Many of the tools proposed addressed a specific censorship problem, be it an observed phenomenon [463,510], or a theoretical attack scenario [47,297]. Several taxonomic and characterization papers have been put forward on circumvention [122,123,260,261]. Some attempted to fill gaps in the capability of existing tools or approaches. These papers would have benefited from a generalized framework of threats to Internet communications to guide their design goals and anticipated outcomes. Admittedly, informed abstraction of censorship problems might have been difficult to formulate until real-world censors were observed, documented, and worked around by circumvention approaches over the years.

A 2016 study in Proceedings on Privacy Enhancing Technologies (PoPETS) titled *SoK: Making Sense of Censorship Resistance Systems* [245] resembled the goals of this dissertation. Khattak et al. termed the systems they analyzed "Censorship Resistance Systems" (CRSs), inclusive of deployed software and theoretical systems from academic papers, as well as "access-centric" and "publication-centric" schemes. The paper comprehensively surveyed 73 such systems. The primary differences between [245] and this dissertation are its view of the threats and the focus of its scope. This dissertation strives to model censorship as it happens in real-world networks and does not focus on unimplemented academic designs. Anti-censorship tools in this dissertation's context are low-latency and access-based systems, providing Internet-based services despite censor attempts at blocking. Khattak et al. also focused on the goals of CRS designers, not directly on censor threat actor abilities. When creating software, software

designers have different design goals and threat models. Khattak et al.'s results greatly illuminated the literature surrounding these kinds of systems but would benefit from an adversarial analysis of threats to Internet communications based on measurement data.

Leberknight et al. classified circumvention tools and studied the relationship between a tool's classification and its longevity for use [260,261]. Their papers examined 15 tools and categorized them as HTTP proxy, CGI proxy, rerouting, IP tunneling, and distributed hosting. Their studies provided recommendations for anti-censorship software developers from several qualitative and non-technical standpoints. They set forth the development of quantitative metrics for the technical elements of Internet censor and anti-censorship methods as future work.

Winters categorized the problems faced by censorship circumvention tools (within the context of Tor onion routing) into three sets of problems: bootstrapping, endpoint blocking, and traffic obfuscation [472]. These categories help to frame the external threats during the threat modeling portion of this study. Bootstrapping involves all of the preliminary steps necessary to allow a user to begin using anti-censorship software [221,265]. This step may include accessing the software's source code or binary executables; many censors deny access to popular anti-censorship provider web pages. This preliminary stage may also include setup configurations, such as the software discovering available relay nodes or proxy servers. Once a tool is bootstrapped, the next set of issues involves connecting to available circumvention service infrastructure. This is known as the endpoint blocking problem. An example of endpoint blocking is a VPN connection that would otherwise succeed in circumventing a censor, except that its server endpoint IP address is publicly known and has been placed on a blacklist. Finally, the last challenge faced by anti-censorship tools is that of traffic obfuscation. Increasingly sophisticated censorship methods analyze and create digital signatures for particular kinds of network traffic. If a censor can detect the use of a tool, it can deny real-time traffic from particular tools or protocols. These same DPI or traffic analysis methods may be used for surveillance to identify users attempting to circumvent the censor to punish them. Anti-censorship tool developers may implement traffic obfuscation to randomize the characteristics of their network traffic or design them to mimic other characteristics to blend in with legitimate traffic. Not all anti-censorship tools offer obfuscation features, as not all censors use advanced

detection methods, and not all regimes or organizations seek in-person punishment for censor violations. Regardless, traffic obfuscation remains a desirable property for some anti-censorship software, especially in the presence of an advanced adversary.

Fifield characterized a censor as a traffic classifier coupled with a blocking mechanism [140]. Fifield's study divided detection techniques into two classes: detection by content and detection by address. The former addresses threats such as content filtering and protocol identification, while the latter more closely resembles the traffic analysis problem of "who talks to whom." Detection closely follows the array of surveillance problems discussed in this work, while the technical blocking mechanisms are reflected in the censorship problems. These categories help to frame the censorship-specific problems during threat modeling in this study.

Goldberg summarized the levels of protection necessary for a piece of software to provide depending on the context of the user's goal (see Figure 3) [180]. The first level (level 0) of protection is trivial, requiring no protection, and the message can be freely and publicly transmitted. An example is posting to an HTTP web forum that does not utilize Transport Layer Security (TLS) encryption; the HTTP message is sent over the Internet in plaintext. Level 1 protection demands protection of the content of the message. The most common means of protecting a message's contents on the Internet is to use encryption to scramble the message, rendering it unreadable by a snooping adversary. An example is using a PGP key to encrypt the contents of an email before sending it to a colleague. Note that an eavesdropper can still see the email's original sender and the intended recipient. Level 2 demands protection of the metadata of the message. Privacy-enhancing technologies are recommended for concealing sender (or recipient) information or other metadata concerning the message. An example of this is using a VPN to conceal the source of some particular IP traffic on its way to its destination. Finally, level 3 protection attempts to conceal the existence of a message. Techniques known as steganography can obscure a message and embed it within another innocuous channel that a censor permits. Steganographic methods enable messages to be transmitted undetected and are often the most difficult to implement [274]. In this study, Goldberg's categories help frame the privacy-centric problems during threat modeling.

Level	What to protect	Method
3	Existence of message	Steganography
2	Metadata of message	Privacy-enhancing technologies
1	Content of message	Encryption
0	Nothing	None

Figure 3. Levels of protection for a message [180]

In 2020, Nasr et al. presented a summary of the weaknesses of several circumvention methods, as shown in Figure 4 [310]. Additional Internet censorship countermeasures are discussed in Chapter 4, alongside their corresponding threats.

Category	Easily blocked	Costly	Poor QoS	Deployability
Proxy-Based	●	◐	●	○
Domain Fronting	○	●	○	○
CacheBrowsing	○	○	●	○
Tunneling	○	◐	●	◐
Decoy Routing	○	◐	○	●

Figure 4. Weaknesses of major types of circumvention systems [310]

This dissertation acknowledges two studies outside of peer-reviewed publications that conducted assessments of anti-censorship software from an end-user perspective. They are summarized in the following paragraphs.

In 2010, Freedom House produced a special report with the goal of evaluating censorship circumvention software, titled *Leaping Over the Firewall: A Review of Censorship Circumvention Tools* [65]. The authors of the report conducted two studies involving 11 specific pieces of anti-censorship software: Dynaweb, Freegate, Gtunnel, Gpass, Google Reader/Translation/Cache, Hotspot Shield, JAP, Psiphon, Tor, Ultrasurf, and Your Freedom. The first study performed a technical assessment of each tool in a lab environment using three categories: "ease of use," "performance," and "support and security," with a scoring of 1-5 stars.

The second study consisted of a qualitative survey, organizing questions based on the same categories as the first study with anonymous participants from Azerbaijan, Burma (aka Myanmar), China, and Iran. The audience for the report was primarily users of censorship circumvention tools rather than developers.

Researchers at the Berkman Center for Internet & Society at Harvard University performed another study entitled *2011 Circumvention Tool Evaluation* [372]. The study involved testing 17 circumvention tools in terms of utility, accuracy, and speed. The authors rented virtual private servers (VPSs) from companies in China, South Korea, Vietnam, and UAE to conduct their tests and compared the results against the other considered tools.

There are also web pages that attempt to compare and promote various anti-censorship tools and privacy-enhancing technologies. Some are crowdsourced, offering opinions and recommendations for users. Others are maintained by individuals or groups, such as <https://privacyguides.org>. Another example is a spreadsheet comparing hundreds of VPN services on <https://thatoneprivacysite.net>, published by "ThatOnePrivacyGuy," an online pseudonym. Although publicly available, their methodology had gaps from an empirical assessment standpoint. Many of the evaluation criteria for services were not measurable and relied on claims by the providers (as listed on their web pages) to judge specific aspects. The assessments did not consider a granular view of the specific protocols or technologies in use by particular providers. Service providers can make numerous changes to the implementation of a VPN protocol; this situation results in a never-ending attempt for researchers to characterize providers. Providers may come online and offer new services, go out of business, or constantly change server configurations. "ThatOnePrivacyGuy" also chose to use subjective evaluation criteria, such as "Service Provider gives back to Privacy Causes (Yes/No)" in the assessment of VPN providers, which does not speak to the effectiveness of the software. Additionally, in 2021, <https://thatoneprivacysite.net> began redirecting to <https://www.safetydetectives.com>, a for-profit company whose parent organization owns multiple VPN services and hosts affiliate links to those products. The perception of an evaluation being influenced by commercial profitability reduces trust in the objectivity of the analysis. The studies in this dissertation intend to provide open, objective frameworks that focus on the software as it performs on a network.

2.2.2 Deployed Anti-Censorship Tools

There have been many anti-censorship tools deployed over the last three decades. Some have persisted for years, while others have gone offline or are no longer supported. Journalists, dissidents, and citizens of censoring nations rely on anti-censorship technologies to gain access to information and to protect themselves.

Khattak et al. surveyed 73 "Censorship Resistance Systems" (CRSs) in 2016. The authors defined CRSs broadly to include publication-centric schemes, access-centric schemes, academic papers without implementation, and deployed systems [245]. This dissertation focuses more narrowly on deployed tools that are widely available and are access-centric in nature.

In this dissertation, the author outlines three categories of circumvention approaches within the context of anti-censorship tools: Access-focused, Privacy-focused, and Incidental. Access-focused approaches concentrate their efforts on enabling access to Internet content first and foremost. Example tools are Psiphon and Lantern. Privacy-focused approaches attempt to separate the communicator from the content they access or the communication they transmit. This may involve manipulating metadata, proxying traffic through third parties, or batching transmissions to hide their origins. Multi-party relays (MPRs), such as the Tor network and INVISV Relay, are examples of privacy-focused approaches that often work as censorship circumvention. Incidental approaches are systems that were not designed to circumvent web censorship but functionally are able to do so in the correct environment. Examples of incidental approaches are VPNs and web proxies.

Below is an exploration of deployed tools available at the time of this writing. They appear in no particular order, and the author has no affiliation or relationship with any of the projects discussed. Current systems are helpful for the use case demonstrations of the reference model presented in Chapter 3.

2.2.2.1 Access-focused Approaches

Psiphon

Psiphon is a purpose-built anti-censorship tool designed with security, ease of use, and performance as its primary goals. Psiphon "is a centrally managed, geographically diverse network of 1000s of proxy servers. Most of [the] infrastructure is hosted with cloud providers. Psiphon is a "one hop" architecture with secure link encryption between clients and servers" [355]. The client software uses a combination of a web proxy, secure shell (SSH), and VPN protocols to connect to their infrastructure, then routes user traffic to the broader Internet. Psiphon developers have implemented improvements to bypass deep packet inspection (DPI) threats and have supported pluggable transports to obfuscate "first-mile" connections [141]. However, the developers specifically do not provide privacy protections and prioritize low-latency performance. Psiphon offers downloads for Windows, macOS, Android, and iOS.

Lantern

Lantern is a purpose-built anti-censorship tool without privacy or anonymity features [258]. Lantern uses a series of HTTPS proxies authenticated through a centralized infrastructure to connect users to uncensored web connections. Lantern also implements a "peer-to-peer" option to allow Lantern users to share their connections with others; authentication is still required, however, reducing the benefits of distributed networking. Lantern has commissioned independent, external security audits of its client software and received some fair and poor ratings. Lantern clients are available on Windows, macOS, Ubuntu, Android, and iOS.

Ultrasurf

Ultrasurf is a closed-source anti-censorship tool designed for Windows operating systems [435]. Ultrasurf initially relied on Internet Explorer to allow user connections but now uses Google Chrome browser. Fingerprinting and blocking attacks against Ultrasurf have been demonstrated in the literature [17].

Your Freedom

Your Freedom is a proxy tool designed for anti-censorship. Your Freedom is closed-source and supports connections for various Internet protocols. Your Freedom offers binaries for Windows, macOS, and Android [500].

Freegate

Freegate is a closed-source anti-censorship tool designed for Windows operating systems [119]. The tool's company, Dynamic Internet Technology (DIT), claims that millions in China, Cuba, Iran, North Korea, and many other countries use it. The developers focus on providing easy access to a network of proxies to provide fast access to filtered web pages. The tool connects to the DynaWeb network and hosts a local proxy to which users connect their web browser.

GoodbyeDPI

GoodbyeDPI is an open-source tool for Windows operating systems that bypasses deep packet inspection (DPI) blocking found in some ISPs [182]. 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 manipulations have been demonstrated to bypass some DPI implementations and access blocked content, such as; (1) using TCP-level fragmentation of first packets, (2) replacing "Host" header values, (3) adding additional spaces in URIs, (4) mixing letter cases of header values, and (5) faking TTL/sequence/acknowledgment numbers.

Powertunnel

Powertunnel is a software fork of GoodbyeDPI implemented in Java [353]. Powertunnel is designed as a proxy server with built-in DPI-circumvention and DNS over HTTPS (DoH) capabilities.

2.2.2.2 Privacy-focused Approaches

The Tor Browser

The Tor Browser is a modified version of the Firefox web browser, specifically designed to route web traffic over the Tor network [109,110]. The browser is bundled with a Tor executable and automatically creates a local proxy to tunnel traffic over Tor. The Tor network consists of around 7000 relay servers run by volunteers [428]. The Tor protocol uses onion routing to provide anonymity and obfuscate the source of IP traffic [110]. After three nodes are selected (an entry "guard" relay, a middle relay, and an exit relay), the initial negotiation is wrapped in three layers of encryption, using the public keys of each relay. A guard relay only ever knows the source and the middle hop; a middle relay only ever has knowledge of the guard and the exit, and an exit relay only ever sees the IP address of the middle relay and the destination website. Tor was originally designed as a privacy-enhancing technology, funded in part by the Naval Research Laboratory of the United States. The Tor Project's original stated goal was anonymity, not censorship avoidance, but users discovered that the design of the Tor Browser made it particularly effective as an anti-censorship tool. When initially connecting to the Tor network, the Tor Browser greets users with the following message: "The Tor Project is a U.S. 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open-source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding" [429]. Several academic papers have been written about attacks against the Tor network [239,145,130,198,8], and many protocol and network improvements have been implemented to make the network robust.

INVISV Relay

INVISV Relay is an Android application that uses multi-party relay (MPR) architecture to route user traffic in such a way as to decouple the source of the request from the destination [218]. Relay is designed as a privacy-enhancing technology rather than for anti-censorship. Depending on how the blocking is implemented, its technique for routing traffic through two encrypted hops (rather than three as designed in Tor) can circumvent censor blocking. Relay also ensures that the IP address (provided by a third-party Content Delivery Network) of a user's exit node resolves nearby to the device's geolocation. Relay does this to provide localized or region-specific content, which is uncommon for VPN providers or anonymizing software.

Apple iCloud Relay

iCloud Relay on Apple iOS devices is also an MPR service [29]. Apple calls its exit nodes "egress proxies" and its first hops "ingress proxies." Similar to INVISV Relay, a third-party CDN provides similarly situated geolocation IP addresses while separating source traffic from its destination. Traffic is encrypted using QUIC at the transport layer, and DNS queries are resolved using an oblivious DNS over HTTPS (DoH) implementation. Apple prioritizes speed and the user experience over anonymity properties.

2.2.2.3 Incidental Approaches

Cloudflare WARP

WARP is a specifically tailored VPN client with additional DNS functionality. Cloudflare released the tool to increase DNS privacy using their public 1.1.1.1 and 1.0.0.1 DNS resolvers. WARP utilizes the Wireguard VPN protocol to funnel traffic over its low-latency global network. WARP offers several configurations; Wireguard all traffic with unencrypted DNS through the tunnel, Wireguard all traffic with DoH, or DoH DNS resolution only. WARP offers free and paid tiers for its service. Cloudflare offers client software for iOS, Android, Windows, macOS, and Linux desktops [354].

OpenVPN

OpenVPN is a widely-used, open-source VPN protocol that has compatibility with several encryption libraries and can operate over TCP or UDP. "For key establishment, OpenVPN can either use TLS as a handshake protocol or use pre-shared keys" [126]. Angelo suggested that OpenVPN has advantages over IPsec in terms of ease of deployment and complexity [25]. Critics of OpenVPN describe its large code base as difficult to audit or find flaws in the software, despite reliance on the technology in many industries to protect high-value internal computer systems. Two investigations into the commercial VPN ecosystem are available here for further reading [361,244]; most of the companies discussed rely upon the OpenVPN protocol to provide their services.

*WireGuard*²

WireGuard is a communication protocol that was designed to address shortfalls in similar VPN technologies. The project was started by Jason Donenfeld in late 2016, according to the earliest commits on <https://git.zx2c4.com>. Jason describes how his idea was to create a replacement for OpenVPN and IPsec in his talk given at Black Hat 2018 at Mandalay Bay Casino, Las Vegas [113]. Overall, the protocol operates at layer 3 of the Open Systems Interconnection (OSI) model, commonly referred to as the network layer. This is in contrast to IPsec, which offers layer 2 functionality. The WireGuard team began with the concept of a Linux network interface and built their protocol around that concept [114]. The protocol supports IPv4 and IPv6 traffic outside and inside the tunnel. WireGuard uses what Jason describes as "modern, conservative" cryptographic principles and primitives. He also describes the protocol as "opinionated," meaning that it provides the exact cipher suite and key exchange mechanisms to make WireGuard work. It does not allow for negotiation or administrator configuration of the underlying protocol without fundamentally redesigning it. WireGuard only operates using UDP at the transport layer. The WireGuard team also emphasizes the protocol's simplicity and auditability. The intent is that a single researcher, or a small team of security professionals, can easily audit the entire code base. The Linux implementation of WireGuard has under 4,000 lines of code, significantly less than other competitors in the VPN space. Additionally, the authentication model is similar to that of Secure Shell (SSH) and its `authenticated_keys`; any administrator that knows how to administrate with SSH can fundamentally understand WireGuard's authentication.

The WireGuard protocol has many advantages, including forward secrecy, ease of auditing and implementation, high performance, and minimal attack surface. The protocol has the potential to be a building block for many different system designs. Projects such as Tailscale [414] and Cloudflare WARP [354] demonstrate how WireGuard can be used to implement secure communication into larger software platforms. WireGuard can assist in integrating encryption mechanisms into other systems that would otherwise potentially be transmitted in the clear. It

² Portions of this section were previously published in a Purdue University Technical Report [284].

was not designed to be an anti-censorship tool, but its properties allow for the circumvention of many non-targeted threats against Internet communications.

The protocol also has limitations. When faced with an ISP or a nation-state actor that wishes to block VPN-based traffic circumventing censorship, WireGuard performs similarly to other incidental approaches. Given the nature of the WireGuard exchange format and encrypted traffic formatting, when subject to deep packet inspection (DPI), WireGuard traffic is easy to detect — and subsequently, filter out.

2.3 Nation-state Censorship Overview

Several concerted efforts have been undertaken in the last several decades to develop an understanding of how and where Internet censorship happens. In 2008, Deibert et al. presented results of "the first systematic, academically rigorous global study of all known state-mandated Internet filtering practices" [105], showing evidence of how 26 of 40 countries conducted Internet filtering activities; the trend has only increased since then. The OpenNet Initiative partnership Deibert et al. operated under shut down research operations in 2014 [328] but made all of its datasets and published materials publicly available online.

Other labs and advocacy organizations have taken on the task of measuring Internet connectivity around the globe, showing censorship where it takes place. The Open Observatory of Network Interference (OONI) began data collection on Internet censorship in 2012 and continues today [331]. OONI datasets, data explorer, and API are available online.³ Censored Planet Lab at the University of Michigan, USA, has created and hosted several global Internet measurement projects [68]. "Satellite" [413] and "Hyperquack" [358,447] measure DNS interference and application layer HTTP/HTTPS manipulation, respectively. Their dashboard for viewing data is also publicly available online.⁴ ICLab is a different global, longitudinal measurement platform utilizing commercial virtual private networks (VPNs) to gain vantage points in countries around the globe to determine censorship activities. The Citizen Lab at the University of Toronto, Canada, has a research effort focused on freedom of expression [421] — although their reporting

³ OONI: <https://ooni.org/data>

⁴ Censored Planet: <https://dashboard.censoredplanet.org>

often focuses on specific political or social impacts of technology censorship rather than wide Internet measurements.

Freedom House is a non-governmental organization (NGO) based in Washington, DC, USA. The non-profit group conducts research and advocacy on democracy, political freedom, and human rights, often focusing on Internet freedoms [163]. The group has produced the FOTN report since 2009, qualitatively measuring censorship in up to 70 countries around the world. The report provides valuable macro-level analysis of how users experience the Internet and if freedom of expression is permitted on a scale of "free," "partly free," "not free," or not assessed. Freedom House breaks down survey results into scores for three categories; Obstacles to Access, Limits on Content, and Violations of User Rights. The first two categories are particularly relevant to this study. The FOTN country list and rank order were the foundation for the data collection in Chapter 5.

In their seminal report, *Access Denied*, Deibert et al. summarized the output of their study in several tables, shown in Figure 5 and Figure 6. The nations shown to have evidence of filtering in Figure 5 did so by technical means, not by legal orders or intimidation. While not wholly comprehensive, their sampling of 40 countries gave the world insight on a larger scale into where technical censorship was being conducted in 2006. The authors concluded that the nation-states that practice state-mandated filtering are predominately clustered into three regions of the world: east Asia, the Middle East/North Africa, and central Asia. While these insights are still relevant, censorship has expanded to many other countries in the last 15 years. Censorship occurs even in countries that espouse freedom of speech and expression as values, demonstrating the complexity and nuance of the issues.

Filtering by state		
Evidence of filtering	Suspected filtering	No evidence of filtering
Azerbaijan	Belarus	Afghanistan
Bahrain	Kazakhstan	Algeria
China		Egypt
Ethiopia		Iraq
India		Israel
Iran		Kyrgyzstan
Jordan		Malaysia
Libya		Moldova
Morocco		Nepal
Myanmar		Russia*
Oman		Ukraine
Pakistan		Venezuela
Saudi Arabia		West Bank/Gaza
Singapore		Zimbabwe
South Korea		
Sudan		
Syria		
Tajikistan		
Thailand		
Tunisia		
United Arab Emirates		
Uzbekistan		
Vietnam		
Yemen		

* Testing in Russia was limited to a selection of ISPs in Moscow; these preliminary results may not extend beyond this sample.

Figure 5. Evidence of censorship by nation-states, as of 2006 [105]

Figure 6 elaborates further on the technical censorship means detected in each nation based on OpenNet's testing methodology. Measurement methods were manually implemented and more crude than in recent studies. Lists of websites were generated based on categories of content that are often censored (e.g., free expression, human rights, gambling, pornography, minority faiths, and anonymizers). Researchers then browsed those websites from various vantage points within ASes of particular ISPs in target countries. Deibert et al. categorized the censorship they observed into four broad categories: IP blocking, DNS tampering, Blockpage, and Keyword.

Blocking techniques				
	IP blocking	DNS tampering	Blockpage	Keyword
Azerbaijan	X		X	
Bahrain		X	X	
China	X			X
Ethiopia	X			
India	X	X		
Iran			X	X
Jordan	X			
Libya	X			
Myanmar			X	
Oman			X	
Pakistan	X	X		
Saudi Arabia			X	
Singapore			X	
South Korea	X	X	X	
Sudan			X	
Syria			X	
Thailand			X	
Tunisia			X	
United Arab Emirates			X	
Uzbekistan*			X	
Vietnam		X	X	
Yemen			X	X

Blocking behavior included in this table may include international gateway level filtering, and filtering techniques used by different ISPs.
 * In Uzbekistan, the blockpage does not clearly indicate that filtering is occurring but rather redirects users to a third-party Web site.

Figure 6. Blocking techniques by nation-states, as of 2006 [105]

More recent studies broadened global Internet measurement by using more automated means and relying less on volunteers within censored countries for data collection. Ethical concerns, the cost of computing resources, and the availability of connectivity in censored nation-states inspired the Censored Planet Lab to create Satellite [390]. The tool uses a single host to collect DNS resolutions from many globally-distributed and public DNS resolvers. Satellite leverages the Alexa top 10,000 list of domains for testing. Researchers rely on precise, weekly measurements to show aggregate trends rather than focusing on one specific event or geographic area. Satellite monitors for successful DNS resolution and has several methods for estimating DNS censorship techniques when resolution queries fail. Figure 7 illustrates worldwide DNS interference in a snapshot at the end of 2020 [512].

Percentage of resolvers facing interference by country

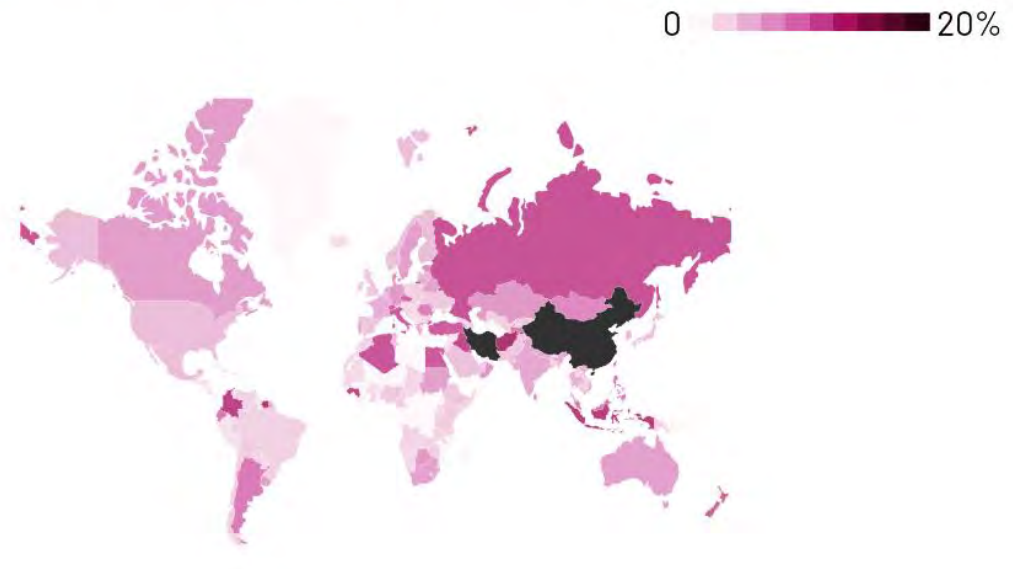


Figure 7. Censored Planet Satellite visualization (August 10, 2020)

Freedom House, USA releases an annual *Freedom on the Net* report, evaluating "Internet freedom" on a 100-point scale of free, partly free, or not free. Their methodology includes 21 questions and about 100 sub-questions from three categories; "obstacles to access," "limits on content," and "violations of user rights." The "limits on content" category specifically addresses the technical filtering of websites. The overall report results provide an overview of where censorship is occurring and trends from year to year. Figure 8 shows the mapped results from *Freedom on the Net 2021* report [396].

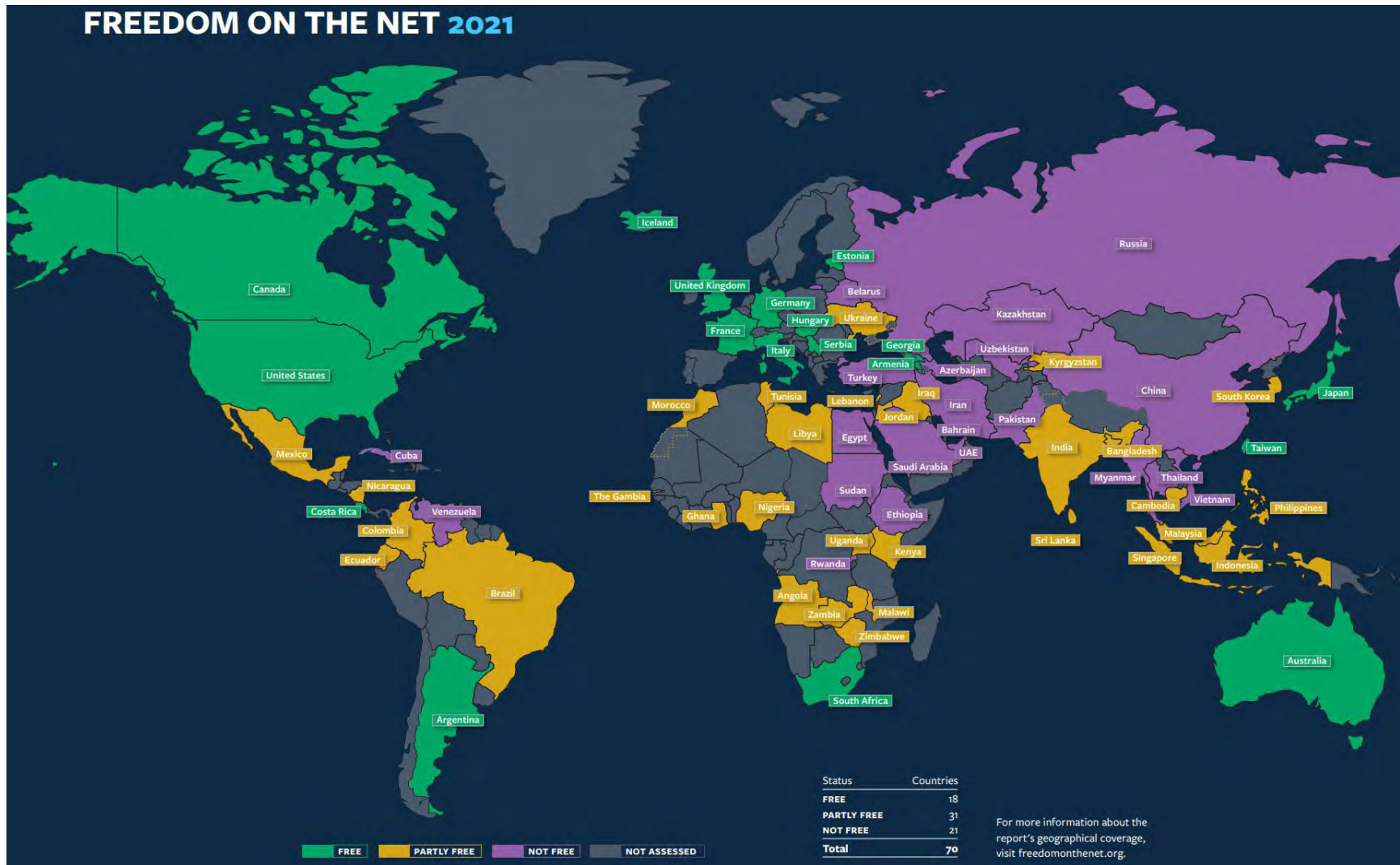


Figure 8. *Freedom on the Net 2021* global overview map [396]

CHAPTER 3: A REFERENCE MODEL FOR INTERNET CENSORSHIP TECHNOLOGIES

3.1 Background

Internet censorship is an increasingly relevant area of study as global communications become further reliant on computer networks. As societies determine what information is objectionable, authorities in some nation-states implement content filtering or deny access to Internet resources. Some censorship is widely agreed upon as a social good. In other instances, censorship is seen as a limit on individual freedom of expression or freedom of assembly in violation of international norms. In response, software developers have created anti-censorship tools that circumvent censors to promote free and open access to information online. The "arms race" of censors versus circumventors continually evolves as technology advances.

Several intersecting research communities pursue the study of Internet censorship. Internet measurement researchers observe and describe how Internet censorship occurs from a technical perspective. Political and social science researchers discuss modern censorship, its impacts on people in different societies, and its interplay on the international stage. Internet freedom advocates and researchers bridge the gap between these disciplines. Privacy-enhancing technologies communities create, promote, and evaluate software that enables circumvention of Internet censorship.

No current conceptual model exists to describe Internet censorship technologies. Any knowledge area "has an underlying model of the phenomena it investigates, be it tacitly assumed or explicit" [225]. Creating a reference model to holistically represent the problem space across the domain of Internet censorship methods will assist researchers, policymakers, and civil liberties advocates in conceptual understanding of the technical ways in which Internet censorship occurs. The model can serve as an educational tool and, with future development, an evaluation framework.

3.2 System Modeling

The Organization for the Advancement of Structured Information Standards (OASIS) defines a reference model as "an abstract framework for understanding significant relationships among the entities of some environment, and for the development of consistent standards or specifications supporting that environment. A reference model is based on a small number of unifying concepts and may be used as a basis for education and explaining standards to a non-specialist. A reference model is not directly tied to any standards, technologies or other concrete implementation details, but it does seek to provide a common semantics that can be used unambiguously across and between different implementations" [323]. The author chose a reference model over other representations because of their widespread use in Information Systems research [303] and their accessibility to an interdisciplinary audience. Reference models also facilitate understanding among many stakeholders from different backgrounds and areas of expertise [76]. Schuba and Spafford posit that "[computing] systems are, at a conceptual level, composed of separate, interacting functional components" [389]. The model presented in this paper is descriptive in that it captures the functionality of Internet censors (extensively covered in Chapters 4 and 5) in an abstract and technology-agnostic fashion. The model can also be used prescriptively, given its comprehensive nature.

Fettke and Loos provided a methodology to construct an empirically grounded reference model. The author used the steps shown in [139] to provide transparency and validity to the model in §3.3. The process consisted of five phases: Planning, Model Construction, Validation, Practical Testing, and Documentation. The methodology is summarized and depicted in Figure 9. Phases 1 and 2 consisted of all the preparatory scholarship needed to understand the scope of the problem domain. The systematic literature review (SLR) in Chapter 4 and prior work §2.1-§2.2 enumerated the elements that comprise the model's functional components in a comprehensive manner. Phases 3 and 4 involved validation of the model, using the systems and evidence of censorship methods from Chapters 4 and 5 to ensure the model is all-inclusive. The author chose these methods over the qualitative methods suggested by Fettke and Loos (e.g., workshops, surveys, or Delphi studies). This paper's author asserts that Internet censorship is a widely studied problem domain, with hundreds of research publications worth of empirical data to draw from. Subject matter expert (SME) consensus was not necessary to achieve verisimilitude in the

model representation. Others in the Information Systems (IS) research communities have taken similar approaches in modeling systems [76,307,388]. Phase 5, the documentation of the model, is Chapter 3 of this dissertation.

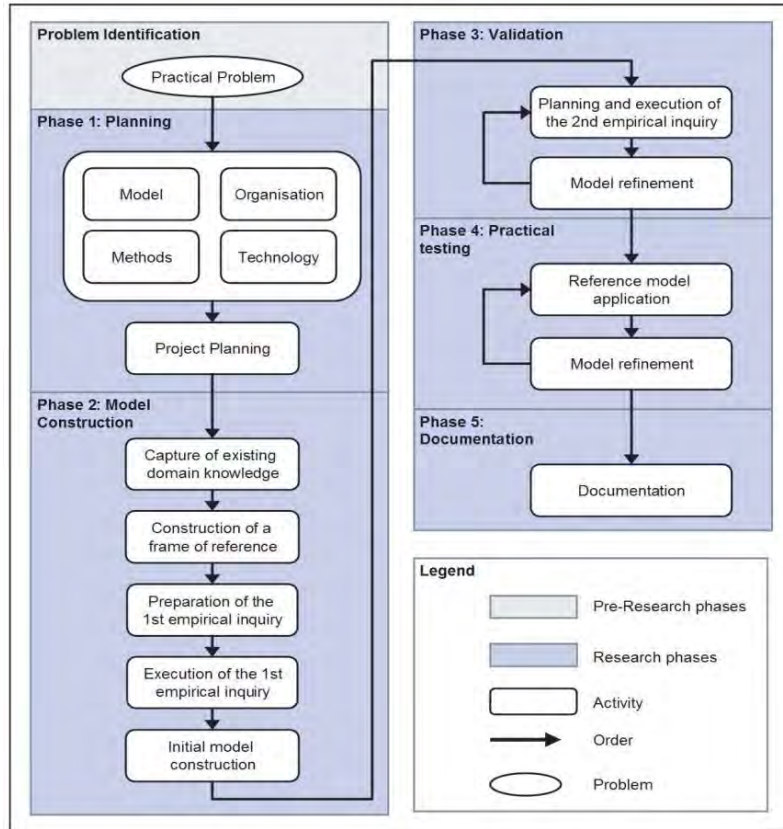


Figure 9. Methodology for construction of an empirically grounded reference model [139]

3.2.1 Validity

To validate the model, the author performed a systematic literature review pertaining to Internet censorship. The survey encompassed Internet censorship methods and evidence of technical blocking or filtering over the past three decades. By studying all known censor methods, as well as relevant theory leading to emerging technological advancements, the author captured the conceptual functions necessary to build the abstractions of the reference model. The survey is available in its entirety in Chapter 4. That survey also resulted in the creation of a taxonomy of

Internet censorship methods, a one-page reference material for characterizing censor activities. Additionally, the author revisited the functional components of the reference model in §3.3 after the completion of the study in Chapter 5 [286] to ensure the model encompassed the real-world measurement data and analysis presented there. This iterative process enabled a more comprehensive development cycle for the model's components.

3.3 Reference Model

The reference model explains the functionality of computing systems involved in allowing or denying access to Internet resources. The model is an abstraction intended to describe existing Internet Protocol suite configurations and potential future protocol or technology advancements. The model can be interpreted as a conceptual system composed of several functional components. §3.4 describes the components in detail.

Figure 10 depicts a high-level overview of the reference model for Internet censorship technologies. It is an abridged version of the detailed representation shown in Figure 11. Figure 10 shows how the functional components make up the overall system, the flow of messages through the system components, and how the components interact with one another. Lines with arrows on both sides indicate bidirectional communications; Lines with one arrow on a receiving end indicate unidirectional communications; and dashed lines represent internal system communications. Red indicates censor-controlled entities and processes, blue represents anti-censorship, and gray intermediaries are third parties that comprise parts of the global Internet. Circles are entities, quadrilaterals are processes, and a diamond shape represents decision enforcement. "Users" typically initiate communication, while "publishers" typically host or provide content.

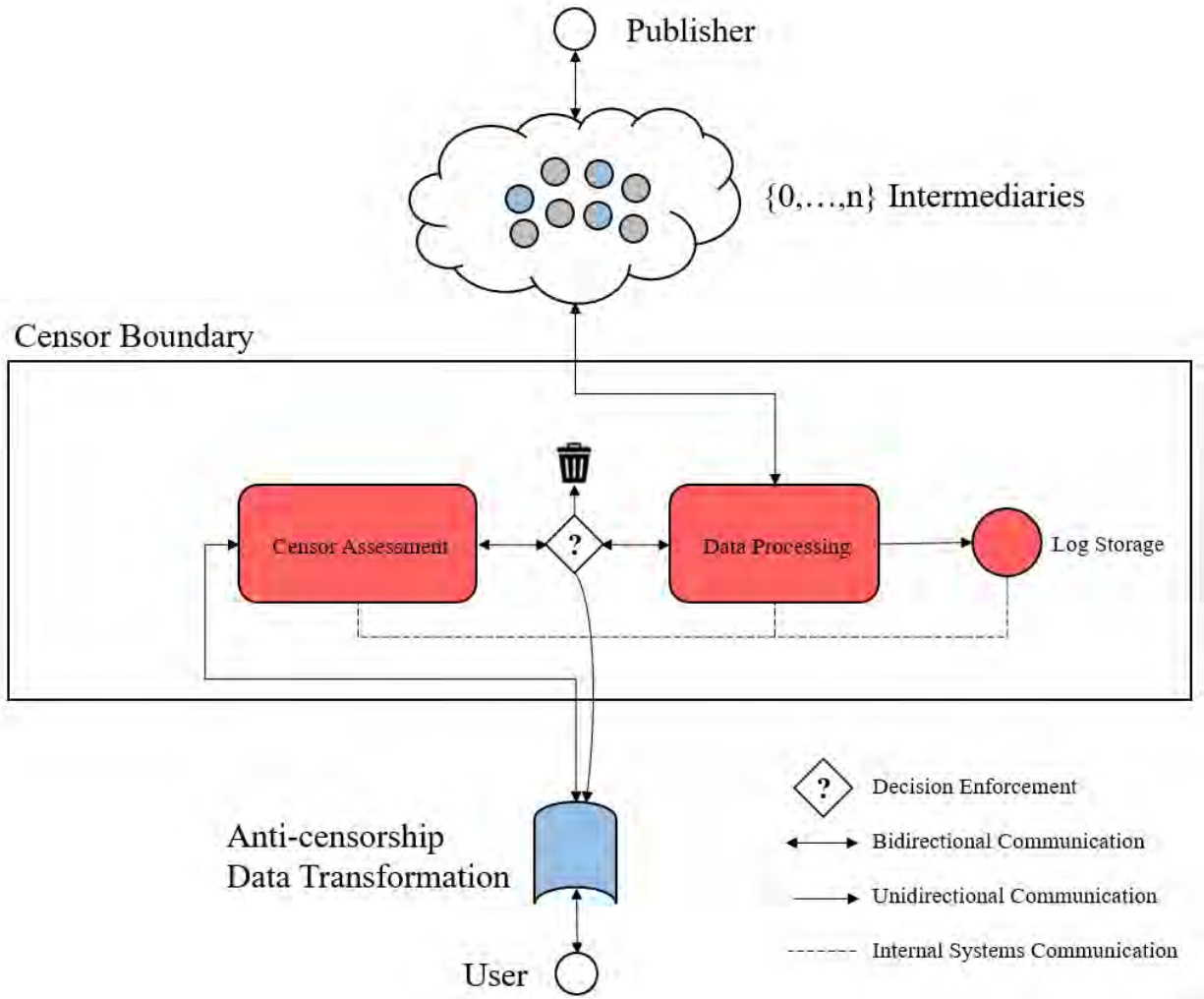


Figure 10. Abridged version of the reference model for Internet censorship technologies

Consider the scenario where a user wishes to communicate with a publisher. The user must use communication channels available to them, some of which are controlled by a censor. The message must traverse censor infrastructure and systems before it reaches the global Internet and eventually is routed to the publisher. A publisher may sometimes act as a user themselves (e.g., a web API or an interactive user) and vice-versa; communication may be bidirectional and continuous or one-way and delimited. A common practical case of an exchange represented by the model would be an Internet user with a web browser attempting to access a web page (publisher) on the world wide web.

The user may send their message according to the default parameters of the software they use. They may also choose to perform a data transformation of some kind on their message before it reaches the censor boundary. This may involve obfuscating the contents of the message (e.g., by using encryption), manipulating metadata of the message (e.g., its source, destination, packet header fields, and timestamps), or initiating a tunnel or proxy connection to pass the message through an intermediary. Once the user's message reaches the censor boundary, the user has no control over how the message is handled.

Within the censor boundary, a censor has several functional components. First, the censor does an assessment of traffic arriving at its border. The assessment process observes the traffic and characterizes it according to predefined parameters in search of "objectionable" material. Based on the censor assessment, a decision is made. The message can be silently discarded, rejected and returned to the user, or passed along for further processing. Once a decision is made, some level of data processing will occur. This processing could involve logging transactions, prioritization of traffic, routing and re-addressing decisions, or otherwise.

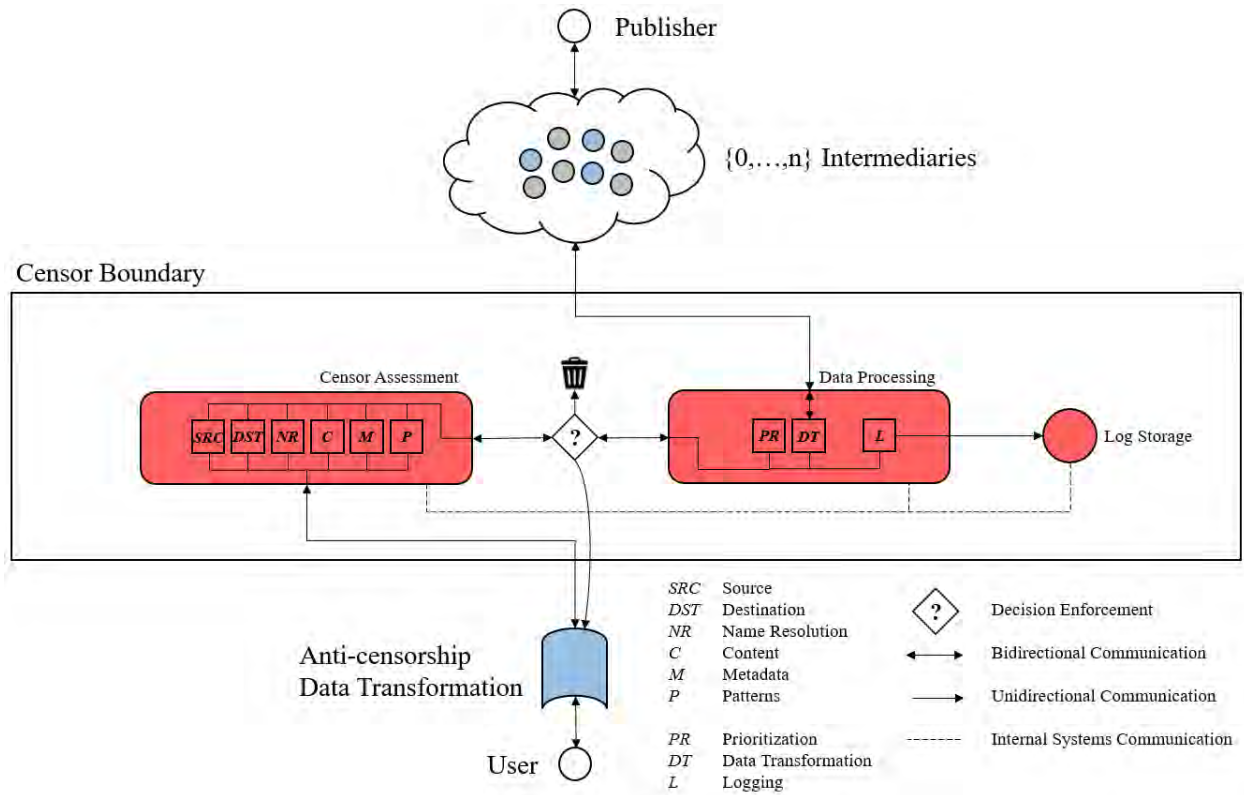


Figure 11. Reference model for Internet censorship technologies

3.4 Reference Model Components

The reference model depicted and described in §3.3 consists of the following functional components: Censor Assessment, Decision Enforcement, and Data Processing. The model also contains the essential entities involved in conceptualizing Internet censorship technology activity. Figure 12 provides a detailed view of the censor boundary components, described in the following subsections.

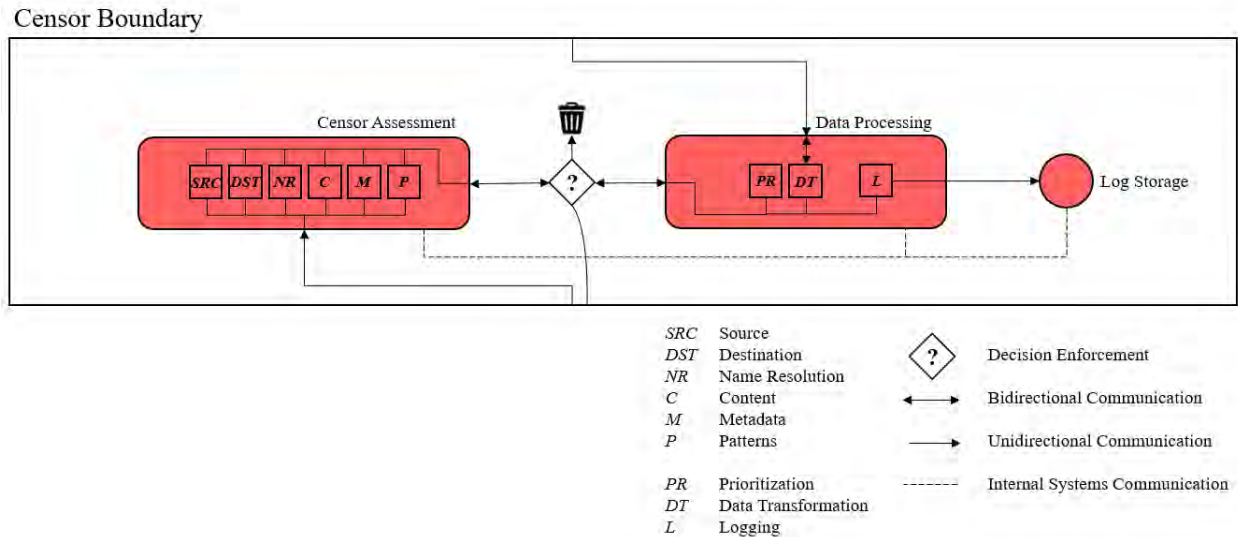


Figure 12. Censor Boundary depicted

3.4.1 Censor Assessment

Whenever traffic arrives at the censor boundary, the censor assesses if a message should be permitted. The censor makes this assessment based on configured rules, log data of previous transactions the censor has negotiated, and characteristics of the communication it observes upon arrival. The range of characteristics and methods for detecting said characteristics is wide; see Chapter 4 for a taxonomy of Internet censorship methods and examples of associated techniques. At the conceptual level, these characteristics can be generalized into six categories: Source, Destination, Name Resolution, Content, Metadata, and Patterns.

Source and Destination. Source and destination are self-explanatory. In modern systems, these characteristics are usually defined by an Internet Protocol (IP) address or port number. It is common for censors to deny access to resources based on destination, such as by using IP blocklists, Uniform Resource Locator (URL) blocklists, or even destination ports of popular applications. Denying access based on the traffic source is less common, given how IP addresses are assigned and their ephemeral nature.

Name Resolution. Name resolution has developed to be a critical element of the modern Internet. Because human beings are the primary users of the world wide web, the translation of a human-readable name to an IP address enhances the user experience online. Name resolution also assists software developers — hard-coding IP addresses into code would be difficult to maintain. Using words that can be translated to an address allows for flexibility in hosting infrastructure. The primary protocol to enable name resolution on the Internet has been the Domain Name System (DNS) since the 1980s.

Internet censors can monitor name resolution for objectionable destinations. Service providers, such as Internet Service Providers (ISPs), often provide name resolution services to their users and are uniquely situated to interfere or tamper with the name resolution responses as a means of censorship or surveillance. Advancements to DNS, such as DNSSEC, DNS over TLS (DoT), and DNS over HTTPS (DoH), have attempted to add integrity, authentication, and obfuscation to the name resolution process. The process is integral to how the Internet functions and is, therefore, a common target of censorship activities.

Content. Another evident approach a censor may take in determining if a message is objectionable is to look at its content. If the content of a message is observable and intelligible, a censor may filter traffic based on keywords or phrases. In the context of IP traffic, the payload of an IP packet is everything found after the packet headers. If the packet is unencrypted or uses a protocol that is inherently transmitted in plaintext, a censor may passively search for objectionable content and take action when it is found. Censorship of this kind has occurred in HTTP, SMTP, FTP, and various other Internet protocols (see Chapter 4 for details). Transparent proxies, in-line network filtering, or middleboxes can enable deep packet inspection (DPI) activities.

Metadata. When targeting a message, a censor may refer to the context surrounding the message rather than the message's content. Metadata is "data about data" [370]. In the years following the Edward Snowden disclosures related to surveillance activities conducted by Western intelligence services, the term metadata rose in prominence and common public usage. Agencies did not necessarily collect the content of phone calls, emails, or simple message service (SMS) messages

but rather information about those exchanges [174]. In this context, examples could include transactional information about the communication — timestamps, geolocation, phone numbers, and others.

In terms of Internet traffic and the reference model, metadata includes a variety of pieces of information a censor can use to make censorship assessments. A censor may be able to *infer* sensitive information about a message or its sender based on the frequency of messages or timing, even if the traffic stream is encrypted [30,408,228,137]. Correlation attacks have also been demonstrated in the literature, where a censor uses statistical techniques to correlate traffic from different parts of an anonymity network to de-anonymize a user's online activity [130,239]. There are also side-channel attacks against devices or software implementations, which rely on metadata, such as measuring the power consumption of a device or sound output during normal functioning. See [411] for a survey of such attacks. While many censorship methods that rely on metadata currently occur in academic research rather than widely implemented national systems, increases in computational power may make them more feasible in the future.

Patterns. In the context of the reference model for Internet censorship, the author refers to patterns as discernable sequences in the bitstream of the message traffic. Rather than looking inside the content of a message or at metadata derived from the message, patterns involve observing the bitstream as it transmits. This may involve observing "bursty" activity in an encrypted bitstream to identify a particular application in use or the inverse; a lack of a specific bit pattern could represent an anomaly and reveal information about the message. As Transport Layer Security (TLS) has proliferated and been adopted by popular web servers, more cybersecurity products focus on detecting specific traffic despite encryption. Some operate based on signatures, while others rely on a machine learning classifier to make determinations and dynamically detect patterns. A survey of methods for encrypted traffic classification by Velan et al. is available [449].

3.4.2 Decision Enforcement

After the censor assessment has concluded, a decision about what to do with a message must be made. There are four available outcomes. The first option is to silently drop the message. The

user will not be informed that their request was denied, and the client software will handle the error in whatever way it was programmed. In terms of a web browser, if a request is silently denied by a firewall, the web browser will eventually time out and present the user with an error message. A censor may still perform data processing after the decision to drop a message, such as logging that the attempt was made. This first option is represented by the one-way direction to the “bit bucket” or “trash bin” icon in the model.

The second option is to reject the message and inform the originating user of the rejection. An example of this in Internet traffic is a TCP reset flag on an IP segment. When a user receives a TCP-RST, the connection is closed, and the user is aware that a rejection happened. This contrasts with silent drops, which may present similarly to the way network errors or timeouts manifest.

A third option would be to redirect the user's request to a resource the censor controls rather than the intended destination. Practical examples of this have been demonstrated in nations that use blockpages to inform users that their request for access has been denied (see §4.4.1 for further discussion). Redirection may also involve serving the user a "honeypot" [15,16] or false information masquerading as a legitimate message.

The fourth decision option is to allow the message to move toward its destination, optionally logging aspects of the communication or applying data transformation or prioritization to the message.

3.4.3 Data Processing

Data processing is a critical aspect of any communication device. This process component within the model represents all of the standard functions a router, middlebox, software-defined network (SDN), or other Internet routing device must perform. Enumerated elements for the purposes of Internet censorship are prioritization, logging, and data transformation.

Prioritization involves manipulating traffic based on some criteria of importance. In enterprise IT architecture, administrators may prioritize real-time communication traffic (e.g., voice over IP

calls) to ensure appropriate quality sound, while traffic that is minimally impacted by waiting in a queue (e.g., email) is deprioritized during peak throughput usage on a network. There are several example approaches and protocols available for quality of service (QoS) on IP networks, such as the type of service (ToS) indicator in the IPv4 header, the differentiated services (DS) field in the IPv6 header, or the Resource Reservation Protocol (RSVP). Services may also indiscriminately throttle traffic. Customers may pay for a particular amount of throughput each month, and after the data quota is consumed, the customer is throttled down to a slower speed — to preserve the throughput for other customers and encourage the throttled user to pay for more data allowance if they continually incur large amounts of usage. In terms of Internet censorship, these approaches can also be used to deny access to objectionable content. A censor may throttle connections to particular social media sites for a specific period of time or at certain times of the day, such as nightly curfews. A censor may also use indiscriminate throttling to achieve the same effect as an Internet shutdown but attempt to distance their involvement by blaming the lack of access on networking errors. See §4.4.6 for an in-depth discussion of censor throttling.

Logging is integral to computer networking. Logs allow devices to "remember" previous transactions and activity, especially in the case of stateless connections. Many cybersecurity solutions rely on log data to make inferences about traffic. Censors may use log servers to monitor frequency between particular sources or destinations, identify previous offenders, or store the most up-to-date blocklists. Logging actions may occur after any decision enforcement action in the reference model.

Data transformation (DT) is the final and critical element of the data processing component. DT is an abstraction that refers to any data manipulation of a message that traverses the censor boundary. It is rare in IP-based communication for a message to pass through routing devices unchanged; processes such as network address translation (NAT) to modify source addresses and ensure traffic returns to the appropriate RFC1918 private LAN are commonplace. IPv6 can allow for end-to-end reachability of devices from across the Internet because of its significantly larger address space. Still, end-to-end configurations have seen limited implementation thus far, even with IPv6 addressing [327]. Censorship circumvention researchers cannot change the

manipulations that happen within a censor boundary. Still, they can study the data transformations and use that information to inform their evasion strategies [489,53,51,54,50].

3.5 Example Applications of Reference Model

The reference model for Internet censorship can foremost be used as a pedagogical tool. The model allows for conceptualization without inundating the learner with technology-specific detail or considerations. For example, a censorship regime may be as small as one middlebox or as large and complex as China's "Great Firewall" [467]. The reference model's construction allows for mutual understanding and system design representation without the associated cost or expertise required to build a prototype or emulation.

Another example application of the model is for comparing inputs to the system. Demonstrating the effectiveness of anti-censorship software can be illustrated based on which elements within the censor boundary components are impacted. This approach will not offer a detailed or nuanced technical discussion of each individual piece of software but can inform users and policymakers of the general protections each tool provides for a defined threat scenario.

Figure 13 illustrates a specific anti-censorship tool's capabilities against a particular censor threat model. The author drew data from Chapter 5, which showed that Turkey performed DNS tampering, HTTP/URL/Keyword filtering, and TLS-based filtering against its citizens. The author depicted Tor Browser as the anti-censorship data transformation the message travels through before entering the censor boundary.

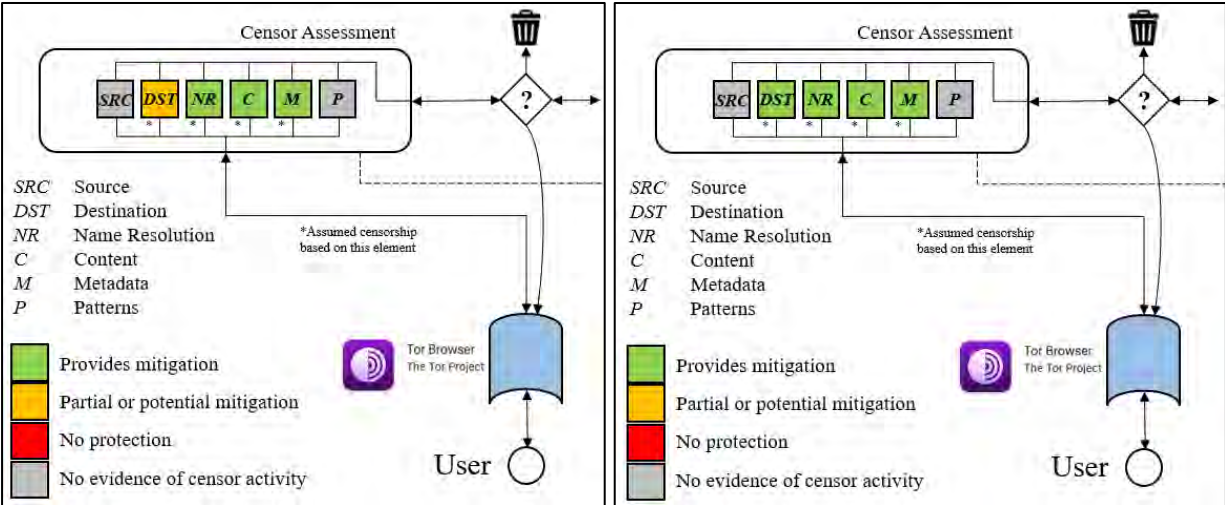


Figure 13. Example use of reference model assessing Tor Browser (Left) Bootstrapping phase, (Right) After connection establishment. Assumed threat model: Turkey, 2021. Censor performs DNS tampering, content filtering, and TLS-based filtering.

The Tor Browser is a modified version of the Firefox web browser, specifically designed to route web traffic over the Tor network [109,110]. The browser is bundled with a Tor executable and automatically creates a local proxy to tunnel traffic over Tor. The Tor network consists of around 7000 volunteer relay servers [428]. The Tor protocol uses onion routing to provide anonymity and obfuscate the source of IP traffic. After three nodes are selected (an entry "guard" relay, a middle relay, and an exit relay), the initial negotiation is wrapped in three layers of encryption, using the public keys of each relay. A guard relay only ever knows the source and the middle hop; a middle relay only ever has knowledge of the guard and the exit, and an exit relay only ever sees the IP address of the middle relay and the destination website.

The author must represent the Tor Browser in the reference model in two stages. First is the bootstrapping stage, where the Tor service contacts a directory authority server to receive lists of possible relay nodes so the client can build a circuit of three encrypted hops. The censor could attempt to deny the establishment of a Tor connection by blocking destination servers (e.g., directory servers or relays themselves). Tor browser has a built-in feature for censorship circumvention called bridges, which use obfuscation techniques or unpublished relays to bypass Tor censorship. Because Tor has potential mitigations for destination blocking that can be

enabled by a user, it is labeled in amber on the reference model. Tor Browser does not use name resolution to establish connections (green for *NR*), and no content is passed during bootstrapping (green for *C*). The other elements of the censor assessment are colored gray, given the lack of evidence that the censor utilizes methods that use those elements. Once bootstrapping is complete and a proper Tor circuit is built, Tor Browser mitigates the risk of censorship for all three elements of censor assessment, as shown on the right side of Figure 13.

For comparison, Figure 14 illustrates the capabilities of a different anti-censorship tool, GoodbyeDPI. This tool was specifically designed to thwart deep packet inspection (DPI) filtering. GoodbyeDPI uses manipulations to access blocked content, such as; (1) using TCP-level fragmentation of first packets in an HTTP request, (2) replacing "Host" header values, (3) adding additional spaces in URIs, (4) mixing letter cases of header values, and (5) faking TTL/sequence/acknowledgment numbers.

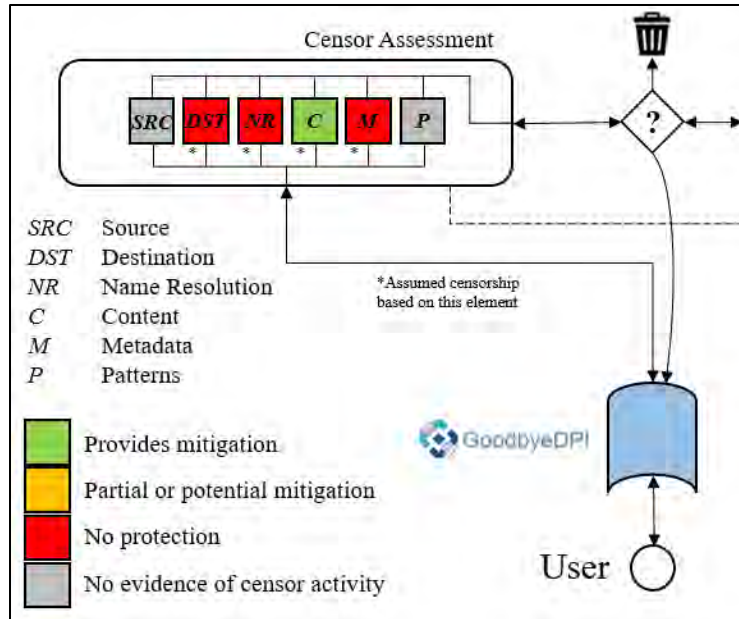


Figure 14. Example use of reference model assessing GoodbyeDPI
 Assumed threat model: Turkey, 2021. Censor performs DNS tampering, content filtering, and TLS-based filtering.

The author can represent GoodbyeDPI using the reference model as well. The tool focuses specifically on thwarting content filtering and provides mitigation against the censor scenario used in the previous Tor Browser comparison (green for *C*). GoodbyeDPI provides no protection against endpoint blocking or DNS-based filtering (red for *DST* and *NR*). GoodbyeDPI may be an appropriate tool for a user in Turkey, depending on the user's risk tolerance and the importance of maintaining consistent access to filtered content. The reference model better informs the user's decision. People can also adjust the threat model scenario to suit their needs (see Chapter 5 for a globally representative sample) and evaluate different anti-censorship tools accordingly.

This approach demonstrates an advantage over previous works that assess anti-censorship; the model describes censor capabilities and limitations from literature and measurement data (how it performs "on the wire") rather than relying on the design goals of anti-censorship software developers or on SME intuition.

3.6 Summary

This chapter presented a reference model for Internet censorship technologies. The model serves as a descriptive, conceptualized representation of censorship systems. The model is depicted graphically and consists of three functional components: censor assessment, decision enforcement, and data processing. It can serve as a pedagogical tool as well as a point of comparison among system designs. The model is presented so experts and non-specialist stakeholders alike can benefit from it. The descriptive knowledge of the model was validated by an iterative methodology, and the research studies that resulted are the next two chapters of this dissertation.

CHAPTER 4: A SURVEY OF INTERNET CENSORSHIP METHODS

4.1 Background

Internet censorship is a relatively new phenomenon in the human experience. 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. Given the advent of the world wide web in the early-1990s and the decreasing costs of computing devices and software, Internet technologies became available to the average citizen in some nations around the globe. Internet-connected devices continued to proliferate, allowing more people to communicate worldwide in near real-time over various mediums and protocols. In conjunction with these advancements, governments of nation-states around the globe 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.

Aceto and Pescapé define Internet censorship as "the intentional impairing or blocking of access to online resources and services," regardless of the intent, scope, or legitimacy of the actions [6]. The technical means by which Internet censors implement censorship vary widely but are generally constrained by standardized protocols that allow the Internet to function as a network of networks. Some Internet censors block web pages with "objectionable" content and inform users that their request was denied. Others simply drop the connection or manipulate the traffic so the connection appears to fail. Others will degrade the connectivity of a user when undesirable activity is detected, rendering the communication unusable. Applications that allow for unmonitored communications will often be blocklisted, denied based on ports used by the application's software or signatures of its data packets. In addition to blocking communication, Internet surveillance is closely tied to censorship activities. Detection of objectionable content (or anti-censorship tunnels) is generally the first and most important step toward implementing a blocking action. More aggressive nation-state censors will also completely disconnect Internet connectivity during perceived critical events, such as elections or periods of civil unrest.

Countless examples of Internet censorship have occurred over the last three decades. Social movements, such as the "Arab Spring" in the early 2010s, were accelerated by the use of technology to organize protests and garner support and became a target for censorship. Authoritarian leaders have demonstrated a willingness to selectively censor information they deem dangerous to maintaining power, sometimes disconnecting Internet connectivity completely during tumultuous periods [188] (see §4.4.7 for further discussion).

Censorship is a broad issue encompassing numerous aspects of modern societies. Some censorship is mandated by law in particular countries for various reasons, ranging from morality to political manipulation and control of the information environment. This work does not seek to make value judgments on the reasons for Internet-based censorship nor encourage the violation of laws. Instead, this study recognizes the paradigm that international expectations and norms are being violated in some places around the globe. In Article 19 of the universal declaration of human rights, the United Nations 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" [438]. 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.

4.2 Research Goals

This study offers a global view of the issues related to Internet censorship. While the definition and operationalization of freedom of expression are derived from an international organization (the United Nations), the author acknowledges that this work is influenced by Western philosophy because it originates from the United States. This work is also limited to scholarly sources available in the English language. In this article, censorship will refer specifically to censorship experienced by Internet users unless specified otherwise.

The primary question addressed in this chapter is, *what are the technical threats to Internet-based communications?* Thoroughly answering this question benefits several stakeholders. Users in countries that censor content benefit from a summary of threats and the historical context in which they occur. Internet measurement researchers benefit from a survey of literature in

detecting censorship and a direction toward unexplored avenues for future research. Researchers and developers who create anti-censorship software benefit from comprehensive metrics of *how* Internet traffic is filtered in practice. The Internet standards community, such as contributors to the Internet Engineering Task Force (IETF), may use the analysis when making foundational changes to Internet protocol implementation. Finally, policymakers who support freedom of expression benefit from a more nuanced understanding of how online censorship occurs.

4.3 Systematization Methodology

To answer the research question posed in §1.2, the author used a systematization of knowledge (SoK) approach. SoK papers have proven invaluable contributions to research communities, providing an overview of an entire body of literature to experienced researchers and new scholars. These works save researchers significant time and effort in discovering the edges of the state-of-the-art. Several SoK papers influenced this dissertation [245,433,437]. Systematic literature review methods help aggregate and distill knowledge from across a field of study. 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" [146]. Systematic reviews and meta-analyses found early success in medical research [302], and other research communities have benefited from their insights and approaches since then. Technology research must move as quickly as new technology is developed, and it remains 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 I.S. researchers face [325]. Their work is summarized in Figure 15. This dissertation utilizes Okoli and Schabram's approach to systematize the literature pertaining to Internet censorship. Detailed documentation of a research protocol promotes transparency and ease of reproducibility.

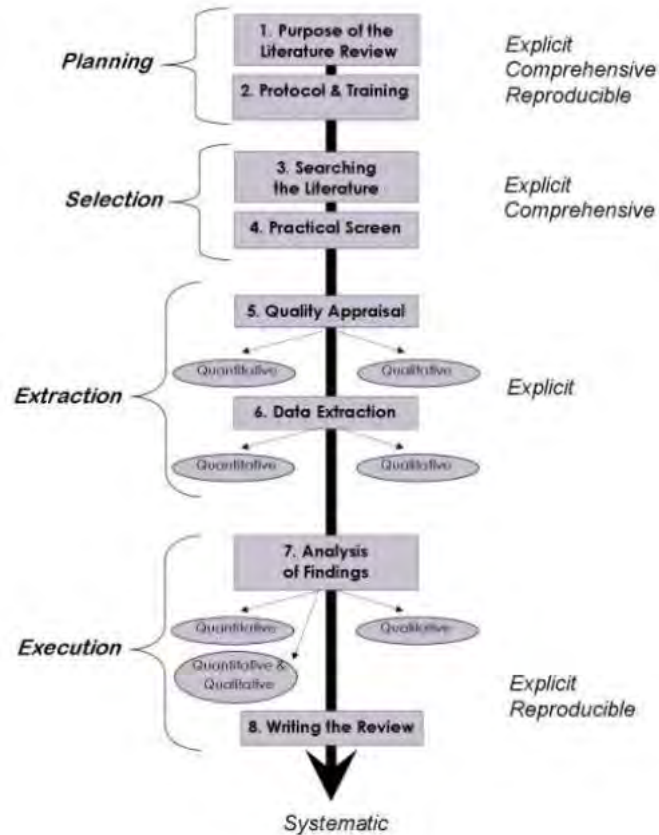


Figure 15. A systematic guide to literature review development [325]

The purpose of the survey was to systematize and categorize Internet censorship methods. In terms of this study, these methods are the 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 as a network of networks, namely, Internet Protocol (IP), Border Gateway Protocol (BGP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and QUIC. Several application-layer protocols are covered in-depth because of their importance to the world wide web. Thus, technology-focused literature was the primary subject of data collection. Communications, political science, and social science journals were also referenced when domains intersected.

Scholarly, peer-reviewed journals and conferences were the primary data source in the research protocol. In cases of emerging technology where scholarly works were not yet available, governmental reports, technical reports, and blogs from reputable organizations were utilized. Data sets from Internet measurement communities were important to a holistic view of how Internet censorship takes place. Finally, if necessary, qualitative data from advocacy organizations and media reporting was cited. While coverage of censorship was global, the author was limited to content written in the English language.

CensorBib⁵ was the starting point for citations. CensorBib is an online archive of selected research papers in the field of Internet censorship, maintained by Dr. Philipp Winter [473]. The archive's focus is capturing papers that approach Internet censorship from a technical perspective, making it the ideal repository for this endeavor. CensorBib has archived papers from 1996 to present, from across a wide array of journals and conferences. Most of the entries on CensorBib are included in this study. Next, four top cybersecurity venues were surveyed: IEEE Security & Privacy, USENIX Security Symposium, ACM Computer and Communications Security, and Network and Distributed System Security (NDSS) Symposium. All are distinguished venues for high-quality, technology-focused research and helped to fill any gaps in CensorBib's methodology for inclusion. Three additional venues were surveyed for their particular relevance to the field of Internet censorship, namely the proceedings of the Privacy Enhancing Technologies Symposium (PETS), the proceedings of the Workshop on Free and Open Communications on the Internet (FOCI), and the proceedings of the Internet Measurement Conference (IMC) sponsored by ACM. Scholarly papers were initially screened by title and abstract for relevance. Once selected, papers were read to identify which censorship methods were discovered or revisited. Methods were noted, and a running list of technique keywords was updated. Citations within the references or bibliography section of identified papers were also acquired and noted if applicable.

After all of the research publications were reviewed, the initial elements of the taxonomy were constructed. Internet censorship happens on computing systems; using an existing conceptual model that abstractly describes computing system interconnection assisted in ensuring the

⁵ Available at <https://censorbib.nymity.ch/>

comprehensiveness of the taxonomy. The Open Systems Interconnection model (OSI model) helped place the censorship methods at each of its seven layers. OSI is also well-known in the information technology industry, and ensures ease of understanding for readers. Each censorship method was grouped and abstracted based on the author's experience and faculty review from senior researchers.

The second round of data collection filled gaps and provided additional supporting sources to the taxonomy elements. In the second round, keywords derived from the first round were searched in Google Scholar, the author's institution's digital library of journal subscriptions, and two search engines (Google and DuckDuckGo). This allowed for coverage of scholarly sources not included in CensorBib or the pre-selected venues, as well as government reports and blog postings not available in research publications.

4.4 Internet Censorship Methods

4.4.1 HTTP/URL Filtering

Uniform Resource Locators (URLs) were one of the early and common targets for filtering Internet content. URLs are defined in RFC 1738 [281] and consist of a protocol, 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, to define all sites that should be restricted upfront. An administrator can also use URL regular expressions (regex) to filter based on sets of characters or objectionable words.

URL filtering is done for a variety of reasons. Some companies seek to limit the kinds of websites employees can access while working. Adult materials may be deemed inappropriate for a workplace setting, social networking sites may be perceived as a distraction from productivity, or the company may limit access to pre-defined resources and deny all others. This practice is also often done in the name of security if the company subscribes to cyber threat intelligence (CTI) [118] feeds that provide blocklists of domains (or other indicators of compromise) associated with malware. Public Internet resources, such as libraries and Internet cafes, may limit

the websites patrons can visit to comply with the laws of their jurisdiction [132,153,169,172,173]. Depending on the country and situation, filtering online content may not be considered censorship. However, from a technical perspective, the software and tactics for filtering content are generally the same. Sambaluk noted, "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" [382]. This applies not only to privacy-preserving communication applications but also to cybersecurity controls that filter content. Controversially, multiple commercial products originating from the United States for the purposes of commercial Internet filtering have been observed in use in nation-state censorship. Historically, 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 [100,101]. These are a few examples of corporate products repurposed for censorship. Researchers may also encounter difficulties investigating countries that design their own filtering software without recognizable signatures.

URL filtering can be performed locally on a device or as traffic traverses a network. In the context of nation-state censorship, client-side local filtering is rarely done in practice, as managing configurations across numerous platforms (and gaining access to users' devices) is difficult. In contrast, network-based filtering is commonplace. Generally, a proxy, firewall, or middlebox is implemented upstream from a client device and performs filtering on the traffic of many clients.

URL filtering typically relies on the ability of the censor to examine the destination URL and match it against their list of blocked content to determine if the packet can continue. The URL exists at the application layer of an HTTP GET or POST request. As of October 2021, Firefox Telemetry reports that 82% of all web traffic observed from the Firefox web browser worldwide was encrypted using Transport Layer Security (TLS) [263]. Results for Japan and the United States were even higher, at 86% and 92%, respectively. In October 2017, Google published a transparency report with an analysis of the top 100 popular (non-Google) web pages globally, finding that all 100 had a modern TLS configuration to allow the use of HTTPS, and 95 of the

100 sites directed users to HTTPS by default without user interaction [183]. This change improves the security and privacy of all Internet users and presents significant challenges to censors. TLS encrypts the contents of HTTP packets, defeating basic URL filtering mechanisms.

In contrast, many web pages in Africa, Latin America, and southwest Asia are disproportionately served as unencrypted HTTP. The ease with which these connections can be manipulated or denied is a problem for Internet freedom advocates. Movements such as the "HTTPS Everywhere" campaign encouraged users to upgrade their web connections to use TLS by default, and major browsers (Google Chrome, Microsoft Edge, Mozilla Firefox, and Apple Safari) now have built-in functionality to upgrade connections where available [194]. In 2018, Troy Hunt launched a website to perform analysis specifically on global web pages that do not perform TLS redirection by default and offers resources to server administrators to help them implement HTTPS at low or no cost [214]. Notably, projects such as Let's Encrypt, a non-profit certificate authority, provide X.509 certificates at no cost and regardless of which registrar a domain name is maintained by [216]. Let's Encrypt was founded by the Internet Security Research Group and is credited with the mass proliferation of TLS usage over the past five years.

More advanced URL filtering approaches have been observed as well. A way censors deal with HTTPS requests is by observing and pattern matching against fields on the TLS certificate being passed to the client. These will be plaintext, and fields such as subjectAltName (SAN) or Common Name (CN) will sometimes contain portions of the URL or domain name [343]. This method of blocking is prone to error, however. Certificate authorities differ in implementation as to what certificate fields contain, and shared domains could lead to over-blocking.

Aside from TLS, users in censored countries or filtered corporate environments have also used proxies to evade content filtering. Prior research has shown that a least tens of thousands of open HTTP/SOCKS proxies are available on the Internet for any user to connect to [373]. Rather than connecting to the censor's proxy, many web browsers and Internet applications allow for manual entry of a proxy server. As long as the user can initiate a connection to a proxy outside of the censor's influence, they may be able to bypass URL filtering. Users sometimes chain multiple proxies together to further obfuscate the source and destination of their traffic. However, these

circumvention techniques can be easily thwarted if the censor requires all connections to be negotiated through the censor’s proxy servers to access external Internet resources.

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 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 geographically close to users and reduce latency [185]. It should be noted that 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. See §4.4.4 for further discussion of DPI censorship.

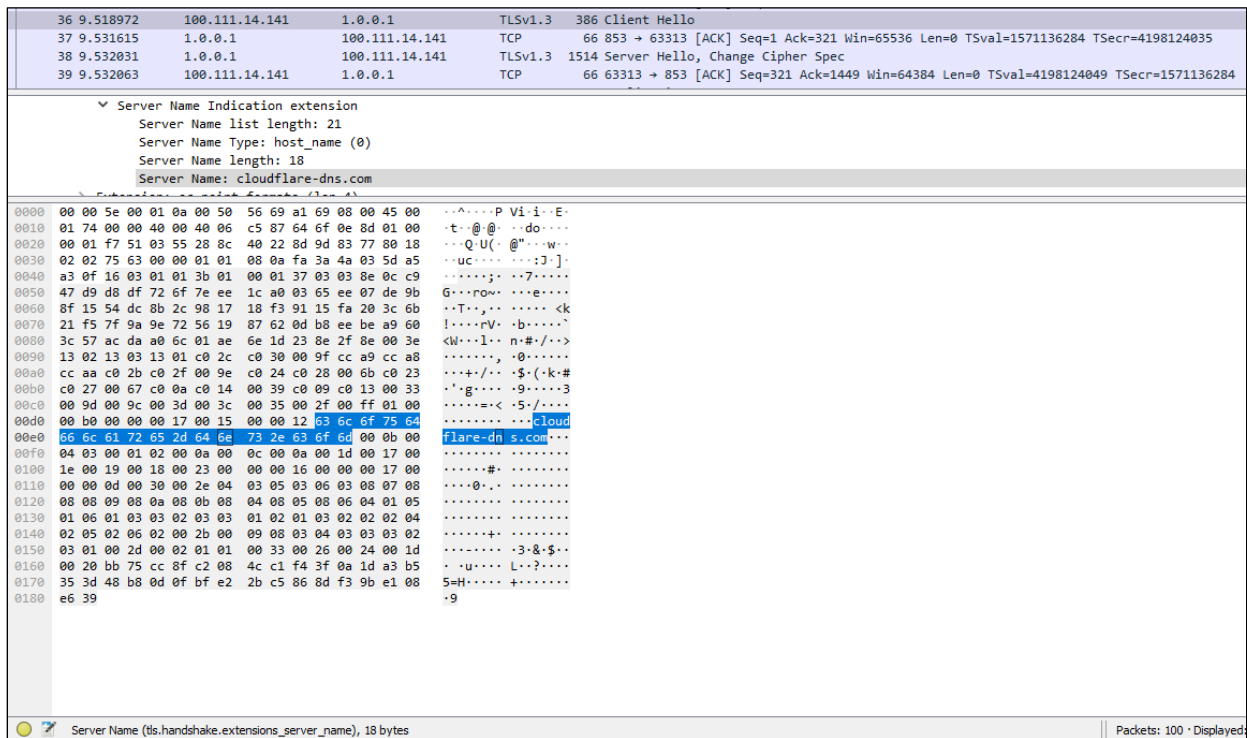


Figure 16. Example plaintext SNI for cloudflare-dns.com
Domain name shown in SNI extension within packet capture of TLS connection

Several attempts have been made to increase the privacy of TLS. For example, in the fall of 2018, Cloudflare proposed an extension to TLS called 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 resource [178]. The approach caught the attention of some censors, as researchers revealed that the People's Republic of China had begun blocking all TLS 1.3 connections utilizing ESNI crossing the great firewall [50]. 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) [220]. ECH would enable clients to encrypt the entire ClientHello of a TLS handshake (not only SNI), thus concealing the destination from an eavesdropping adversary. Until ECH is ratified by the Internet Engineering Task Force (IETF) and subsequently adopted by web servers around the world, censors will still be able to use SNI destinations for censorship and allow for mass surveillance of web browsing activities.

4.4.2 DNS Detection, Manipulation, and Denial

Another method widely used by censors is tampering with 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 [248]. Siby et al. have stated that "...virtually every connection to an Internet service is preceded by a DNS lookup" [401].

Some aspects of the original design of DNS have led to security and privacy problems for Internet users. The client may receive a DNS server address via DHCP or DHCPv6, as is often the case in operating system configurations. DNS servers may also be manually configured. The client submits the request, and a DNS resolver server checks its cache. If it has the IP address of the destination, it returns the address. If not, it makes the request to a DNS resolver upstream, and the process repeats until the answer is found or an error occurs. By default, most DNS requests are transmitted unencrypted. Several of these elements open avenues for censors to surveil or block websites their users attempt to visit.

Unencrypted DNS requests pose several security and privacy considerations. Internet Service Providers (ISPs) can easily surveil users' Internet activity based on DNS. ISPs often provide DNS servers for customers to use and can monitor all requests. Even in cases with manually configured external DNS servers, ISPs can "hijack" unencrypted DNS requests and return an IP address of their choosing to the client (see Figure 17). Suppose the censor is only concerned with the monitoring of 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 DNS requests observed are unencrypted), the censor has many options available. Requests that match objectionable 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 [268]. 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 [233,451]. See Figure 18 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.

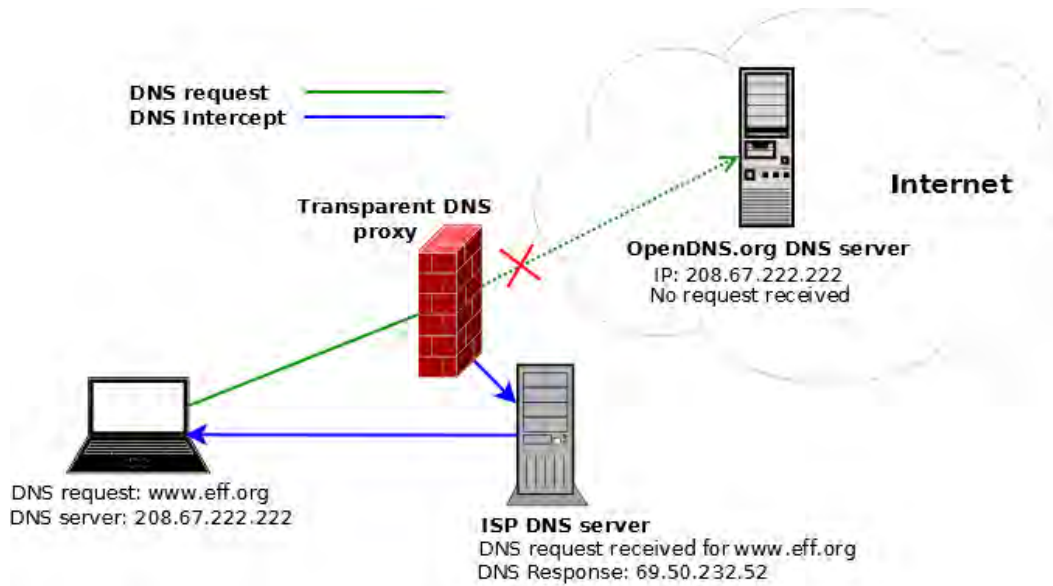
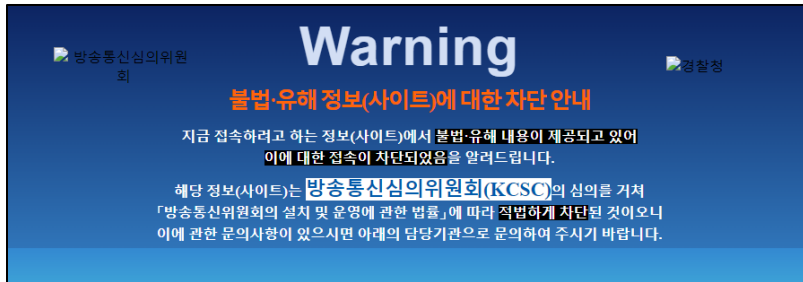


Figure 17. Transparent DNS proxy illustrated [513]

One countermeasure for DNS tampering is to manually define the DNS server for a device to use for domain resolution. Naive censors that only filter requests they receive will be bypassed, and the user will be able to resolve an IP address for their website successfully. As illustrated above, state censors and corporate filtering have grown in sophistication — manually defined DNS servers are often not enough to avoid censorship. Even low-resource censors can easily block all DNS traffic, with one firewall exception for their resolver, and defeat this countermeasure.



Warning

불법·유해 정보(사이트)에 대한 차단 안내

지금 접속하려고 하는 정보(사이트)에서 **불법·유해 내용이 제공되고 있어 이에 대한 접속이 차단되었습니다.**

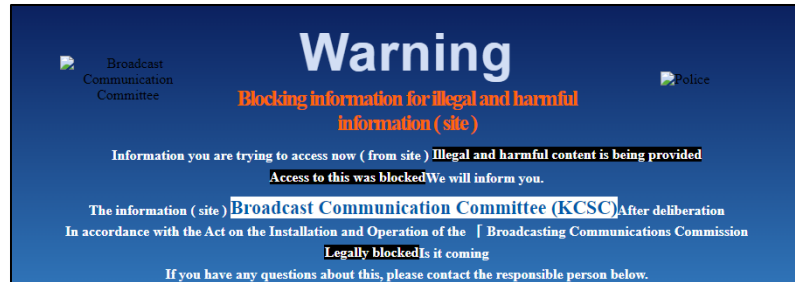
해당 정보(사이트)는 **방송통신심의위원회(KCSC)**의 심의를 거쳐 「방송통신위원회의 설치 및 운영에 관한 법률」에 따라 **적법하게 차단된 것이오니 이에 관한 문의사항이 있으시면 아래의 담당기관으로 문의하여 주시기 바랍니다.**

※ 차단안내페이지(warning.or.kr)를 도용한 피명사이트가 발견되어 각별한 주의가 필요합니다.
(차단안내페이지는 개인정보를 요구하거나 프로그램 설치를 유도하지 않습니다.)

사이트분야	담당기관	전화번호
불법 도박	사이버 경찰청	1566-0112
	사행산업통합감독위원회	1855-0112
불법 체육진흥투표권 판매	사행산업통합감독위원회	1855-0112
	국민체육진흥공단 클린스포츠 통합콜센터	1899-1119
불법 승차권표 구매대행	국민체육진흥공단 경륜·경정 종합본부	1899-0707
불법 마권 구매대행	한국마사회	080-8282-112
불법 의약품 판매	식품의약품안전처 사이버조사단	(043)719-1921
불법 의약품 판매 및 허위과대광고	식품의약품안전처 사이버조사단	(043)719-1921
불법 식품 판매 및 허위과대광고	식품의약품안전처 사이버조사단	(043)719-1914
불법 건강기능식품 판매 및 허위과대광고	식품의약품안전처 사이버조사단	(043)719-1914
불법 화장품 판매 및 허위과대광고	식품의약품안전처 사이버조사단	(043)719-1906
불법 의료기기 판매	식품의약품안전처 사이버조사단	(043)719-1906
불법 마약류 매매	식품의약품안전처 마약정책과	(043)719-2806
성매매 및 음란	방송통신심의위원회	(02)3219-5844
상표권(위조상품 유통)	한국지식재산보호원	(02)2183-5825
저작권(불법복제물 유통)	한국저작권보호원 온라인보호부	(02)3153-2464
안보위해행위	사이버 경찰청	1566-0112
명예훼손, 조상권 침해	방송통신심의위원회	(02)3219-5341-4
잔혹, 혐오, 차별 비하 등	방송통신심의위원회	(02)3219-5161
디지털성범죄정보	방송통신심의위원회	(02)3219-5834

◎ 운영자 이의신청 안내

사이트 운영자는 시정요구를 받은 날로부터 15일 이내에 방송통신심의위원회에 이의신청 할 수 있고, 「행정심판법」, 「행정소송법」 등 관련 법규에 따라 행정심판 및 행정소송을 제기할 수 있습니다.
차단사유 및 이의신청 관련 문의사항이 있으시면 정보내용에 따라 아래의 전화번호로 문의하여 주시기 바랍니다.



Warning

Blocking information for illegal and harmful information (site)

Information you are trying to access now (from site) **Illegal and harmful content is being provided. Access to this was blocked. We will inform you.**

The information (site) **Broadcast Communication Committee (KCSC)**. After deliberation in accordance with the Act on the Installation and Operation of the [Broadcasting Communications Commission **Legally blocked** Is it coming

If you have any questions about this, please contact the responsible person below.

※ A mammingite that steals the intragment page (warning.or.kr) is found and requires special attention.
(The blocking guide does not require personal information or induce the installation of programs.)

Site	Officer	Phone number
Illegal gambling	Cyber Police Agency	1566-0112
	Executive Committee	1855-0112
Sale of illegal physical education campaigns	Executive Committee	1855-0112
	National Gymnast Clinsport integrated call center	1899-1119
Purchasing illegal winners	National Assembly Agency, Gyeongcheong, Gyeongjeong, General Headquarters	1899-0707
Illegal ticket purchase	Korean Board of Directors	080-8282-112
Illegal drug sales	Cyber investigation of food and drug sources	(043)719-1921
Sales of illegal medicinal products and false and high advertising	Cyber investigation of food and drug sources	(043)719-1921
Illegal food sales and false and high advertising	Cyber investigation of food and drug sources	(043)719-1914
Illegal health functional food sales and false and high advertising	Cyber investigation of food and drug sources	(043)719-1914
Illegal cosmetic sales and false and high gloss	Cyber investigation of food and drug sources	(043)719-1906
Sale of illegal medical devices	Cyber investigation of food and drug sources	(043)719-1906
Illegal drug trafficking	Food and Drug Administration Drug Policy Division	(043)719-2806
Prostitution and pornography	Broadcast Communication Committee	(02)3219-5844
Trademark (Distribution of counterfeit goods)	Korea Ii-gyeong Jae-san-san-Kan	(02)2183-5825
Copyright (Distribution of illegal drugs)	Korea Copyright Protection Agency Online	(02)3153-2464
Security	Cyber Police Agency	1566-0112
Honorary Yahweh Son, Portrait Violation	Broadcast Communication Committee	(02)3219-5341-4
Cruelty, hate, discrimination, etc.	Broadcast Communication Committee	(02)3219-5161
Digital crime	Broadcast Communication Committee	(02)3219-5834

◎ Operator Appeal Guide

Site operator You can appeal to the Committee of the Communication and Communication within 15 days from the date you receive the request.
Administrative and administrative submissions may be filed in accordance with applicable laws and regulations, such as [Administrative Judgment Act] , [Administrative Law] .
If you have any questions regarding the blocking company and the appeal, please contact us at the phone number below for information.

Figure 18. Example blockpage from the Republic of Korea

(Left) Original 한국, (Right) English translation. Available at: <http://warning.or.kr/> (Retrieved November 01, 2022)

Another countermeasure for 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 also rapidly increased in popularity for circumvention of censorship and geographic area filtering [244,361]. Despite their initial purpose of providing an encrypted connection between two separate networks across the Internet, commercial providers are increasingly offering paid services to route traffic through their infrastructure. Several censors have taken notice. Notably, the People's Republic of China (PRC) banned non-state-sanctioned VPNs in 2018 [368], and the Russian Federation banned the use of several VPN services in 2021 [430]. VPN connections encrypt traffic between two endpoints, allowing users to tunnel their traffic — selective traffic such as DNS or all IP packets — outside a censor's sphere of influence. Although VPN users may be able to connect to content they otherwise could not access, they are shifting the trust of their data and traffic from their ISP to the VPN provider.

Efforts are ongoing 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. It digitally signs DNS records and relies on a chain of trust similar to how certificate authorities are trusted entities in TLS. 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. As of 2013, researchers identified that only 0.15% of .com top-level domains utilized DNSSEC [264]. Rijswijk-Deij et al. demonstrated how sites that use DNSSEC might also be susceptible to packet fragmentation or amplification-based DoS attacks on their DNS traffic [369]. Domain administrators should weigh the potential cost, complexity addition, and potential downtime when deciding whether to implement security extensions.

Encryption of DNS can address some of the privacy and authenticity problems of the original protocol. Many public DNS services now offer DNS over TLS (DoT) and DNS over HTTPS (DoH). Both have been used as countermeasures to DNS tampering. DoT and DoH work by

encrypting DNS requests in transit and bypassing DNS resolvers provided by service provider gateways [401]. Several major web browsers support DoH natively. However, there are several 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 proliferation 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 [40]. When used in isolation, DoT and DoH do not fully address Internet privacy concerns, as censors can target many other vulnerable aspects of a web request aside from the IP address to domain name translation. However, DoT/DoH may be helpful if a nation-state only implements its censorship regime via domain name blocklisting. Encrypted DNS is one potential element anti-censorship software developers may consider.

4.4.3 IP Address and Port Matching, Blocking

Another common form of Internet censorship is blocking based on Internet Protocol (IP) addresses. Censors can maintain large blocklists of IP addresses associated with objectionable endpoints. Censor systems continually monitor traffic and drop it when a blocked address is observed inbound or egress from 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 the blocklists may grow large and quickly become outdated as a result of the ephemeral nature of IP addresses [484]. With the continued growth in the adoption of IPv6, these resource constraints will only continue to accelerate. Despite these constraints, some nation-states choose to censor Internet traffic utilizing IP blocklists — likely because of ease of implementation.

IP address spoofing could serve as a naive 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 source address field on packets [42]. If a censor implements blocking based on source IP address, spoofing the address of a known allowed endpoint may allow traffic that would otherwise be denied. However, source blocking is seldom done in

practice for large-scale censorship; censors often focus on the content they wish to deny access to 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 done indiscriminately across all traffic. Many applications openly advertise their software's ports and transport protocols, and censors may wish to deny access to specific applications — such as when the Burmese government blocked access to Skype in 2011 [291]. A more advanced blocking regime in Iran involving port blocking was revealed in 2020 by the Open Observatory of Network Interference (OONI) and Bock et al. Four Iranian ISPs were shown to have blocked port 853, commonly associated with DNS over TLS, to dozens of popular DNS providers [39] (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 [32] before abandoning the effort the same year. In 2020 Bock et al. demonstrated that Iran had re-implemented 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 [53]. Traditional port blocking is a naive approach relying on software to follow common conventions. These methods are effective against applications that explicitly follow RFC specifications or their own documentation. However, transport layer protocols can easily use non-standard port mappings, and many applications have been shown to do so. Most nation-state 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 recent study [52] 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 renewed, time-based approach to IP and port blocking in China, Iran, and Kazakhstan. Further research is needed to determine if other nation-states are implementing similar functionality into their censorship systems.

Using high ephemeral ports is a simple yet easily detectable countermeasure against censorship. By altering the listening port of a web application or service, naive censors that only filter based on static port numbers may be bypassed. Censors that block/reject all traffic except for particular common ports and those that utilize allowlisting are not bypassed using this technique.

Complexity on the modern 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), intended to provide access to web resources as close to the user as possible to reduce latency [185]. Censors have been shown to cause widespread collateral damage in overblocking by denying access to the IP address space of large CDNs [289]. A particularly salient example of inadvertent censorship is the blocking of Google Scholar in the PRC. Despite the service being considered a valid academic resource and legal service by CCP governmental regulators, the great firewall filters traffic destined for US-based google.com regardless [269]. Legal frameworks and technical implementations change over time and often come into 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 — 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 methods.

4.4.4 Deep Packet Inspection and Protocol Fingerprinting

In response to the success of various early circumvention tactics, some censors sought more advanced capabilities to detect undesirable Internet traffic. As the name suggests, Deep Packet Inspection (DPI) allows for searching payload content in data packets [400]. 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. DPI is frequently used in cybersecurity contexts by system administrators. DPI-enabled network devices can "be programmed to detect certain bit sequences associated with known malicious

code" [186] 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.

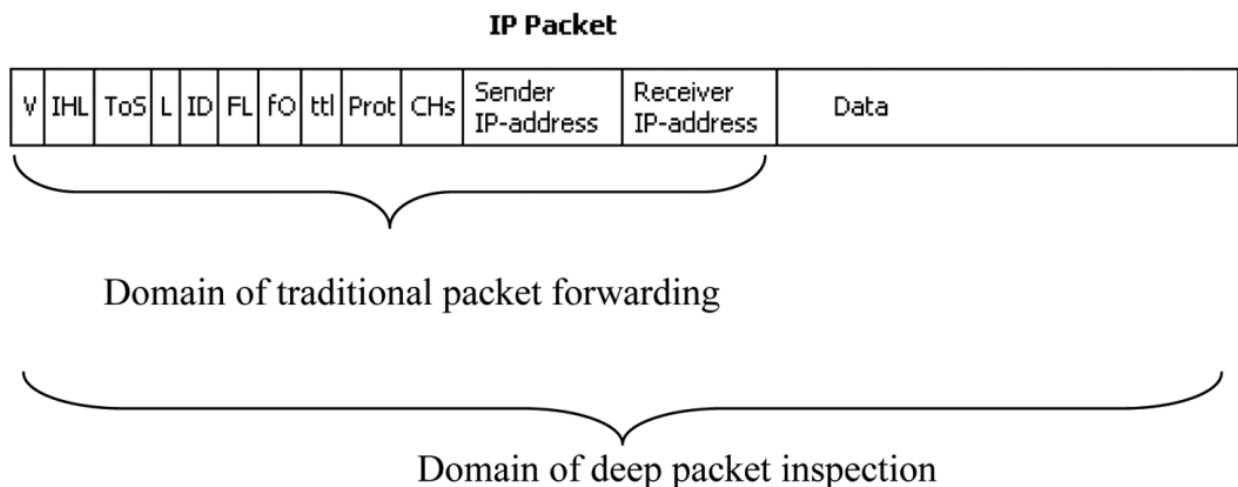


Figure 19. DPI Diagram from Bendrath and Mueller [41]

In the context of censorship, DPI allows for content matching, such as with keywords of objectionable materials. While still a relevant point of discussion for Internet censorship, the large-scale proliferation of encryption across many Internet resources [263] has rendered simple content matching obsolete in many protocol exchange scenarios online. Additionally, many anti-censorship solutions implement encryption at multiple layers to protect traffic confidentiality and thwart simple content filtering.

DPI is often considered extremely expensive in terms of computing costs and challenging to implement on high-speed network systems [446]. But the potential for abuse of heuristic or machine learning-informed DPI of encrypted traffic remains. Open-source DPI tools are increasing in sophistication and accuracy. The open project ntop maintains a software fork of OpenDPI named nDPI, which maintains the flow signatures of hundreds of protocols and applications [514]. At the same time, commercial next-generation firewalls (Palo Alto, Fortinet FortiGate, and Forcepoint are examples) already claim to be able to filter data from custom

applications on a network [151,152]. Palo Alto has a blog post guide for their customers on all the steps to block Tor using their product [344]. The most aggressive nation-state censors have demonstrated an increased willingness to implement DPI for censorship in recent years, discussed in detail in Chapter 5.

Some anti-censorship software developers and researchers have implemented countermeasures against deep packet inspection. One approach is to randomize the payload entirely to make the traffic "look like nothing" [111]. This is the approach taken by "obfs" tools such as Dust [471] and ScrambleSuit [476]. 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 with 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 [469] for HTTP, SkypeMorph [301] for Skype, and CensorSpoofer [461] for SIP-based Voice over IP. This approach has been criticized by Houmansadr as "fundamentally flawed," as any slight variation not imitated by the spoofing software can allow a determined censor to detect the anomaly and win by blocking the traffic [207]. Balboa works as a middleware and attempts to overcome the shortfalls of mimicry approaches by using standard outputs of existing software and injecting traffic into allowed TLS streams [377]. Newer approaches, such as format transformation encryption (FTE), claim that observation-based FTE steganography can be used as an undetectable covert channel [322]. In all, pluggable transports have become an important tool for allowing the bootstrapping of anti-censorship tool connections. Projects other than Tor have also begun to code compatibility for pluggable transports into their software [515].

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 actively target Tor bridges [475], as well as SSH [318] and VPN endpoints [319]. 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 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 [166,168]. Currently, Tor Browser uses obfs4 as its default pluggable transport for bridges. Previous versions of obfs were vulnerable to active probing by the GFW of China. In its current implementation, every obfs4 server has a per-bridge secret. The client must prove knowledge of this secret before allowing communication with the protocol, and this defeats automated methods of active probing, as the censor would need the same out-of-band information as each legitimate client to prove the IP address of a server is, in fact, a hidden Tor bridge [142]. Another pluggable transport approach, such as Meek, uses a routing method known as domain fronting [141] to direct first-hop traffic under cover of HTTPS to a large CDN provider domain that is unlikely to be filtered. Psiphon and Tor both have Meek implementations shipped with their software.

Additionally, some newer anti-censorship tools have been introduced, leveraging techniques to bypass less-aggressive censors that only use DPI blocking (and no other combinations of network filtering). Software such as GoodbyeDPI [182] and a related fork called PowerTunnel [353] 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. These techniques must be used cautiously, only in censored jurisdictions where legal or physical threats are absent, as these tools do not provide protections similar to other anti-censorship approaches (such as masking source IP addresses).

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, sometimes called encrypted traffic analysis (ETA). 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 the initial unencrypted initiation of an encrypted network stream, as illustrated by Velan et al. in Figure 20. Protocol header metadata can often reveal the kinds of encryption implemented or software application versions. A comparison of the available DPI systems that perform this analysis is available at [61].

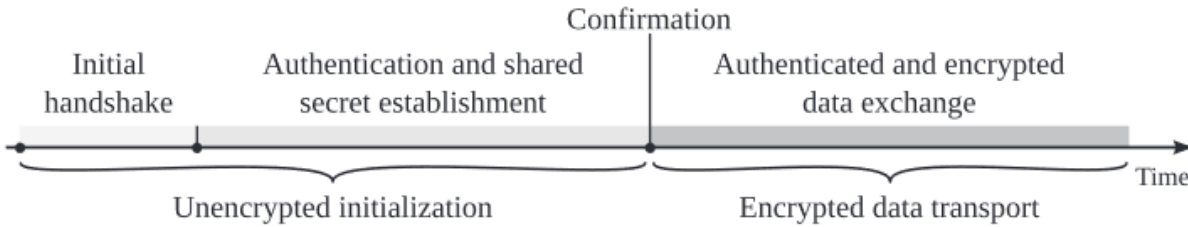


Figure 20. A general scheme of network security protocols [449]

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 [449].

One example of pattern or behavioral-based blocking is the denial of a secure messaging app such as Signal [234]. Blocking of Signal has been observed in Iran, China, Cuba, and Uzbekistan [494]. Admittedly, these nations used more common blocking 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 further in §4.4.6.

4.4.5 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 between devices worldwide. At the highest levels, the Internet Assigned Numbers Authority (IANA) assigns blocks of IP addresses to regional Internet registries (RIRs). RIRs designate 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 [192]. There are approximately 64,000 ASNs in use worldwide with continual growth [88], and BGP (versions 4 and 6) are the protocols that allow them to communicate with one another. "DNS tells you where you're going, and BGP tells you how to get there" [84]. While BGP is intended to provide the most efficient routing options available between ASes, there are many associated factors beyond simply 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 medium complicate routing decisions.

In addition to routing complexity, design choices made when creating BGP have security and availability implications for the global Internet. The protocol assumes that advertisements from interconnected networks always tell the truth about which IP addresses they own. "BGP hijacking" attacks are nearly impossible to prevent today [89]. One likely avenue an attacker might take is advertising a specific route for a smaller range of IP addresses than other ASes had previously announced. Another attack involves offering a shorter route to particular blocks of IP addresses. Both would allow the attacker to divert large swaths of Internet traffic in a direction of their choosing. For an attacker to carry out a BGP hijack, they must be an AS administrator or a malicious actor taking control of an AS system. This limits the scope of who might perform such

attacks, but does not rule out censoring nation-states or large technology corporations from using these methods to deny access to information.

There have been several BGP-related incidents over the years. In 2004, a Turkish ISP named TTNNet (AS9121) inadvertently modified its routing tables to include a full table of entries (>100k). This modification effectively advertised AS9121 as the shortest route to most of the Internet's addresses [436]. 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 across the country. This error resulted in most Australians losing online connectivity for 30 minutes. 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 worth of routes to Canadian ISP Bell [43]. More recently, in 2021, Facebook (now Meta) incurred a global outage partially caused by BGP route errors. During routine maintenance, an engineer disconnected Facebook's backbone data centers with an accidental command. 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 [223]. The company restored services within six to seven hours but at enormous business and advertising costs.

Malicious BGP-related attacks have also occurred. In 2008, Pakistan Telecom (AS17557) allegedly started an unauthorized BGP announcement of the prefix 208.65.153.0/24 to attempt to censor YouTube from its citizens [371]. This effort temporarily hijacked all YouTube traffic on a global scale, denying access to all users for part of the day on February 24, 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 [99]. 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 [352]. Criminals masqueraded a fake version of a web-

based Ethereum wallet service⁶ and stole approximately \$152,000 worth of cryptocurrency. In 2022, a sophisticated supply chain attack on a Korean cryptocurrency exchange platform (which involved BGP hijacking perpetrated by AS9457) also resulted in the theft of approximately \$1.9 million (₩2.37 trillion KRW) [80]. On February 5, 2021, after the Burmese military overthrew the government of Myanmar in a coup d'etat, 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 [342].

The threat of abuse with BGP manipulation has motivated proposals for security enhancements in academic circles [300]. However, for most governments, BGP attacks have not been used in practice as an intentional technique for routine censorship, instead relying on other methods with less collateral damage. Additionally, software developers of anti-censorship tools are unlikely to influence the routing, implementation, or prioritization of ASes that their traffic traverses. 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.

4.4.6 Bandwidth Throttling

Bandwidth throttling involves deliberate slowing of communication speed. In the context of computer networks, throttling can happen at the application software or the network management level. 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 [235]. However, throttling often arises in public debate surrounding "net neutrality," a network design principle that states all data packets should be treated equally regardless of their content, sites, and platforms [483]. Network neutrality is a contentious topic. It has been interpreted and implemented differently and has been subjected to legal challenges in multiple countries.

⁶ <https://www.myetherwallet.com/>

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 a degree of deniability on behalf of the censor, differentiating it from many other Internet censorship methods. In Iran, the government slowed down Internet speeds nationwide in the lead-up to a presidential election in 2009 [23] and 2013 [129], as well as other periods of political unrest [70]. In recent years, the Russian Federation has deployed an unprecedented censorship technique by leveraging selective throttling [489]. 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 up to that point, 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 [378]. Xue et al. discovered that Russian ASes used deep packet inspection to detect SNI within TLS connections specifically for Twitter and its sub-domains (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 [489].

Taye described several techniques that governments use to throttle Internet connectivity [304]. First, traditional bandwidth management, such as traffic shaping and policing, can slow down 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) on 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 add latency artificially. 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. No purpose-built tools exist as a countermeasure for this kind of censorship method. Anecdotes online suggest that commercial virtual private networks (VPNs) may bypass ISP throttling, depending on how the throttling is implemented [147]. 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 [489]. More research and development are needed in this emerging area of censorship studies.

4.4.7 Internet Shutdowns

Even as societies around the globe increasingly rely on Internet connectivity for economic, financial, and social functions, some governments have stepped up 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" [135]. 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 incidences 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." [136]. Shutdowns may be implemented for minutes, hours, weeks, or several months at a time. 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, "The right to access and use Internet and other digital technologies for the purposes of peaceful assembly is protected under article 20 of the Universal Declaration of Human Rights and article 21 of the International Covenant on Civil and Political Rights" [210,211]. Protection of freedom of expression and association are often cited as obligations within international human rights law. A plurality of nations across ideological and governmental institutions agree,

but perhaps not always in practice. Internet shutdowns often lead to unintended consequences for Internet censors and society at large. From an economic perspective alone, researchers estimated \$5.62 billion dollars of financial impact on the global economy in 2021 as a result of Internet shutdowns [480].

One of the most cited incidents of Internet shutdown efforts in the literature took place from December 2010 to 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 across Tunisia, Egypt, Libya, Yemen, Syria, and Bahrain. The overthrow of several heads of state and some governmental reform occurred as a result. Demonstrations took place in the streets of Algeria, Iraq, Lebanon, Jordan, Kuwait, Morocco, Oman, and Sudan, while minor protests also happened in Djibouti, Mauritania, Palestine, and Saudi Arabia [379]. Citizens (often youth or union groups) protested in response to political leader corruption, governmental abuse of power, economic stagnation, extreme poverty, and unemployment. Power vacuums in the Arab world in the mid-2010s led to the rise of the Islamic State caliphate group [13], the Syrian Civil War [397], the crisis in Egypt, the Libyan Civil War, and the Yemeni Civil War [329]. 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 the Arab Spring protests and circumventing the traditional media and means of communication typically controlled by censoring states [11,482]. According to some academic works, the impact of Facebook and Twitter during the uprisings has been overstated by popular media [60]. Regardless, several regimes deemed Internet connectivity important enough to the protestors' cause to selectively deny online access to prevent communication or the spread of information [479].

In 2013, Shavitt and Zilberman published an analysis of Internet shutdowns during the Arab Spring, specifically in Egypt, Libya, and Syria [398]. 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. Efforts to logically deny all access to Internet endpoints were relatively straightforward, especially in a small nation such as Syria, which only had one government-

controlled autonomous system [286]. The denial of Internet access may have hampered some protestor mobilization efforts while simultaneously fueling the discontent of the Arab youth by controlling their access to Internet content.

Internet shutdowns have taken place in many countries worldwide since the Arab Spring events. Censoring nation-states have diverse geo-political and social systems and widely varying legal systems. Yet controlling access to information is central to the conflicts, and Internet censorship is increasingly essential to shaping narratives. India, the largest self-proclaimed democracy, had 132 regional Internet shutdowns in 2020 [406]. Politicians in India use shutdowns as a tool of governance under the auspices of countering misinformation and disinformation (sometimes termed "fake news" for the public). These leaders cite national campaigns such as "Digital India," intended to use connectivity to promote prosperity and wealth accrual. Shah argued their efforts do not stop fake news. He stated, "...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" [395]. 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" [395].

In 2019, in response to large anti-government demonstrations against rising gasoline prices, Iranians experienced a several-day Internet blackout [315]. In November 2020, Myanmar held national elections in which the National League for Democracy Party candidate, Win Myint, won the presidency. The Tatmadaw (Burmese military forces) staged a coup d'etat on February 1st, 2021, rejecting the election outcome and installing a military junta in place of Myanmar's elected government [380]. 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 April 2, 2021 [224]. The junta ordered telecommunications companies to disconnect connectivity to mobile and wireless Internet customers, the only services available in the country to get online. Although Internet penetration rates in Myanmar were only 35% in 2020 [424], the censorship measures put in place are some

of the most draconian observed in this century and has spurred debate regarding free expression, freedom of assembly, and free access to information [439].

Researchers have noted a trend that despite the surge in Internet shutdown events in the past five years, many governments have opted to selectively block (or throttle) individual content or platforms [136]. Rather than total shutdowns, authorities have attempted to avoid more potent political backlash from their citizenry 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 and persistent Internet censorship are important trends 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 should remain adaptive in their approaches to circumvent censorship where it occurs.

4.4.8 Computer Network Attacks and Resource Exhaustion

The study of computer network attacks (CNA) and exploitation has been the subject of much 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 [445] their targets' computing systems in pursuit of their objectives. In terms of the world wide web and private sector actors, much of the focus of network attacks manifest as denial of service (DoS) and distributed denial of service (DDoS) attacks. Both are forms of resource exhaustion, denying access to services by overwhelming target servers.

DDoS attacks have captivated the cybersecurity literature over the past several decades [267,273,276,299,431,502], 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 accomplished by flooding the targeted host or network with traffic until the target cannot respond or crashes, preventing access for legitimate users" [81]. 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 belaying the attack more difficult. Participants in DDoS are often unwitting, as their devices may have been infected with malware that joined them into the attacker's botnet.

From a technical perspective, DDoS attacks can be categorized broadly into network-layer attacks 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 [20], or other allowed protocols. Application-layer attacks occur using data higher in the OSI model. Some attacks 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 [502] 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 in the network conversation when the victim replies. Amplification-based attacks rely on external services to help create additional traffic, "amplifying the message" [431]. They may exploit an IP broadcast feature of a network device or service to reduce the effort the attacker or botnet must put forth 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 [431] and a more general taxonomy of DDoS attacks and defense mitigations is available in [299].

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 how the attack techniques are 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 [502]. 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") [386] 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 [58,199]. In 2006, the Bureau of Industry and Security in the United States suffered "a debilitating attack on its computer systems," forcing the organization to disconnect its systems from the Internet and disrupting its operation. The attack was "traced to websites hosted by Chinese ISPs, but the attackers were never identified" [58].

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 [85]. The economic damage resulting from system downtime and societal disruption was estimated to cost tens of millions of Euros [465]. The campaign against Estonia has been cited as the second state-sponsored act of cyber warfare (the first being a series of coordinated cyber operations, dubbed Titan Rain, against the U.K. Defense Ministry and U.S. Defense Intelligence Agency (DIA) beginning in 2003 [95]).

In 2008, coinciding with a shooting war between Georgia and the Russian Federation, large-scale DDoS attacks began against Georgian web pages [425]. Targets included the Georgian president's website, governmental ministry pages, and news agencies. While the Russian

government may have benefitted from the disruption, evidence suggests that much of the attack resources were crowdsourced from underground hacker communities sympathetic to the Russian cause [425]. 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) [90]. The Mirai botnet targeted Dyn using compromised Internet of Things (IoT) devices to attack its victims. It denied Internet access to many users on the east coast of the United States on October 12, 2016.

In 2017, the U.S. government released a report documenting malicious cyber activity performed by the government of the Democratic People's Republic of Korea (DPRK, commonly known as North Korea). The report outlined the activities and capabilities of the Lazarus Group (also called 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 [442]. 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 [82]. Lazarus group was likely responsible for DDoS and offensive cyberspace operation campaigns against South Korean media, financial institutions, and critical infrastructure in 2011 and 2013 [504].

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 [294]. Cloudflare confirmed that the attack against Google was the largest known DDoS attack in history [90].

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

hactivist group Anonymous in 2011 [187]. 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 traffic related to censorship has often been shown to originate from Chinese ASes. On March 16, 2015, greatfire.org observed via their Amazon CloudFront hosting service that their website was under attack from a DDoS, and their hosting costs had risen to \$30,000 per day because of the added throughput [405]. 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 [279]. The same paper alleges a capability called QUANTUM, maintained by the U.S. National Security Agency (NSA) and U.K. GCHQ, similarly abuses plaintext HTTP traffic as a "man-on-the-side" attack. However, the tool is allegedly used for exploitation rather than DDoS.

Another example of politically motivated DDoS attacks happened in southeast Asia in recent years. On February 27, 2022, CNN Philippines journalists were preparing to cover a presidential candidate debate when their website went down because of a DDoS attack [175]. 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" [191]. 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 [19].

Definitive attribution of DDoS attackers is difficult, and it is unclear whether some attacks denying access to political commentary in the Philippines were conducted by a nation-state actor.

A paper from 2009 specifically analyzing DoS attacks with political motivations suggests that most DDoS attackers online are non-state actors [311], while a more recent study in 2020 evinced the notion that authoritarian states are increasingly willing to perform attacks on foreign entities during elections and changes of power [270]. However, the ease of access to attack resources coupled with difficult attribution often leaves nation-state, governmental proxy, and non-affiliated attacker involvement an open question.

4.4.9 Additional Censorship Considerations

The Internet censorship methods detailed 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 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 Figure 21 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 cases of 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 free expression norms [215]. Web services that host pirated content in violation of intellectual property laws of certain jurisdictions may also be targeted in a similar manner.



Figure 21. Example law enforcement domain seizure [444] (Retrieved October 2, 2022)

Determined state censors may also use substitution as a form of censorship. Redirection of web requests is commonly used to display a blockpage, warning the user of the reason they were denied access [105]; a censor could also use redirection to display a website that appears legitimate but contains false information [409]. While 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 [392,501]. These efforts may distract or discourage citizens from seeking out the information they wish to read, or reduce overall institutional trust among Internet users [324].

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 [208,107,506,1,249,35]. The Chinese government encourages Chinese companies to host alternative services to Western social media (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." Additionally, section 230 of the communications decency act is a federal law that protects online services from lawsuits based on user content [254]. 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 belief) 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 US: 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 non-compliance [387]. 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 any discussion of censorship. Humans often decide to withhold or selectively disclose their own discourse [94,206]. 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 reflect authorities in a negative light [415]. In extreme examples, citizens may feel compelled to feign positive attitudes toward ruling elites when there is little electoral competition for executive power [399].

A final consideration for potential Internet censorship is publisher denial of access. It is common practice for web servers to filter inbound 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 [434] 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 [246]. Some servers naively block all Tor exit nodes. Others use heuristic methods to detect abusive behavior and punish any user sharing the same exit node as a malicious actor [404]. 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 [361,244,120,45]. Finally, publisher-side filtering happens by 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 [434]; Figure 22 is one such example. The decision likely happened to avoid compliance with GDPR's privacy rules or out of an abundance of caution for liability. This kind of server blocking is not government censorship, but it is relevant to a holistic discussion of what it means to be able to access information freely in the modern, interconnected world.

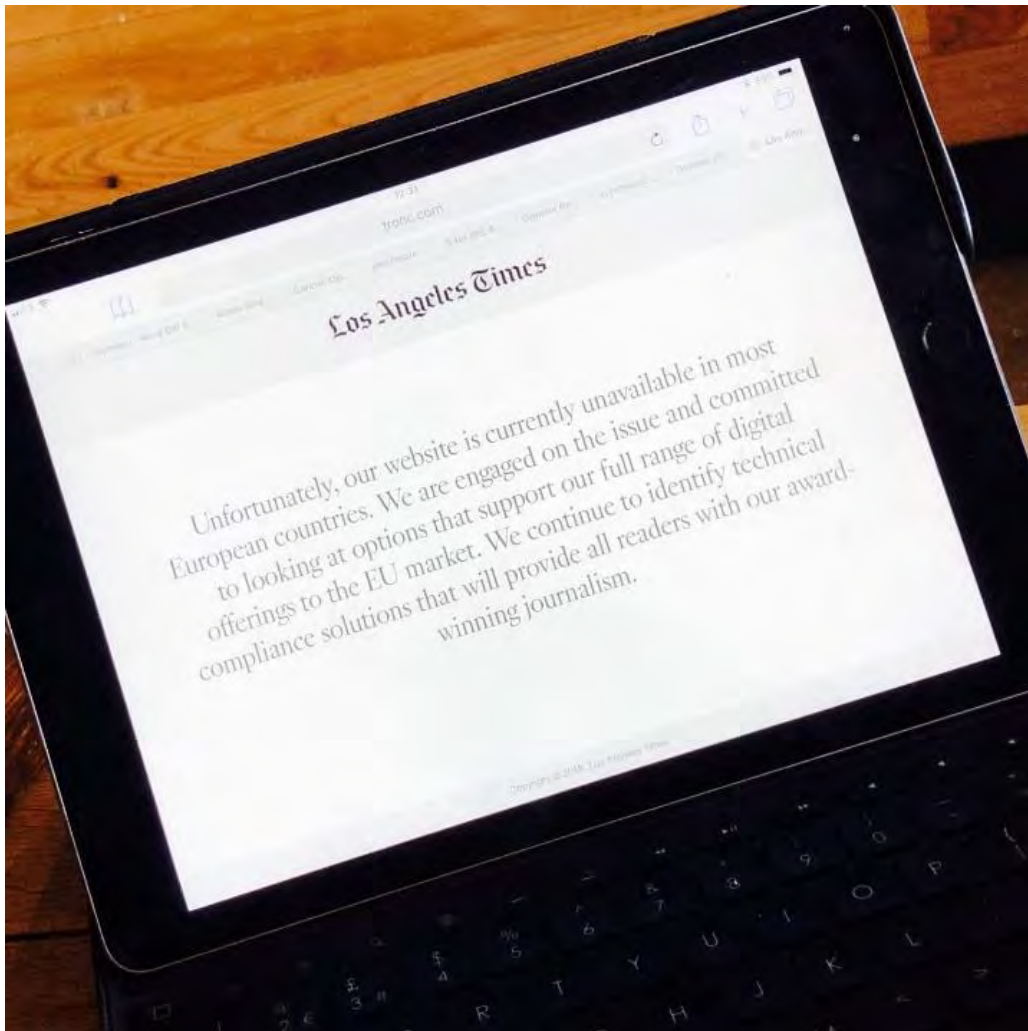


Figure 22. Website blocking a user with a European IP address after GDPR enacted [426] (May 25, 2018)

4.5 A Taxonomy of Internet Censorship Methods

The culmination of the systematization in this chapter resulted in the Internet Censorship Methods Taxonomy, shown in Table 2. The author organized the taxonomy within the framework of the OSI model for ease of organization, logical visualization, and to promote mutual understanding. A censorship method is an abstraction of similar techniques used by censors together. Examples of techniques that comprise a censorship method are listed but not exhaustive. Layers 1-4 represent methods that only require "shallow packet inspection" methods,

only require reading of packet headers, and are much less resource intensive. Deep packet inspection methods analyze the content of data packets, the payload beyond packet headers. Notably, bandwidth throttling bridges the gap and can occur network-wide or on an application-layer basis. Distributed denial of service attacks also happen at both network and application layers. Below DPI, the author depicts Traffic Behavior Analysis, which involves observing patterns (or anomalies) in bitstreams of traffic, including those protected by encryption. Encrypted traffic analysis (ETA) often leverages machine learning or statistical models to create profiles of traffic behavior for particular applications or protocols. In general, moving up the layers of OSI (down the taxonomy chart), censorship methods increase the complexity of circumvention analysis and censor implementation. Table 3 represents the bibliography of evidence of Internet censorship methods and techniques. The author sorts citations chronologically by method and delineates them by decade.

Table 2. Internet Censorship Methods Taxonomy

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

*No published examples of nation-state censorship use, as of 2021

Internet censorship occurs using a broad spectrum of methods and activities. Some nations have shown an increased willingness to use Internet shutdowns to achieve their goals. The effects of communication disconnection are overt and obvious to the user population. Other countries seek to minimize economic collateral damage from overblocking and use more targeted techniques to deny "objectionable" content. Some authorities wish to conceal the fact that they are censoring content and turn to techniques such as TCP-level reset packets or bandwidth throttling. In these cases, users may simply believe they are experiencing poor network service, increasing Internet measurement research's difficulty in detecting censor activity and changes over time. Additionally, as end-to-end encrypted (E2EE) messaging services gain popularity for their security and privacy properties, censoring nation-states have demonstrated an increased willingness to target these protocols with existing methods and more advanced protocol fingerprinting techniques. The proliferation of ETA tools or next-generation firewalls (NGFWs) that can block applications such as Signal or Tor Browser may represent a new threat to private communication methods.

Foundational improvements in Internet architecture can reduce censor abilities 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. The IETF has a draft RFC for an Encrypted ClientHello (ECH) to be implemented into the TLS standard [366]. If ratified and implemented in web servers across the Internet, ECH may eliminate an entire class of censor method. When Cloudflare attempted to deploy its own encrypted SNI (ESNI), China blocked all TLS 1.3 traffic that had ESNI in 2020 [50]. If ECH becomes the global standard for TLS connections, censors will be forced to either upgrade or eventually be left behind.

Censorship circumvention has historically 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, while more recent efforts have been put forward to automate evasion strategy discovery [55]. However, as discussed in §4.5, many censors have resource or political willingness constraints. A country may be willing to implement a censorship regime knowing that determined users will get around their blocking and be content in knowing

that the majority of the Internet user population will not have access to denied content. On the whole, censors are constrained by the fundamental protocols that allow the Internet to operate as a network of networks. The Internet Censorship Methods Taxonomy scopes the problem space for anti-censorship software developers by characterizing what censor methods and techniques are possible. Future work may involve assigning metrics to assess a software tool's ability to counter particular censor methods. This would allow for objective comparison between the capabilities of different anti-censorship software.

Table 3. Citations of evidence of Internet censorship methods (by decade)

Censorship Method	References			
	2020-2023	2010-2019	2000-2009	1990-1999
Internet Shutdowns	[136,480,380,342,188,395,277]	[433,196,398,99]	-	-
IP Address Blocking	[342,44,487,124,494,52,316,362,12,413]	[317,289,404,462,433,142,6,71,451,394]	[335,105,484,86,115]	-
Port Blocking	[44,124,52,316]	[433,6,420]	-	-
Computer Network Attacks and Resource Exhaustion	[240,49,51,431,270]	[433,279,6,106,104,99,34,267]	[87,299,81]	-
BGP Attacks and Disruption	[89,342,223,277]	[300,6,43]	[371,436]	-
Bandwidth Throttling	[489,505]	[433,32,23]	-	-
DNS Tampering	[44,195,204,193,203,229,342,257,40,494,403,316,54,362,12,28,53,413]	[317,497,73,349,462,226,452,131,390,433,4,232,453,179,71,247,24,27,32,306,7,451,26,116,143,481,486,394]	[335,105,268,86,477,115]	-
Protocol/Application Content Filtering	[195,360,193,229,51,467,253,403,316,54,463,358,362,12,53,413,463,485]	[447,317,497,102,462,226,6,468,433,4,453,179,6,71,247,100,32,306,451,143,486,394,345]	[105,97,87,86,477,115]	[75]
TLS-based Filtering	[204,487,360,193,51,467,229,489,124,56,385,494,50,403,357,12,413,39]	[167,72,447,317,343,433,6,237,83,32,475]	-	-
Protocol/Application Fingerprinting	[195,488,494,53,14]	[462,117,234,344,433,142,449,127,460,128,207,32,475]	-	-

4.6 Summary

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." [112]. Accordingly, a growing number of authorities across the globe in many jurisdictions apply censorship to online communications. Understanding *how* censors implement content filtering, throttling of connections, or Internet shutdowns is crucial for researchers, policymakers, and practitioners implementing Internet protocols. A detailed analysis of the problem space also benefits developers of anti-censorship software, who provide users with a means of circumventing undue censorship where it happens.

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

CHAPTER 5: A WORLDWIDE VIEW OF NATION-STATE INTERNET CENSORSHIP ⁷

5.1 Background

5.1.1 Overview

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

5.1.2 Introduction

The Internet has become one of the most significant communication mechanisms in human history. In terms of media influence, it has surpassed television, print media, and radio [112] and is a routine aspect of daily life for millions of people globally. However, some nation-states impose censorship on Internet communications within their sphere of influence. Irrespective of the motivation behind Internet censors — ideological, autocratic, legal, social, or otherwise —

⁷ Preliminary results of the study in this chapter were presented at AvengerCon VII [282] and the Purdue CERIAS Security Symposium [285]. A paper based on this chapter was also published in the proceedings of the Free and Open Communications on the Internet (FOCI) workshop at the Privacy Enhancing Technologies Symposium (PETS) [286].

Internet censorship research is a broad interdisciplinary endeavor, with emphasis on explaining *how* online censorship occurs.

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

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

The research contributions of this study are three-fold: (1) First, the author conducted a cross-sectional study of 70 countries during a specified period of one year. The author used the same countries surveyed in the Freedom on the Net (FOTN) annual report by Freedom House [163] to ensure global representation across the continents. Diverse datasets showed how Internet censors deny access to information resources and communication mediums. (2) Second, the author analyzed prior work to illustrate historical censorship methods from these same nation-states over the past 20 years. The results of the analysis illustrate trends in Internet censorship and changes in Internet censor methods over time. For example, the author observed that most censors are seemingly willing, and in fact continue, to use "old" filtering methods, even though

they are easy to bypass. And increasingly, governments deliberately perform total Internet shutdowns to achieve their censorship goals. (3) Finally, the methodology presented offers an easily reproducible framework for continuous reporting and studying of worldwide censor activity.

5.1.3 Nation-state Internet Censorship

The authorities of some countries go to great lengths to deny their citizens free and open access to Internet resources. Nation-state Internet censorship is generally characterized as either centralized or decentralized in nature. Centralized censorship often occurs on government-controlled infrastructure. In some nations, there are few (or only one) Internet Service Providers (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 is the most cited example of centralized censorship [337,203,253,467,56,505,50,374,450,269,279,128,127,250,249,486,335,268,87,508]; their censorship apparatus is known as the "Great Firewall of China." Other examples include small countries with limited access to transnational fiber switching. Syria, which only has one government-controlled autonomous system (AS) [71], 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 [362,487] and India [184,403,497]. Authorities in these nations legally compel private-sector service providers to perform web filtering, throttling, or shutdowns. Technical implementations may vary widely between corporations, resulting in a patchwork of censorship. The author will refer to any entity that manipulates network traffic for the purposes of censorship a "censor" throughout this paper. While Freedom House's data shows an overarching continual reduction in global Internet freedom overall, some nations have scaled back censorship efforts, such as Myanmar from 2012-2019 [342], The Gambia from 2017-present [155], and Saudi Arabia from 2017-present [12].

5.1.4 Summary of Censor Methods

Internet censors use a variety of technical means to deny access to Internet resources. A crude and straightforward method is an Internet shutdown. Feldstein defines Internet shutdowns as "activities undertaken by states to intentionally restrict, constrain, or disrupt Internet or electronic communications within a given geographic area or affecting a specific population in order to exert control over the spread of information, within a timebound period" [135]. Shutdowns can be accomplished by physically disconnecting cable links, logically segmenting network traffic, or manipulating routing tables to ensure traffic does not reach its intended destination. Internet-wide disruptions have occurred when ASes in censoring countries tamper with Border Gateway Protocol (BGP) routing advertisements [342,371]. Censors also use bandwidth throttling to limit access to particular platforms or media sources [23,489] for a defined time period, sometimes during elections or incidents of civil unrest. Throttling can be implemented by injecting artificial latency, altering routing paths, traffic shaping, traffic policing, or applying quality of service (QoS) algorithms to "undesirable" traffic [304].

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

If a censor has deep packet inspection (DPI) capabilities, they can observe the payload content of IP packets. DPI enables the filtering of HTTP, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and other traffic based on keywords in the content of the

communication [446,61,41]. When users request websites protected by TLS, the traffic is encrypted so a passive observer cannot read its contents. However, censors can read the plaintext Server Name Indication (SNI) extension of a TLS header and block a destination website based on it. Finally, censors with more advanced capabilities use protocol fingerprinting techniques to identify particular protocols, applications, or other encrypted packets based on traffic patterns — and subsequently block associated traffic [383,400].

5.2 Methodology

The author used a mixed methods (quantitative and qualitative) approach to data collection in this study. Data from the 2021 FOTN report served as a foundation for analysis⁸, scoping the project while ensuring global representation. The author assessed all 70 countries from the FOTN report using the framework produced by this study. The author used the Internet censorship methods from the taxonomy in Chapter 4 to ensure comprehensive coverage of techniques.⁹ The taxonomy elements in the framework are those summarized in §5.1.4 above.

5.2.1 Data Sources

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

- **OONI.** The Open Observatory of Network Interference (OONI) [143] performs over a dozen Internet measurement tests for censorship in over 200 countries using crowdsourced data from software probes they distribute, and ingest tens of millions of data points monthly. The "web_connectivity" test provides detection mechanisms for DNS tampering, TCP/IP blocking, or blocking by a transparent HTTP proxy.

⁸ While the 2022 report has since been published, it did not exist at the time of this analysis.

⁹ The author chose not to include "Resource Exhaustion" (e.g., DDoS attacks) and "Computer Network Attack" from the Internet censorship methods taxonomy in this framework because those methods target resources outside of the censor's sphere of influence, to deny access to *all* Internet users. This study focuses on nation-state censorship against each nation's citizenry. The author also combined IP blocking and port blocking into one category.

- **Censored Planet.** Censored Planet provides a web-based dashboard to display the results of their Internet censorship detection. The platform utilizes various passive remote measurement techniques in more than 200 countries. This combination of tools includes: (1) Auger [348] uses TCP/IP side channels to measure reachability between two Internet locations without the use of a vantage point, (2) Satellite [390] uses public DNS resolvers to compare how popular webpages are resolved to determine where interference happens, (3) Quack and Hyperquack [358] use Echo and Discord servers to detect deep packet inspection (DPI) blocking for HTTP and HTTPS traffic.

- **Internet Society Pulse.** Internet Society Pulse curates information about Internet shutdown events occurring around the world and analyzes their economic and human impact. Data from their platform shows time-based network disconnections executed by authorities in the studied countries [217].

- **Access Now.** Access Now is a non-profit organization that promotes digital civil rights around the world [2]. The #KeepItOn project by Access Now generates an annual report and dataset to track Internet shutdowns, social media blockages, and network throttling globally [3].

5.2.2 Methods

Journal articles, conference proceedings, and technical reports covering the study timeframe filled gaps unobserved by the data sources above, if applicable. IClab [64,316] did not have published data for the entirety of the study period dates and was thus excluded. Based on the findings, the author filled in the columns and rows of this study's framework (see §5.5.1).

After the cross-sectional portion of the study was complete, the author used a systematic literature review (SLR) approach [325] to capture the historical context of censorship methods documented outside of the measurement period for each country. The author conjectured that presenting historical censorship activities with recent ones would illuminate inter-country and global trends.

CensorBib [474] was the starting point for SLR citations. CensorBib is an online archive¹⁰ of selected research papers on Internet censorship maintained by Dr. Philipp Winter [473]; nomination submissions are open to the public. The archive captured many of the country-specific studies from relevant journals and conferences. The author treated peer-reviewed journals and conferences as primary data sources, and technical reports and blog postings were considered case-by-case when primary sources were unavailable. Rather than surveying select journal proceedings, the author searched for country-specific case studies of Internet censorship. This study's list of surveyed nations began with the lowest scores on the FOTN 2021 report (“not free”) and ended with the highest scores (“free”). Low-scoring countries tended to have the highest number of citations, while free nations had few (if any) case studies on their censorship practices, with some exceptions.

5.2.3 Limitations and Delineations

This study was not intended to measure the quantity or frequency of particular censorship methods, only evidence of their occurrence. In pursuing this study's goal of illuminating global trends for censor methods, the author consequently loses some granularity. For example, in a nation-state with a decentralized implementation of DNS tampering, users served by one AS may be unable to access specific websites, while citizens in other regions can because of non-uniform distribution or implementation of blocklists nationally. If there is enough evidence of censorship in at least one AS, this study's data will reflect the nation in question as using that censor method. Additionally, this study's framework does not delineate "censorship leakage" [78], in which the blocking decisions made by particular ASes impact users in other countries outside of the censor's geopolitical borders.

There are limitations inherent to the use of Internet measurement data. Fletcher and Hayes-Bircher demonstrated in [149] that remotely measured Internet censorship datasets were less likely to contain false positives than subject matter expert (SME) analysis when taken as a whole. However, platforms such as OONI have documented records of false positives [358,497]. To minimize false positives, the author manually reviewed instances of "confirmed" censorship for accuracy. The author considered detected blockpages in OONI data, regardless of censor method,

¹⁰ Available at <https://censorbib.nymity.ch/>

as definitive censorship. For Censor Planet data, the author first ensured a URL with an "unexpected outcome" had a sufficient sample size from the probe (>30 count) prior to consideration. If so, the author then considered the proportionality of suspected blocking behavior. If over 50% of attempts resulted in strong indicators (e.g., TCP reset packets), the author considered it evidence of censorship. If the majority of attempts resulted in "matches" (page loaded correctly) or less clear-cut anomalies (e.g., "content mismatch"), the author did not document it as evidence during the cross-sectional study period.

Internet measurement data is also prone to sampling bias; researchers tend to focus on nation-states that heavily censor content or use advanced techniques to do so. Specific issues arise with OONI data, which is crowdsourced from users who download the OONI probe and run the software. The data will tend to skew toward countries with a history of censorship, or a sudden overt change (e.g., blockpages or social media restrictions) that incentivizes users to participate.

Research publications have limitations and potential for bias as well. Researchers often publish Internet censorship papers on "high-profile" offending countries, while certain Western nations receive little scrutiny or attention. Examples include China having 35 citations in this study, while Costa Rica had zero. A globally representative study (such as this Chapter) helps to highlight these gaps in the literature, and point toward important open research questions. Without continual effort across the continents to assess censorship activity, reporting may lean heavily towards historic offenders and not detect new ones. Articles in the literature also tend to focus on key historical events or problems, which may bias researchers' conclusions toward a perception of ever-increasing censorship [236] while potentially leaving out nations that make progress in reducing censorship. Recent efforts by groups such as OONI and Censored Planet to quantitatively highlight emerging censor trends [359,418,332] may help to balance this reporting.

5.3 Results and Analysis

5.3.1 The Framework

The final data and overall results of the study are depicted in Figure 23; citations of evidence (2001-2021) are shown in Table 5. The 70 assessed countries are the rows of Figure 23, sorted

by lowest to highest FOTN "total score." The column headers are organized into four sections; (1) Country name and ISO country code, (2) FOTN scores and status data, (3) Internet censorship methods, and (4) notes.

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

Internet censorship methods are listed as columns across the top, and are the central element of this study. Countries the author found evidence of using a particular method during the measurement period are identified with a circle icon. If the censorship method was only instituted for a specified period of time (rather than persistent filtering), the author indicated that with an unfilled circle icon. If the author encountered anecdotal observations of censorship but could not confirm it with quantitative evidence or a prior study, the author marked that country with a square icon to mean "unconfirmed."¹¹ These data represent all censor activity during the study period. The key in the top right corner of Figure 23 illustrates the shapes representing the different categories of evidence cited.

After completing the cross-sectional portion of the study and the SLR, the author illustrated historically observed censorship in Figure 23 using an upside-down triangle icon; that is, documented censor activity that occurred at some time outside of the study period over the last 20 years. The "notes" field on the far right includes additional qualitative context for each particular country. Historical events (e.g., war, conflicts, elections, civil unrest) often coincide with Internet censor activity. Exceptions or further explanations for a particular piece of evidence may have been warranted and included in the notes section as well. Table 5 documents all citations and evidence of Internet censorship methods by country.

¹¹ The author did not report unconfirmed (square icon) censor activity in any totals, discussion, or figures other than the framework in Figure 23 and associated citations in Table 5.

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

5.3.2 Analysis and Trends

Table 4 and Figure 24 are examples of quantitative analyses that can be derived from this study's framework. Figure 24 illustrates summary totals of countries that utilize particular censor methods. The bottom bars (red) indicate active use during the measurement period, while the top bars (pink) show countries that have historically made use of a censor method (but not as of 2021).

COUNTRY	ISO 3166-1 Country Code	FOITN 2021 Total Score				FOITN 2021 Status	Internet Shutdowns	IP Address	BGP Attacks or Port Blocking	Bandwidth Throttling	DNS Tampering	HTTP/URL	TLS-based Filtering	Protocol Fingerprinting	Notes	Study period for ●/○: June 01, 2020 to May 31, 2021
		Observed to Access	Limits on Content	Violations of User Rights	FOITN 2021 Status											
China	CN	10	8	2	0	Not Free	○	○●	▼	●	●	●	●	Centralized active blocking of VPNs, circumvention tools, and secure messengers		
Iran	IR	16	8	5	3	Not Free	○	○●*	▼	●	●	●	●	*Particular endpoints associated with QUIC/UDP targets, and residual censorship		
Myanmar (Burma)	MM	17	4	7	6	Not Free	○	●	○	●	▼			Military junta coup d'état after 2020 elections		
Cuba	CU	21	5	9	7	Not Free	○				●	●	▼	Mass anti-government protests of COVID-19 pandemic response, censored social media		
Vietnam	VN	22	12	6	4	Not Free				▼	▼			Censorship focus in print media		
Saudi Arabia	SA	24	12	8	4	Not Free		▼		▼	●	●		Reduced overall Internet filtering between 2017-2020		
Pakistan	PK	25	5	13	7	Not Free	○	▼	▼*	▼	●	●		*Global YouTube disruption via BGP 24FEB2008		
Egypt	EG	26	12	10	4	Not Free	○	●		●	●	●	●			
Ethiopia	ET	27	4	12	11	Not Free	○	▼			●	▼	▼	Tigray civil war		
United Arab Emirates	AE	27	12	9	6	Not Free				●	●	●	▼			
Uzbekistan	UZ	28	9	12	7	Not Free	○				●	●				
Venezuela	VE	28	6	12	10	Not Free				▼	●	●				
Bahrain	BH	30	16	8	6	Not Free				▼	●	●				
Russia	RU	30	12	10	8	Not Free	○	●	▼	○	●	●	○●	●	Decentralized, novel hybrid censor approaches observed	
Belarus	BY	31	10	14	7	Not Free	○	▼			●	●	●			
Kazakhstan	KZ	33	11	11	11	Not Free	○	○●	▼	▼	●	●	●	▼	Nation-wide deployment of government-issued root certificate, MITM interception 2019	
Sudan	SD	33	6	15	12	Not Free	○				▼					
Turkey	TR	34	15	10	9	Not Free	▼	▼	▼*	▼	●	●	●	*Global Internet disruption via BGP routes to Turkey 24DEC2004		
Azerbaijan	AZ	35	10	14	11	Not Free	○	▼			●	●	●	Second Nagorno-Karabakh war, late 2020		
Thailand	TH	36	16	13	7	Not Free				▼	●			High levels of inconsistency in routing, content mismatches		
Rwanda	RW	38	13	11	14	Not Free					▼					
Bangladesh	BD	40	12	17	11	Partly Free	○		▼		●	●				
Iraq	IQ	41	11	16	14	Partly Free	○			▼						
Cambodia	KH	43	13	18	12	Partly Free					●	●				
Zimbabwe	ZW	46	8	22	16	Partly Free	▼				▼					
Jordan	JO	47	13	17	17	Partly Free		▼	○*	●	●	●		*Throttling of a social media service during public protests		
Indonesia	ID	48	14	17	17	Partly Free				▼	●	●				
Libya	LY	48	7	25	16	Partly Free	▼		▼							
Nicaragua	NI	48	12	18	18	Partly Free					●	●				
India	IN	49	11	21	17	Partly Free	○	▼	○	●	●	●		89 Internet shutdowns during the measurement period		
Uganda	UG	49	11	19	19	Partly Free	○	▼				□*		2021 elections - shutdowns and social media; *Potential DPI censorship from AS21491		
Lebanon	LB	51	11	22	18	Partly Free					□*			*Limited data available		
Sri Lanka	LK	51	11	23	17	Partly Free	○									
Kyrgyzstan	KG	53	13	23	17	Partly Free					▼			Inconclusive for evidence of URL filtering during study period		
Morocco	MA	53	15	22	16	Partly Free				▼						
The Gambia	GM	53	12	22	19	Partly Free	▼				□			Internet freedom improvement since 2017		
Singapore	SG	54	19	17	18	Partly Free					●	□				
Malaysia	MY	58	18	21	19	Partly Free	▼				●	▼				
Malawi	MW	59	11	25	23	Partly Free	□*				□**			*2019 elections; **2011 alleged short-term blocking of news and social media		
Nigeria	NG	59	17	25	17	Partly Free	○	▼		▼	▼					
Zambia	ZM	59	15	24	20	Partly Free	▼				▼	▼		2021 elections, social media platform blocking (outside study period)		
Mexico	MX	60	18	25	17	Partly Free		▼*			●	●**		*Blocking of Tor directory authorities; **state-owned AS8151 TLS-based filtering		
Angola	AO	62	12	30	20	Partly Free						●**		*Blocking of anti-censorship software websites		
Ecuador	EC	62	17	25	20	Partly Free					●	●				
Ukraine	UA	62	20	21	21	Partly Free					●	●	●			
Tunisia	TN	63	16	28	19	Partly Free		▼			▼					
Brazil	BR	64	20	24	20	Partly Free					▼	▼				
Ghana	GH	64	14	27	23	Partly Free					●	●				
Colombia	CO	65	19	25	21	Partly Free	□*				▼			*Potential shutdown in parallel with anti-government protests		
Philippines	PH	65	17	26	22	Partly Free	▼*				●		▼	*Cellular telephony service shutdowns		
Kenya	KE	66	16	27	23	Partly Free								Government orders for removal of content in leu of blocking actions		
South Korea	KR	67	22	24	21	Partly Free		▼	▼	▼	●	●		Authorities have publicized their use of TLS-based filtering for illegal content		
Hungary	HU	70	21	24	25	Free					□*	□*		*AS60436 potentially performing filtering actions		
Argentina	AR	71	19	27	25	Free				▼						
Armenia	AM	71	19	26	26	Free	●				●	●		Second Nagorno-Karabakh war, late 2020		
Serbia	RS	71	21	25	25	Free					▼*			*State blocking of gambling websites		
South Africa	ZA	73	17	29	27	Free										
Australia	AT	75	23	27	25	Free			▼		□			State blocks gambling, torrent, and streaming sites		
United States	US	75	21	29	25	Free								Law Enforcement compels the removal of intellectual property theft rather than blocking		
Italy	IT	76	21	30	25	Free				●*				*Mostly blocking alleged criminal activity or copyright infringement		
Japan	JP	76	21	29	26	Free										
Georgia	GE	77	19	31	27	Free					□*			*Temporary blocking of "pro-Islamic State" websites 2015		
France	FI	78	23	30	25	Free					●	●		State blocking of websites related to "terrorism" and copyright infringement		
United Kingdom	GB	78	23	30	25	Free	▼	▼			●	●	●	IWF maintains court-ordered blocklist ("extreme pornography" and copyright infringement)		
Germany	DE	79	22	29	28	Free				▼	▼			Repeal of the Access Impediment Law (Zugangerschwerungsgesetz) 2011		
Taiwan	TW	80	24	31	25	Free					□*			*City of Taipei filters select websites on its public wifi		
Canada	CA	87	23	32	32	Free		▼	▼		●	●		State blocking of copyright infringement		
Costa Rica	CR	87	20	33	34	Free										
Estonia	EE	94	25	32	37	Free					●*			*State blocking of gambling websites		
Iceland	IS	96	25	34	37	Free					□*			*State blocking of copyright infringement		

Figure 23. Framework for evidence of Internet censorship methods by country

Table 4. Percentage of countries that use each Internet censorship method in the framework

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

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

Nation-state Censor Methods Summary

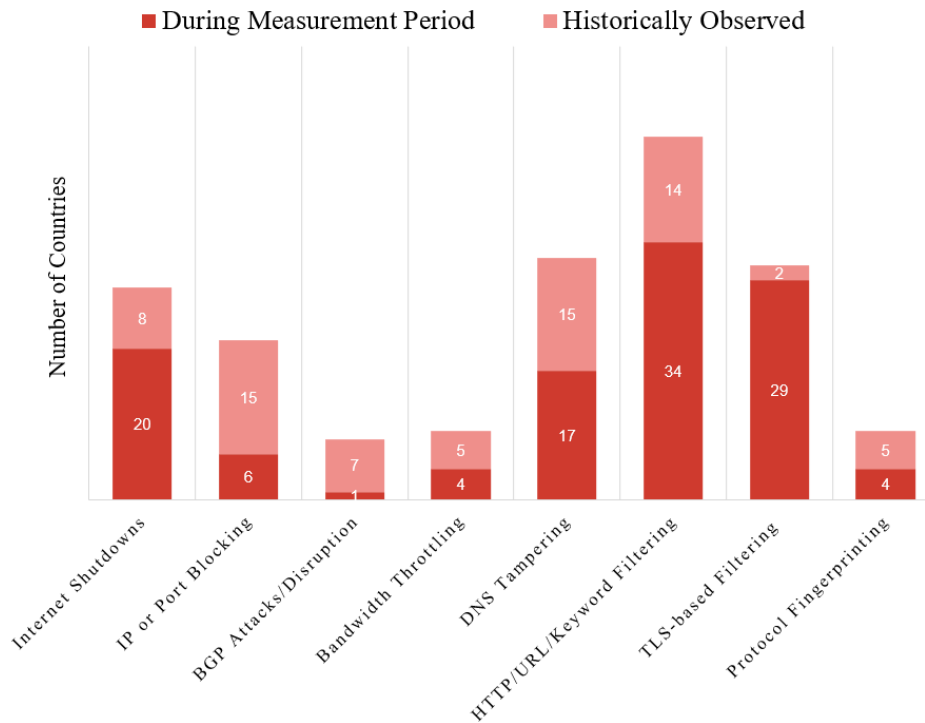


Figure 24. Nation-state censor methods summary

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

The author also observed a large percentage of nations (41%) leveraging TLS-based filtering capabilities against HTTPS traffic. This trend likely occurs because of the widespread adoption of TLS encryption. Encrypting HTTP traffic denies censors' ability to filter based on the network packet content of a website. Mozilla's telemetry reporting shows 82% of global traffic is HTTPS as of October 2021 [263], and adoption has only increased since then. Given this dilemma, censors with higher motivation have invested in hardware and software capable of targeting SNI in TLS headers of HTTPS requests.

Oddly enough, HTTP-based censorship remains the most utilized censor method (49%), despite the proliferation of TLS. This suggests that some censors are satisfied to sponsor content-based censorship regimes, despite being ineffective against most web traffic. Some of these

governments may not have agencies or individuals that understand the technology thoroughly enough to make informed decisions about updating their censorship architecture. There is also the reality that some parts of the world are underserved by HTTPS compared to more developed nations [214], and older censor methods may continue to work in these countries until system administrators update their web servers.

Some censor methods are reflected as mostly historic. IP and port blocking occurred frequently in the past (30%) but seldom during the study period (9%, or six countries). These will be discussed further in §5.3.3. BGP disruptions were also infrequent — likely because of the nature of manipulation of BGP announcements, which impact Internet routing far beyond a nation's borders. Two famous examples of actions by nation-states illustrate BGP-based censorship attempts [342,371], and both were short-lived.

Table 5. Citations for evidence of Internet censorship methods by country
(Sorted by FOTN ranking, as in Figure 23)

China	[333,229,164,498,467,494,40,52,505,72,348,349,127,279,205,128,179,27,319,250] [451,475,26,481,106,486,8,345,97,268,87,477,335,202,508]
Iran	[229,333,217,3,124,494,277,40,52,39,53,238,349,348,433,179,32,23,8,23,451,22]
Myanmar (Burma)	[217,3,342,179,233,101,333]
Cuba	[217,3,68,103,338,494,37]
Vietnam	[38,179,105]
Saudi Arabia	[229,12,233,100,451,18,507,105]
Pakistan	[333,217,229,4,306,111,5,247,105,371]
Egypt	[217,69,229,111,179,99]
Ethiopia	[217,3,69,495,418,111,8,433,105]
United Arab Emirates	[333,229,433,179,233,100,8,105]
Uzbekistan	[217,333,494,229,256]
Venezuela	[77,156,179]
Bahrain	[333,229,451,105]
Russia	[333,3,487,489,229,480,362,352,348,179,24,451,157]
Belarus	[217,3,492,111,349,333]
Kazakhstan	[217,3,229,441,40,52,357,111,349,433,179,8,336]
Sudan	[217,348,105]
Turkey	[333,229,348,499,415,111,433,416,9,150,24,451,436]
Azerbaijan	[217,177,333,69,347,233,105]
Thailand	[333,69,176,433,179,233,451,8,106,105]
Rwanda	[288,171,459,356]
Bangladesh	[217,3,69,229,46,451]
Iraq	[217,349,312]
Cambodia	[69]
Zimbabwe	[496]
Jordan	[69,229,313,304,278,394,105]
Indonesia	[349,179,333]
Libya	[331,348,43,99]
Nicaragua	[69]
India	[217,3,69,229,403,189,497,179,451,105,333]
Uganda	[217,3,490,69,491]
Lebanon	[69]
Sri Lanka	[69,217]
Kyrgyzstan	[69,179]
Morocco	[179]
The Gambia	[33,67,144]
Singapore	[69,158,402]
Malaysia	[333,69,179,478,233,451]
Malawi	[125,275]
Nigeria	[10,179,217,326]
Zambia	[351,493]
Mexico	[69,229,219]
Angola	[69]
Ecuador	[69,229]
Ukraine	[333,229]
Tunisia	[8,433,233,105]
Brazil	[448,454]
Ghana	[69]
Colombia	[105,314]
Philippines	[69,433,8,272]
Kenya	[159]
South Korea	[333,69,80,229,423,179,451,105]
Hungary	[69]
Argentina	[334]
Armenia	[69,480,280]
Serbia	[393]
South Africa	-
Australia	[133,365,381,43]
United States	[48,160,321,391,455,457]
Italy	[333,59,5]
Japan	-
Georgia	[419]
France	[179,229,333]
United Kingdom	[229,160,455,348,86]
Germany	[161,457,57,179,394,115]
Taiwan	[201]
Canada	[162,456,43]
Costa Rica	-
Estonia	[330,417]
Iceland	[190]

5.3.3 Discussion

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

DPI technologies have long been assumed to be too resource intensive to implement at a national scale. This study's data indicates otherwise; an increasing number of countries are willing and able to filter application-layer content. The most aggressive censors utilize hybrid approaches (Russia) [489], active probing of VPN and anti-censorship services (China) [127,319], and allowlisting prior to censorship-in-depth (Iran) [53]. The author also highlights the overall increased use of TLS-based blocking, often when a censor targets the unencrypted SNI to deny access to particular domains. This entire class of censorship techniques could potentially be eliminated by upgrading to an Encrypted ClientHello (ECH) — which is still in IETF draft [366]. Encrypted SNI (ESNI) was an earlier attempt to address privacy concerns of SNI targeting but faced implementation issues and was only supported by one major web browser, Mozilla Firefox [346]. PRC also took the unprecedented step of blocking most ESNI traffic [50]. Firefox has since abandoned ESNI in favor of supporting ECH development [220]; ECH will need to be widely deployed to ensure the cost of overblocking deters authorities from blocking the newest version of TLS.

As end-to-end encrypted (E2EE) messaging services gain popularity for their security and privacy properties, censoring nation-states have targeted these protocols with existing methods as well as more advanced protocol fingerprinting techniques. The proliferation of encrypted traffic analysis (ETA) tools or next-generation firewalls (NGFWs) that can block applications such as Signal or Tor Browser may pose a threat to freedom of expression if implemented by a censor. Notably, all evidence of censorship in the protocol fingerprinting category came from focused individual studies, not from the primary data sources in §5.2.1. As the author demonstrated in the data above, DPI was once assumed to be too resource intensive for implementation at the national level and has now seen widespread implementation. As end-to-end encryption

proliferates and becomes the norm, the author predicts that protocol fingerprinting and ETA methods will see increased adoption by the most aggressive Internet censors.

More targeted censorship methods enable regimes to meet their censorship goals while avoiding overblocking, minimizing economic collateral damage. Censors may also use sophisticated methods because they are more subtle, and deniability that censorship is occurring may avoid the political implications of public outcry. At the same time, countries in other parts of the world are increasingly willing to use blunt instruments of censorship — often total Internet shutdowns — during tumultuous periods of civil unrest or political change (29% of nations during the study period, 40% over all time).

The author also observed that nations typically understudied in terms of Internet censorship have some level of filtering happening within their borders. Several countries (e.g., Italy, France, Estonia, Iceland) use DNS tampering to block content considered illegal (e.g., intellectual property theft, gambling, pornography, terrorism, child sexual abuse materials) in their society. Some surprising Western examples included when Canada blocked COVID-19 information [456] and when police in the United Kingdom turned off WiFi in subway systems during environmental activism protests [455].

There are several positive trends for Internet freedom advocates in this study's data. The author observed a decline in the use of naive methods such as IP blocklists. This is potentially the case for several reasons: (1) difficulty in maintaining blocklists, as IP addresses are often ephemeral, (2) collateral damage, as blocking an IP range belonging to a CDN can deny access to large swaths of the Internet, and (3) as IPv6 is more widely deployed, the total IP address space grows significantly. This observation could be partially distorted based on bias in the literature as outlined in §5.2.3. However, in this study the author rarely observed port blocking in use for censorship. Typical web traffic occurs on ports 443, 80, and 53, and applications using other ports are not necessarily required to follow standard conventions when hosting their services. Iran is a notable exception in that it has implemented allowlisting for the three ports mentioned above on several occasions, denying access to all others. Another recent study highlighted "residual censorship," where censors detect an objectionable connection using one censorship

method, then proceed to deny all connections between the two endpoints for a short duration using a 3-tuple (client IP + server IP + port) or 4-tuple (client IP + port + server IP + port) [52]. Bock et al. observed this renewed, time-based approach to IP and port blocking in China, Iran, and Kazakhstan; further research is needed to determine if other nation-states are implementing similar functionality into their censorship systems.

Application layer filtering, specifically HTTP content and URL blocking, has also seen a decline in effectiveness. The broad adoption of encryption via TLS limits a censor's ability to analyze and target packet contents. DNS tampering occurs less often than HTTP-based application layer filtering, and several circumvention techniques remain available for DNS-based censorship: (1) changing the DNS server a user device submits requests to, (2) using encrypted DNS protocols, such as DNS over TLS or DNS over HTTPS, (3) using web proxies that support DNS traffic, such as SOCKS5, (4) using VPNs and tunnel-based anti-censorship tools. Detection and documentation of censors that block DoT/DoH and QUIC endpoints [40,124] are also points of serious consideration for Internet measurement researchers.

5.4 Summary

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

CHAPTER 6: DISCUSSION AND FUTURE DIRECTIONS

6.1 Summary of Contributions

This dissertation focused on the modeling and characterization of Internet censorship technologies. The project promotes a thorough understanding of the threats to Internet communications and protocols and informs researchers, censored users, and policymakers who support free and open communications.

Chapter 1 introduces the problem domain of censorship from an interdisciplinary perspective. Nation-states deny access to particular information based on political, legal, and cultural norms. Some censorship actions are widely considered acceptable (e.g., child sexual abuse material), while others are seen as violations of international human rights. The world wide web has become the primary communications platform for many people and has surpassed other traditional media outlets in terms of reach and influence. As a consequence, censorship on the Internet has become an important and consequential area of concern.

Chapter 2 outlines the existing literature on Internet censorship from multiple research communities. Internet measurement researchers observe how the Internet functions from a technical perspective, and a subsection of those focus on the collection of evidence of censorship online. Some advocacy organizations document instances of Internet shutdowns and blocking of online platforms to promote Internet freedom. Political science and sociology researchers study the effects of censorship on populations of people. Privacy-enhancing technology and anti-censorship developers design software to circumvent censorship where it happens, according to varied threat models. The author draws on these data as a foundation for several studies. The author also proposes three categories for researchers to organize deployed anti-censorship tools: access-focused, privacy-focused, and incidental.

Chapter 3 presents a reference model for Internet censorship technologies. The model serves as a descriptive, conceptualized representation of censorship systems. The model is depicted graphically and consists of three functional components: censor assessment, decision

enforcement, and data processing. It can serve as a pedagogical tool as well as a point of comparison among system designs. The model is presented so experts and non-specialist stakeholders can benefit from it. The descriptive knowledge of the model is validated by an iterative methodology using the outcomes of the studies in Chapters 4 and 5.

Chapter 4 offers a survey of Internet censorship methods. The author uses a systematic literature review methodology to comprehensively survey the literature for the methods used by Internet censors, which must operate within the limitations of the protocols that make the Internet function as a network of networks. The survey systematizes the technical means censors implement, outlined by the legal and social circumstances in which they have occurred over the past three decades. The outcome of the study is a comprehensive taxonomy of Internet censor methods, available in §4.5.

Chapter 5 presents a worldwide view of nation-state Internet censorship. Using a mixed methods (quantitative and qualitative) approach, the author constructs a research framework for documenting nation-state Internet censor activity. The sample countries investigated were globally representative, enriched with qualitative data from Freedom House's annual Freedom on the Net report, and informed by the taxonomy in Chapter 4. A cross-sectional study using data from Internet measurement sources exposes current censor activities. A systematic review then highlights historical censor activities from the same nations over the past 20 years. The author's research outcomes from this study are three-fold: (1) a snapshot of current and emerging Internet censorship methods around the world, (2) a holistic view of changes in censorship trends over the past two decades as the Internet has become a primary means of human communication, and (3) a novel research framework to allow for ease of continual analysis.

6.2 Future Work

Internet censorship is a dynamic and consequential topic of study; the values of the people involved determine what information is objectionable or worthy of being censored. When governments exceed what is perceived as acceptable censoring and deny access to free and open information, others will promote ways to circumvent the censorship. This paradigm was true of print mediums and continues at an accelerated pace with technological advancements.

Understanding *how* censors implement online content filtering, throttling of connections, or Internet shutdowns is crucial for researchers, policymakers, and practitioners implementing Internet protocols.

The topics below are areas in need of attention in the field of Internet censorship. They apply to research communities and practitioners. Some topics are direct extensions of the work in this dissertation, and others are gaps uncovered during these studies.

Granular metrics for anti-censorship evaluation. Chapter 3 presents a reference model for Internet censorship technologies. Aside from being a pedagogical tool, the author explores the example use case of measuring the effectiveness of an anti-censorship tool's data transformation and its impact on a censor's ability to deny access. A future study that assigns sets of quantifiable metrics to each element within the functional component of censor assessment would allow for an in-depth, technical evaluation of an anti-censorship tool's ability to circumvent current and future censor methods. This evaluation framework would benefit funding agencies that want to support anti-censorship software projects, providing an objective and evidence-based assessment of the tool's capabilities.

Replication studies for evidence of global censorship. Replication of results is a basic requirement for scientific integrity. Replication using the research framework presented in Chapter 5 would serve two purposes. First, the studies would confirm the reliability of the framework if separate researchers could reproduce the same study results given the published datasets. Second, performing the study again in several years with the Chapter 5 output data as a historical baseline will longitudinally illuminate global trends in Internet censorship methods over time.

Standardized formatting for Internet measurement data related to censorship. The studies in this dissertation required significant manual analysis. Many dataset sources were required to provide coverage of all Internet censorship methods in Chapter 5. Continued collaboration between Internet measurement researchers towards a common standardized format would ease the burden of manual human analysis and documentation in future studies. Ideally, in the future a

researcher could define specific parameters for an investigation and use an automated script or software process to produce reports quickly. Reports automatically produced at regular intervals would allow the Internet censorship research community to keep track of censor trends longitudinally (and more effectively).

Systematization of knowledge of Internet surveillance. Internet censorship and surveillance are related but distinct topics. Censorship involves access to information, while surveillance addresses privacy problems. This dissertation addresses Internet censorship in-depth, but research communities would benefit from the same level of analysis given to Internet surveillance. An SoK or taxonomy of Internet surveillance methods would significantly benefit researchers concerned with Internet governance.

Encrypted ClientHello (ECH). The author of this dissertation believes that implementing ECH into the TLS protocol (and its subsequent deployment to web servers and services worldwide) would have a near-term, widespread impact on improving the privacy of all Internet communications. TLS is already widely implemented, providing confidentiality to web traffic and thwarting content-based censorship methods. ECH and improvements to the TLS protocol can potentially eliminate a class of censor methods that take advantage of plaintext server name indication (SNI) extensions currently found in HTTPS traffic. The Internet Engineering Task Force (IETF) has a draft request for comments (RFC) for ECH — but needs resources and the support of developers, security researchers, and industry stakeholders to arrive at the point where typical Internet users can benefit from ECH.

APPENDIX: DATASETS

Open Observatory of Network Interference Data

The OONI data used in Chapter 5 are available at the following URL:
<https://doi.org/10.5281/zenodo.8040694>

Censored Planet Data

The Censored Planet data used in Chapter 5 are available in the web application at the following URL: <https://dashboard.censoredplanet.org/>

Access Now Data

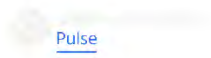
The Access Now, #KeepItOn data used in Chapter 5 are available in an Excel spreadsheet at the following URL: <https://doi.org/10.5281/zenodo.8040694>

Freedom on the Net Data

The FOTN 2021 data used in Chapter 5 are available in Excel spreadsheets at the following URL:
<https://doi.org/10.5281/zenodo.8040694>

Internet Society Pulse Data

The Internet Society Pulse data used in Chapter 5 are presented here:



Internet Shutdowns

An Internet shutdown is an intentional disruption of Internet-based communication, making it inaccessible or unavailable in a specific location. Restrictions to Internet access are on the rise globally, with frequent news of government-mandated disruptions of Internet access. Driven largely by political and national security concerns, state-ordered Internet shutdowns have become the 'new normal' in many countries.

Internet Society Pulse curates information about Internet shutdown events occurring around the world, and looks at the economic and human impact of these actions. Data on regional and national scale disruptions to Internet connectivity is included, as well as on application-level blocking and content blocking (where Internet connectivity remains available but access to certain websites or applications is limited).

Read our previous publications on shutdowns

Related Pulse Posts

- Multiple Internet Disruptions Observed in Iran
- New Report on the Impact of Internet Shutdowns to Prevent Cheating on Exams Launched
- Iran's Internet Shutdowns are Facilitated by Careful Attempts at Fragmentation of the Network



The geographic boundaries in this country series shown on this site do not imply the expression of a viewpoint on the part of the Internet Society concerning the legal status of any country, territory, city or area of its outlying islands, borders and divided lines on maps represent common usage border lines for which there may not be an official agreement. We use ISO 3166 country codes and names. The show coordinates is dictated by the IP. Geocast at network.



Events

Start date
Jun 1, 2021

Search for shutdowns

- May 2021
 - **Syrian Arab Republic (the)**
 - May 31, 2021 01:00 - June 22, 2021 07:30 (22 days)
 - National
 - **Palestine, State of**
 - May 15, 2021 12:15 - May 25, 2021 17:00 (10 days 4 hours)
 - Regional
- April 2021



India

> April 11 - April 13, 2021 (3 days)
Regional

India

> April 8, 2021 (1 day)
Regional

o **March 2021**

Kazakhstan

> March 28, 2021 (1 day)
Regional

Kazakhstan

> March 27 - March 28, 2021 (2 days)
National

India

> March 27, 2021 (1 day)
Regional

Bangladesh

> March 26, 2021 (1 day)
National

India

> March 21 - March 22, 2021 (2 days)
Regional

Congo (the)

> March 20, 2021 23:00 - March 23, 2021 23:00 (3 days)
National

Myanmar

> March 15, 2021 00:00 (562 days) - active
National

India

> March 13 - March 15, 2021 (3 days)
Regional

India

> March 10 - March 11, 2021 (2 days)
Regional

India

> March 8, 2021 (1 day)
Regional

Chad

> March 5, 2021 (1 day)
Regional

Senegal

> March 4 - March 5, 2021 (2 days)
National

o **February 2021**

Chad

> February 27 - March 3, 2021 (5 days)
Regional

Niger (the)



- > February 24 - February 28, 2021 (5 days)
Regional
- India**
 - > February 24, 2021 (1 day)
Regional
- India**
 - > February 18 - February 19, 2021 (2 days)
Regional
- Myanmar**
 - > February 14, 2021 17:30 - April 27, 2021 03:00 (71 days)
National
- Myanmar**
 - > February 6, 2021 02:00 - February 7, 2021 08:00 (1 day 6 hours)
National
- India**
 - > February 5, 2021 (1 day)
Regional
- Myanmar**
 - > February 2, 2021 00:00 (603 days) - active
Content blocking
- o **January 2021**
 - Myanmar**
 - > January 31, 2021 20:50 - February 1, 2021 08:15 (11 hours)
National
 - India**
 - > January 29 - January 31, 2021 (3 days)
Regional
 - India**
 - > January 29 - January 30, 2021 (2 days)
Regional
 - India**
 - > January 27, 2021 12:00 - January 28, 2021 17:00 (1 day 5 hours)
Regional
 - India**
 - > January 26 - February 6, 2021 (12 days)
Regional
 - India**
 - > January 26, 2021 (1 day)
Regional
 - Uganda**
 - > January 13, 2021 16:30 - January 18, 2021 08:00 (4 days 15 hours)
National
- o **December 2020**
 - Jordan**
 - > December 31, 2020 - January 4, 2021 (5 days)
Content blocking
 - India**
 - > December 30, 2020 - January 5, 2021 (7 days)
Regional



- India**
 - > December 18 - December 19, 2020 (2 days)
 - Regional

- India**
 - > December 15 - December 16, 2020 (2 days)
 - Regional

- India**
 - > December 13, 2020 (1 day)
 - Regional

- India**
 - > December 12 - December 23, 2020 (12 days)
 - Regional

- India**
 - > December 9 - December 10, 2020 (2 days)
 - Regional

- Iraq**
 - > December 8, 2020 (1 day)
 - Regional

- India**
 - > December 7, 2020 (1 day)
 - Regional

- India**
 - > December 3 - December 4, 2020 (2 days)
 - Regional

- India**
 - > December 1, 2020 (1 day)
 - Regional

- **November 2020**
 - India**
 - > November 30 - December 1, 2020 (2 days)
 - Regional

 - India**
 - > November 28, 2020 (1 day)
 - Regional

 - Cuba**
 - > November 27 - November 30, 2020 (4 days)
 - National

 - India**
 - > November 19, 2020 (1 day)
 - Regional

 - Cameroon**
 - > November 18, 2020 20:30 - November 19, 2020 08:30 (12 hours)
 - National

 - Belarus**
 - > November 15, 2020 06:00 - 17:35 (11 hours)
 - Regional

 - India**
 - > November 13 - November 15, 2020 (3 days)
 - Regional



India

> November 10, 2020 (1 day)
National

India

> November 5 - November 6, 2020 (2 days)
National

Ethiopia

> November 4, 2020 (693 days) - active
Regional

Ethiopia

> November 3, 2020 22:00 - November 6, 2020 04:00 (2 days 6 hours)
Regional

India

> November 1 - November 2, 2020 (2 days)
National

India

> November 1, 2020 (1 day)
National

o **October 2020**

India

> October 30 - November 4, 2020 (6 days)
National

India

> October 26, 2020 (1 day)
National

Tanzania, the United Republic of

> October 26 - November 6, 2020 (12 days)
Content blocking

Guinea

> October 23, 2020 09:00 - October 27, 2020 13:00 (4 days 4 hours)
National

Egypt

> October 22 - October 23, 2020 (2 days)
National

India

> October 20 - October 21, 2020 (2 days)
National

India

> October 19 - October 20, 2020 (2 days)
Regional

India

> October 16, 2020 (1 day)
Regional

India

> October 16 - October 17, 2020 (2 days)
Regional

Yemen

> October 15, 2020 (1 day)
Regional



India

> October 10 - October 11, 2020 (2 days)
Regional

India

> October 10, 2020 (1 day)
Regional

India

> October 6 - October 7, 2020 (2 days)
Regional

o **September 2020**

Azerbaijan

> September 27 - December 11, 2020 (76 days)
National

India

> September 27 - September 28, 2020 (2 days)
Regional

India

> September 25 - October 13, 2020 (19 days)
Regional

Yemen

> September 24, 2020 (734 days) - active
Regional

India

> September 21 - September 22, 2020 (2 days)
Regional

Sudan (the)

> September 16, 2020 06:00 - 09:00 (3 hours)
National

India

> September 16 - September 19, 2020 (4 days)
Regional

India

> September 15, 2020 (1 day)
Regional

Algeria

> September 13, 2020 06:30 - 17:00 (10 hours)
National

India

> September 13 - September 14, 2020 (2 days)
Regional

Belarus

> September 13, 2020 (1 day)
Regional

India

> September 4 - September 5, 2020 (2 days)
Regional

o **August 2020**

India



- > August 29 - August 30, 2020 (2 days)
Regional
- India**
 - > August 28 - August 29, 2020 (2 days)
Regional
- Belarus**
 - > August 26, 2020 17:20 - 18:20 (1 hour)
Regional
- India**
 - > August 22, 2020 (1 day)
Regional
- Syrian Arab Republic (the)**
 - > August 22 - August 31, 2020 (10 days)
National
- India**
 - > August 19 - August 20, 2020 (2 days)
Regional
- Chad**
 - > August 18 - September 10, 2020 (24 days)
National
- Belarus**
 - > August 17, 2020 08:15 - 09:00 (45 minutes)
National
- India**
 - > August 17 - August 18, 2020 (2 days)
Regional
- India**
 - > August 15, 2020 (1 day)
Regional
- Iraq**
 - > August 12, 2020 15:00 - 18:00 (3 hours)
Regional
- Belarus**
 - > August 9 - August 11, 2020 (3 days)
National
- o July 2020
 - Jordan**
 - > July 29 - August 11, 2020 (14 days)
Content blocking
 - Yemen**
 - > July 22, 2020 - April 14, 2021 (267 days)
National
 - India**
 - > July 18 - July 19, 2020 (2 days)
Regional
 - India**
 - > July 17 - July 18, 2020 (2 days)
Regional
 - Pakistan**



- > July 13, 2020 (1 day)
Regional
- Syrian Arab Republic (the)**
 - > July 12, 2020 00:50 - 05:30 (4 hours)
National
- India**
 - > July 12 - July 13, 2020 (2 days)
Regional
- Mali**
 - > July 10 - July 15, 2020 (6 days)
National
- Syrian Arab Republic (the)**
 - > July 9, 2020 00:50 - 05:30 (4 hours)
National
- Yemen**
 - > July 8 - July 22, 2020 (15 days)
Regional
- India**
 - > July 8, 2020 (1 day)
Regional
- Syrian Arab Republic (the)**
 - > July 7, 2020 00:50 - 05:30 (4 hours)
National
- India**
 - > July 7 - July 8, 2020 (2 days)
Regional
- India**
 - > July 4 - July 5, 2020 (2 days)
Regional
- Jordan**
 - > July 1 - July 23, 2020 (23 days)
Content blocking
- o June 2020
 - India**
 - > June 30 - July 1, 2020 (2 days)
Regional
 - India**
 - > June 30, 2020 (1 day)
Regional
 - Ethiopia**
 - > June 30 - July 23, 2020 (24 days)
National
 - Syrian Arab Republic (the)**
 - > June 29, 2020 00:50 - 05:30 (4 hours)
National
 - India**
 - > June 29, 2020 (1 day)
Regional



India
> June 25 - June 26, 2020 (2 days)
Regional

India
> June 25 - June 26, 2020 (2 days)
Regional

India
> June 23, 2020 (1 day)
Regional

Chad
> June 22 - August 18, 2020 (58 days)
National

Syrian Arab Republic (the)
> June 21, 2020 00:50 - 05:30 (4 hours)
National

India
> June 21, 2020 (1 day)
Regional

Myanmar
> June 21 - July 26, 2020 (36 days)
Regional

India
> June 20 - June 21, 2020 (2 days)
Regional

Belarus
> June 19, 2020 (1 day)
National

India
> June 18 - June 20, 2020 (3 days)
Regional

India
> June 18 - June 19, 2020 (2 days)
Regional

India
> June 16 - June 17, 2020 (2 days)
Regional

India
> June 13 - June 14, 2020 (2 days)
Regional

India
> June 10 - June 12, 2020 (3 days)
Regional

India
> June 7 - June 8, 2020 (2 days)
Regional

India
> June 3 - June 5, 2020 (3 days)
Regional

India

[Pulse](#)

India

» May 31, 2020 (1 day)
Regional

India

» May 30, 2020 (1 day)
Regional

India

» May 25, 2020 (1 day)
Regional

Burundi

» May 20 - May 21, 2020 (2 days)
National

India

» May 19 - May 20, 2020 (2 days)
Regional

India

» May 18 - May 22, 2020 (5 days)
Regional

India

» May 14, 2020 (1 day)
Regional

Sri Lanka

» May 14 - May 16, 2020 (3 days)
Regional

India

» May 13 - May 14, 2020 (2 days)
Regional

India

» May 12 - May 27, 2020 (16 days)
Regional

India

» May 12 - May 17, 2020 (6 days)
Regional

India

» May 6 - May 13, 2020 (8 days)
Regional

India

» May 6 - May 7, 2020 (2 days)
Regional

◊
[Show more](#)

Contact pulse@isoc.org

Follow us

Stay In Touch [Mailing List sign-up](#)

[Privacy Policy](#)

[Terms & Conditions](#)

Pulse

REFERENCES

- [1] Nicholas Aase, Jedidiah R. Crandall, Álvaro Díaz, Jeffrey Knockel, Jorge Ocaña Molinero, Jared Saia, Dan Wallach, and Tao Zhu. 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. Retrieved from <https://www.usenix.org/system/files/conference/foci12/foci12-final17.pdf>
- [2] Access Now. 2022. Access Now - About Us. *AccessNow.org*. Retrieved from <https://www.accessnow.org/about-us/>
- [3] Access Now. #KeepItOn Coalition dataset 2016-2021. *Access Now*. Retrieved from <https://www.accessnow.org/keepiton-2016-2021-data>
- [4] Giuseppe Aceto, Alessio Botta, Antonio Pescapè, M. Faheem Awan, Tahir Ahmad, and Saad Qaisar. 2016. Analyzing Internet Censorship in Pakistan. In *Research and Technologies for Society and Industry*, IEEE. Retrieved from <https://doi.org/10.1109/RTSI.2016.7740626>
- [5] Giuseppe Aceto, Alessio Botta, Antonio Pescapè, Nick Feamster, M. Faheem Awan, Tahir Ahmad, and Saad Qaisar. 2015. Monitoring Internet Censorship with UBICA. In *Traffic Monitoring and Analysis*, Springer. Retrieved from http://wpage.unina.it/giuseppe.aceto/pub/aceto2015monitoring_TMA.pdf
- [6] Giuseppe Aceto and Antonio Pescapè. 2015. Internet Censorship detection: A survey. *Computer Networks* 83, (June 2015), 381–421. DOI:<https://doi.org/10.1016/j.comnet.2015.03.008>
- [7] AFNIC. 2013. *Report of the AFNIC Scientific Council: Consequences of DNS-based Internet filtering*. Retrieved from <https://www.afnic.fr/wp-media/uploads/2021/01/SC-consequences-of-DNS-based-Internet-filtering.pdf>
- [8] Sadia Afroz and David Fifield. Timeline of Tor Censorship. *University of California, Berkeley*. Retrieved from http://www1.icsi.berkeley.edu/~sadia/tor_timeline.pdf
- [9] Mustafa Akgül and Melih Kırılidoğ. 2015. Internet censorship in Turkey. *Internet Policy Review* 4, 2 (June 2015). DOI:<https://doi.org/10.14763/2015.2.366>
- [10] Sodiq Alabi. 2017. President Buhari's Secret War on Free Speech. *Paradigm Initiative*. Retrieved from <https://paradigmhq.org/president-buharis-secret-war-on-free-speech/>
- [11] Albany Associates. 2012. The Arab Spring and the impact of social media. *Albany Associates*. Retrieved from <https://web.archive.org/web/20130512021954/http://www.albanyassociates.com/notebook/2012/03/the-arab-spring-and-the-impact-of-social-media/>

- [12] Fatemah Alharbi, Michalis Faloutsos, and Nael Abu-Ghazaleh. 2020. Opening Digital Borders Cautiously yet Decisively: Digital Filtering in Saudi Arabia. In *Free and Open Communications on the Internet*, USENIX. Retrieved from https://www.usenix.org/system/files/foci20-paper-alharbi_0.pdf
- [13] Hassanein Ali. 2020. THE RISE AND FALL OF ISLAMIC STATE: CURRENT CHALLENGES AND FUTURE PROSPECTS. *Asian Affairs* 51, 1 (January 2020), 71–94. DOI:<https://doi.org/10.1080/03068374.2019.1706940>
- [14] Alice, Bob, Carol, Jan Beznazwy, and Amir Houmansadr. 2020. How China Detects and Blocks Shadowsocks. In *Internet Measurement Conference*, ACM. Retrieved from <https://censorbib.nymity.ch/pdf/Alice2020a.pdf>
- [15] Mohammed H. Almeshekah and Eugene H. Spafford. 2014. Using Deceptive Information in Computer Security Defenses: *International Journal of Cyber Warfare and Terrorism* 4, 3 (July 2014), 63–80. DOI:<https://doi.org/10.4018/ijcwt.2014070105>
- [16] Mohammed H. Almeshekah and Eugene H. Spafford. 2014. Planning and Integrating Deception into Computer Security Defenses. In *Proceedings of the 2014 New Security Paradigms Workshop*, ACM, 127–138. DOI:<https://doi.org/10.1145/2683467.2683482>
- [17] Raed Al-Qura'n, Ali Hadi, Jalal Atoum, and Malek Al-Zewairi. 2015. Ultrasurf Traffic Classification: Detection and Prevention. *IJCNS* 08, 08 (2015), 304–311. DOI:<https://doi.org/10.4236/ijcns.2015.88030>
- [18] Khalid M Al-Tawil. 2001. The Internet in Saudi Arabia. *Telecommunications Policy* 25, 8–9 (September 2001), 625–632. DOI:[https://doi.org/10.1016/S0308-5961\(01\)00036-2](https://doi.org/10.1016/S0308-5961(01)00036-2)
- [19] AlterMidya. 2021. Joint statement by Bulatlat and Altermidya: Hold the Philippine Army accountable for cyberattacks against PH media websites. *AlterMidya*. Retrieved from <https://www.altermidya.net/joint-statement-by-bulatlat-and-altermidya-hold-the-philippine-army-accountable-for-cyberattacks-against-ph-media-websites/>
- [20] Warda Amalou and Merouane Mehdi. 2022. An Approach to Mitigate DDoS Attacks on SIP Based VoIP. In *ICCEIS 2021*, MDPI. DOI:<https://doi.org/10.3390/engproc2022014006>
- [21] George Anastaplo. censorship. *Encyclopedia Britannica*. Retrieved from <https://www.britannica.com/topic/censorship>
- [22] Collin Anderson. 2012. *The Hidden Internet of Iran: Private Address Allocations on a National Network*. Technical Report. Retrieved from <https://arxiv.org/pdf/1209.6398v1.pdf>
- [23] Collin Anderson. 2013. *Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran*. Technical Report, University of Pennsylvania, Philadelphia, PA. Retrieved July 16, 2022 from <http://arxiv.org/abs/1306.4361>

- [24] Collin Anderson, Philipp Winter, and Roya. 2014. Global Network Interference Detection over the RIPE Atlas Network. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/conference/foci14/foci14-anderson.pdf>
- [25] Raymond Angelo. 2019. Secure Protocols and Virtual Private Networks: An Evaluation. *IIS* (2019). DOI:https://doi.org/10.48009/3_iis_2019_37-46
- [26] Anonymous. 2012. The collateral damage of internet censorship by DNS injection. *ACM SIGCOMM Computer Communication Review* 42, 3 (June 2012), 21–27. DOI:<https://doi.org/10.1145/2317307.2317311>
- [27] Anonymous. 2014. Towards a Comprehensive Picture of the Great Firewall’s DNS Censorship. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf>
- [28] Anonymous, Arian Akhavan Niaki, Nguyen Phong Hoang, Phillipa Gill, and Amir Houmansadr. 2020. Triplet Censors: Demystifying Great Firewall’s DNS Censorship Behavior. In *Free and Open Communications on the Internet*, USENIX. Retrieved from https://www.usenix.org/system/files/foci20-paper-anonymous_0.pdf
- [29] Apple. 2021. iCloud Private Relay Overview. Retrieved from https://www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF
- [30] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. 2017. Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. *Proceedings on Privacy Enhancing Technologies* (August 2017). Retrieved June 3, 2021 from <https://doi.org/10.2478/popets-2019-0040>
- [31] N. Scott Arnold. 2009. *Imposing Values: An Essay on Liberalism and Regulation*. Oxford University Press, Oxford ; New York.
- [32] Simurgh Aryan, Homa Aryan, and J Alex Halderman. 2013. Internet Censorship in Iran: A First Look. In *Free and Open Communications on the Internet*. Retrieved from <https://www.usenix.org/system/files/conference/foci13/foci13-aryan.pdf>
- [33] Muhammed S. Bah. 2016. Gambia: Are Social Networking Applications Blocked? *AllAfrica*. Retrieved from <https://allafrica.com/stories/201608240945.html>
- [34] Michael Bailey and Craig Labovitz. 2011. *Censorship and Co-option of the Internet Infrastructure*. Technical Report, University of Michigan, Ann Arbor.
- [35] David Bamman, Brendan O’Connor, and Noah Smith. 2012. Censorship and deletion practices in Chinese social media. *First Monday* 17, (March 2012). DOI:<https://doi.org/10.5210/fm.v17i3.3943>

- [36] Michael N. Barnett. 1997. Bringing in the New World Order: Liberalism, Legitimacy, and the United Nations. *World Pol.* 49, 4 (July 1997), 526–551. DOI:<https://doi.org/10.1017/S0043887100008042>
- [37] Guy Baron and Gareth Hall. 2015. Access Online: Internet Governance and Image in Cuba. *Bulletin of Latin American Research* 34, 3 (July 2015). DOI:<https://doi.org/10.1111/blar.12263>
- [38] Thomas A. Bass. 2017. *Censorship in Vietnam: brave new world*. University of Massachusetts Press, Amherst.
- [39] Simone Basso. 2020. DNS over TLS blocked in Iran. *Open Observatory of Network Interference*. Retrieved from <https://ooni.org/post/2020-iran-dot/>
- [40] Simone Basso. 2021. Measuring DoT/DoH blocking using OONI Probe: a preliminary study. In *Network and Distributed System Security (NDSS) Symposium*, NDSS. Retrieved from <https://www.ndss-symposium.org/wp-content/uploads/dnspriv21-02-paper.pdf>
- [41] Ralf Bendrath and Milton Mueller. 2011. The end of the net as we know it? Deep packet inspection and internet governance. *New Media & Society* 13, 7 (November 2011), 1142–1160. DOI:<https://doi.org/10.1177/1461444811398031>
- [42] Karyn Benson. 2016. Leveraging Internet Background Radiation for Opportunistic Network Analysis. University of California, San Diego. Retrieved September 28, 2022 from <https://www.proquest.com/dissertations-theses/leveraging-internet-background-radiation/docview/1828386151/se-2>
- [43] Karyn Benson, Alberto Dainotti, K. C. Claffy, and Emile Aben. 2013. Gaining Insight into AS-level Outages through Analysis of Internet Background Radiation. In *Traffic Monitoring and Analysis*, IEEE. Retrieved from <https://cseweb.ucsd.edu/~kbenson/papers/tma13.pdf>
- [44] Abhishek Bhaskar and Paul Pearce. 2022. Many Roads Lead To Rome: How Packet Headers Influence DNS Censorship Measurement. *USENIX Security Symposium (2022)*. Retrieved from <https://www.usenix.org/system/files/sec22-bhaskar.pdf>
- [45] Francine Biazin do Nascimento. 2021. Measuring the Accessibility of Popular Websites While Using Mullvad VPN. Delft University of Technology. Retrieved from <http://resolver.tudelft.nl/uuid:190ac398-50a0-4a47-9ec4-5514d5b22e25>
- [46] Mehrab Bin Morshed, Michaelanne Dye, Syed Ishtiaque Ahmed, and Neha Kumar. 2017. When the Internet Goes Down in Bangladesh. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, ACM, Portland Oregon USA, 1591–1604. DOI:<https://doi.org/10.1145/2998181.2998237>
- [47] Benedikt Birtel and Christian Rossow. 2020. Slitheen++: Stealth TLS-based Decoy Routing. In *Free and Open Communications on the Internet*. Retrieved from https://www.usenix.org/system/files/foci20-paper-birtel_0.pdf

- [48] Constance Bitso, Ina Fourie, and Theo J D Bothma. 2013. Trends in transition from classical censorship to Internet censorship: selected country overviews. *Innovation: journal of appropriate librarianship and information work in Southern Africa* (2013). Retrieved from <https://journals.co.za/doi/abs/10.10520/EJC148135>
- [49] Kevin Bock, Abdulrahman Alaraj, Yair Fax, Kyle Hurley, Eric Wustrow, and Dave Levin. 2021. Weaponizing Middleboxes for TCP Reflected Amplification. In *USENIX Security Symposium*, USENIX. Retrieved from <https://www.usenix.org/system/files/sec21-bock.pdf>
- [50] Kevin Bock, Anonymous, Louis-Henri Merino, David Fifield, Amir Houmansadr, and Dave Levin. 2020. Exposing and Circumventing China’s Censorship of ESNI. *Great Firewall Report*. Retrieved from https://gfw.report/blog/gfw_esni_blocking/en/
- [51] Kevin Bock, Pranav Bharadwaj, Jasraj Singh, and Dave Levin. 2021. Your Censor is My Censor: Weaponizing Censorship Infrastructure for Availability Attacks. In *Workshop on Offensive Technologies*, IEEE. Retrieved from http://www.cs.umd.edu/~dml/papers/weaponizing_woot21.pdf
- [52] Kevin Bock, Pranav Bharadwaj, Jasraj Singh, and Dave Levin. 2021. Your Censor is My Censor: Weaponizing Censorship Infrastructure for Availability Attacks. In *2021 IEEE Security and Privacy Workshops (SPW)*, IEEE, San Francisco, CA, USA, 398–409. DOI:<https://doi.org/10.1109/SPW53761.2021.00059>
- [53] Kevin Bock, Yair Fax, Kyle Reese, Jasraj Singh, and Dave Levin. 2020. Detecting and Evading Censorship-in-Depth: A Case Study of Iran’s Protocol Filter. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/foci20-paper-bock.pdf>
- [54] Kevin Bock, George Hughey, Louis-Henri Merino, Tania Arya, Daniel Liscinsky, Regina Pogolian, and Dave Levin. 2020. Come as You Are: Helping Unmodified Clients Bypass Censorship with Server-side Evasion. In *SIGCOMM*, ACM. Retrieved from <https://geneva.cs.umd.edu/papers/come-as-you-are.pdf>
- [55] Kevin Bock and Dave Levin. 2020. Automating the censorship arms race. *XRDS: Crossroads, The ACM Magazine for Students* 27, 30–35. Retrieved April 7, 2023 from <https://dl.acm.org/doi/10.1145/3437410>
- [56] Kevin Bock, Gabriel Naval, Kyle Reese, and Dave Levin. 2021. Even Censors Have a Backup: Examining China’s Double HTTPS Censorship Middleboxes. In *Free and Open Communications on the Internet*, ACM. Retrieved from <https://doi.org/10.1145/3473604.3474559>
- [57] Yana Breindl and Joss Wright. 2012. Internet Filtering Trends in Western Liberal Democracies: French and German Regulatory Debates. *Free and Open Communications on the Internet* (2012). Retrieved from <https://www.usenix.org/system/files/conference/foci12/breindl2012foci.pdf>

- [58] Susan W Brenner. 2007. At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. *The journal of criminal law & criminology* 97, (2007), 379–475. Retrieved from <https://www.proquest.com/docview/218442098>
- [59] Davide Brunello, Arturo Filastò, Maria Xynou, and Simone Basso. 2021. Italy blocks Gutenberg book publishing website. *OONI Reports*. Retrieved from <https://ooni.org/post/2021-italy-blocks-gutenberg-book-publishing-website/>
- [60] Axel Bruns, Tim Highfield, and Jean Burgess. 2013. The Arab Spring and Social Media Audiences: English and Arabic Twitter Users and Their Networks. *American Behavioral Scientist* 57, 7 (July 2013), 871–898. DOI:<https://doi.org/10.1177/0002764213479374>
- [61] Tomasz Bujlow, Valentín Carela-Español, and Pere Barlet-Ros. 2015. Independent comparison of popular DPI tools for traffic classification. *Computer Networks* 76, (January 2015), 75–89. DOI:<https://doi.org/10.1016/j.comnet.2014.11.001>
- [62] Sam Burnett and Nick Feamster. 2015. Encore: Lightweight Measurement of Web Censorship with Cross-Origin Requests. In *SIGCOMM*, ACM. Retrieved from <http://conferences.sigcomm.org/sigcomm/2015/pdf/papers/p653.pdf>
- [63] Xiang Cai, Xin Cheng Zhang, Brijesh Joshi, and Rob Johnson. 2012. Touching from a distance: website fingerprinting attacks and defenses. In *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12*, ACM Press, Raleigh, North Carolina, USA, 605. DOI:<https://doi.org/10.1145/2382196.2382260>
- [64] Calipr Networking Group. 2021. ICLab Data. *ICLab*. Retrieved from https://iclab.gitlab.io/post/iclab_data/
- [65] Cormac Callanan, Hein Dries-Ziekenheiner, Alberto Escudero-Pascual, and Robert Guerra. 2010. *Leaping Over the Firewall: A Review of Censorship Circumvention Tools*. Freedom House. Retrieved from https://freedomhouse.org/sites/default/files/2020-02/Archived_Special_Report_FH_Censorship_Circumvention_tools.pdf
- [66] Franco Callegati, Walter Cerroni, and Marco Ramilli. 2009. Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security & Privacy* 7, 1 (January 2009), 78–81. DOI:<https://doi.org/10.1109/MSP.2009.12>
- [67] Baboucarr Ceesay. 2014. Gambia: Government’s internet phobia and censorship. *Africa Review*. Retrieved from <https://web.archive.org/web/20171123161754/africareview.com/News/Gambia-Government-Internet-phobia-and-censorship/-/979180/2261770/-/3uqtqz/-/index.html>
- [68] Censored Planet. Censored Planet. *Censored Planet lab at the University of Michigan*. Retrieved from <https://censoredplanet.org/>
- [69] Censored Planet Lab. Censored Planet Dashboard 20200601-20210531. *Censored Planet lab at the University of Michigan*. Retrieved from <https://dashboard.censoredplanet.org/>

- [70] Center for Human Rights in Iran. 2018. Iran’s Severely Disrupted Internet During Protests: “Websites Hardly Open.” Retrieved from <https://iranhumanrights.org/2018/01/irans-severely-disrupted-internet-during-protests-websites-hardly-open/>
- [71] Abdelberi Chaabane, Terence Chen, Mathieu Cunche, Emiliano De Cristofaro, Arik Friedman, and Mohamed Ali Kaafar. 2014. Censorship in the Wild: Analyzing Internet Filtering in Syria. In *Internet Measurement Conference*, ACM, Vancouver BC Canada. DOI:<https://doi.org/10.1145/2663716.2663720>
- [72] Zimo Chai, Amirhossein Ghafari, and Amir Houmansadr. 2019. On the Importance of Encrypted-SNI (ESNI) to Censorship Circumvention. In *Free and Open Communications on the Internet*, USENIX. Retrieved from https://www.usenix.org/system/files/foci19-paper_chai_update.pdf
- [73] Sze Yiu Chau, Omar Chowdhury, Victor Gonsalves, Huangyi Ge, Weining Yang, Sonia Fahmy, and Ninghui Li. 2018. Adaptive Deterrence of DNS Cache Poisoning. In *Security and Privacy in Communication Networks (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering)*, Springer International Publishing, 171–191. DOI:https://doi.org/10.1007/978-3-030-01704-0_10
- [74] David L. Chaum. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM* 24, 2 (February 1981), 84–90. DOI:<https://doi.org/10.1145/358549.358563>
- [75] Chen Ding, Chi-Hung Chi, Jing Deng, and Chun-Lei Dong. 1999. Centralized content-based Web filtering and blocking: how far can it go? In *IEEE SMC’99 Conference Proceedings. 1999 IEEE International Conference on Systems, Man, and Cybernetics (Cat. No.99CH37028)*, IEEE, Tokyo, Japan, 115–119. DOI:<https://doi.org/10.1109/ICSMC.1999.825218>
- [76] Yulia Cherdantseva and Jeremy Hilton. 2013. A Reference Model of Information Assurance & Security. In *2013 International Conference on Availability, Reliability and Security*, IEEE, Regensburg, Germany, 546–555. DOI:<https://doi.org/10.1109/ARES.2013.72>
- [77] Mariengracia Chirinos, Andrés Azpúrua, Leonid Evdokimov, and Maria Xynou. 2018. The State of Internet Censorship in Venezuela. *OONI Reports*. Retrieved from <https://ooni.org/post/venezuela-internet-censorship/>
- [78] Shinyoung Cho, Rishab Nithyanand, Abbas Razaghpanah, and Phillipa Gill. 2017. A Churn for the Better: Localizing Censorship using Network-level Path Churn and Network Tomography. In *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*, ACM. Retrieved from <https://doi.org/10.1145/3143361.3143386>
- [79] Sang-Hun Choe. 2012. South Korean Court Rejects Online Name Verification Law. *The New York Times*. Retrieved from <https://www.nytimes.com/2012/08/24/world/asia/south-korean-court-overturns-online-name-verification-law.html>

- [80] Catalin Cimpanu. 2022. KlaySwap crypto users lose funds after BGP hijack. *The Record*. Retrieved from <https://therecord.media/klayswap-crypto-users-lose-funds-after-bgp-hijack/>
- [81] CISA. 2009. *Understanding Denial-of-Service Attacks*. U.S. Cybersecurity and Infrastructure Agency. Retrieved from <https://www.cisa.gov/uscert/ncas/tips/ST04-015>
- [82] CISA. 2017. *HIDDEN COBRA – North Korea’s DDoS Botnet Infrastructure*. U.S. Cybersecurity and Infrastructure Agency. Retrieved from <https://www.cisa.gov/uscert/ncas/alerts/TA17-164A>
- [83] J. Clark and P. C. Van Oorschot. 2013. SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements. In *2013 IEEE Symposium on Security and Privacy*, IEEE, Berkeley, CA, 511–525. DOI:<https://doi.org/10.1109/SP.2013.41>
- [84] Mitchell Clark. 2021. What is BGP, and what role did it play in Facebook’s massive outage. *The Verge*. Retrieved from <https://www.theverge.com/2021/10/4/22709260/what-is-bgp-border-gateway-protocol-explainer-internet-facebook-outage>
- [85] Richard A. Clarke and Robert K. Knake. 2012. *Cyber War: the next threat to national security and what to do about it* (1st ed.). Ecco, New York.
- [86] Richard Clayton. 2006. Failures in a Hybrid Content Blocking System. In *Privacy Enhancing Technologies*, Springer, 78–92. Retrieved from <https://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf>
- [87] Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson. 2006. Ignoring the Great Firewall of China. In *Privacy Enhancing Technologies*. Springer Berlin Heidelberg, Berlin, Heidelberg, 20–35. DOI:https://doi.org/10.1007/11957454_2
- [88] Cloudflare. What is BGP? | BGP routing explained. *Cloudflare Blog*. Retrieved from <https://www.cloudflare.com/learning/security/glossary/what-is-bgp/>
- [89] Cloudflare. What is BGP hijacking? *Cloudflare Blog*. Retrieved from <https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/>
- [90] Cloudflare. Famous DDoS attacks | The largest DDoS attacks of all time. *Cloudflare Blog*. Retrieved from <https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/>
- [91] Orazio Coco. 2020. Contemporary China and the “Harmonious” World Order in the Age of Globalization. *Chin. J. Global Gov.* 6, 1 (April 2020), 1–19. DOI:<https://doi.org/10.1163/23525207-12340044>
- [92] Coding Rights, Privacy LatAm and and Privacy International. 2016. *The Right to Privacy in Brazil*. Report, Privacy International. Retrieved from https://privacyinternational.org/sites/default/files/2018-02/UPR27_brazil.pdf

- [93] Bernd Conrad and Fatemah Shirazi. 2014. A Survey on Tor and I2P. In *ICIMP 2014: the Ninth International Conference on Internet Monitoring and Protection*. Paris, France.
- [94] Philip Cook and Conrad Heilmann. 2013. Two Types of Self-Censorship: Public and Private. *Political Studies* 61, 1 (March 2013), 178–196. DOI:<https://doi.org/10.1111/j.1467-9248.2012.00957.x>
- [95] Council on Foreign Relations. 2005. Titan Rain. *Cyber Operations Tracker*. Retrieved from <https://www.cfr.org/cyber-operations/titan-rain>
- [96] Jedidiah R. Crandall, Masashi Crete-Nishihata, and Jeffrey Knockel. 2015. Forgive Us our SYNs: Technical and Ethical Considerations for Measuring Internet Filtering. In *Ethics in Networked Systems Research*, ACM. Retrieved from <https://www.cs.unm.edu/~jeffk/publications/nsethics2015-syns.pdf>
- [97] Jedidiah R. Crandall, Daniel Zinn, Michael Byrd, Earl Barr, and Rich East. 2007. ConceptDoppler: A Weather Tracker for Internet Censorship. In *Computer and Communications Security*, ACM, 352–365. Retrieved from <http://www.csd.uoc.gr/~hy558/papers/conceptdoppler.pdf>
- [98] Abdi Latif Dahir. 2019. After a record 16-month ban, this president has unblocked social media access. *Quartz*. Retrieved from <https://qz.com/africa/1667263/chads-idriss-deby-unblocks-social-media-after-record-shutdown>
- [99] Alberto Dainotti, Claudio Squarcella, Emile Aben, Kimberly C. Claffy, Marco Chiesa, Michele Russo, and Antonio Pescapè. 2011. Analysis of Country-wide Internet Outages Caused by Censorship. In *Internet Measurement Conference*, ACM, 1–18. Retrieved from <http://conferences.sigcomm.org/imc/2011/docs/p1.pdf>
- [100] Jakub Dalek, Bennett Haselton, Helmi Noman, Adam Senft, Masashi Crete-Nishihata, Phillipa Gill, and Ronald J. Deibert. 2013. A method for identifying and confirming the use of URL filtering products for censorship. In *Proceedings of the 2013 conference on Internet measurement conference*, ACM, Barcelona Spain, 23–30. DOI:<https://doi.org/10.1145/2504730.2504763>
- [101] Jakub Dalek and Adam Senft. 2011. Behind Blue Coat: Investigations of commercial filtering in Syria and Burma. *The Citizen Lab - University of Toronto*. Retrieved from <https://citizenlab.ca/2011/11/behind-blue-coat/>
- [102] Alexander Darer, Oliver Farnan, and Joss Wright. 2017. FilteredWeb: A Framework for the Automated Search-Based Discovery of Blocked URLs. In *Network Traffic Measurement and Analysis*, IFIP. Retrieved from http://tma.ifip.org/wordpress/wp-content/uploads/2017/06/tma2017_paper32.pdf
- [103] Shepardson David. 2021. Censorship circumvention tool helps 1.4 million Cubans get internet access. *Reuters*. Retrieved from <https://www.reuters.com/world/americas/censorship-circumvention-tool-helps-14-million-cubans-get-internet-access-2021-07-16/>

- [104] Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, and OpenNet Initiative (Eds.). 2010. *Access controlled: the shaping of power, rights, and rule in cyberspace*. MIT Press, Cambridge, Mass.
- [105] Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, and Janice Stein. 2008. *Access Denied: The Practice and Policy of Global Internet Filtering*. The MIT Press. Retrieved from <https://muse.jhu.edu/book/60844>
- [106] Ronald Deibert, Jonathan Zittrain, Rafal Rohozinski, and John Palfrey (Eds.). 2012. *Access contested: security, identity, and resistance in Asian cyberspace information revolution and global politics*. MIT Press, Cambridge, MA.
- [107] Kevin Michael Deluca. 2016. Weibo, WeChat, and the Transformative Events of Environmental Activism on China’s Wild Public Screens. *International Journal of Communications* 10, (2016).
- [108] Roger Dingledine. 2000. The Free Haven Project: Design and Deployment of an Anonymous Secure Data Haven. Massachusetts Institute of Technology. Retrieved from <https://www.freehaven.net/doc/freehaven.pdf>
- [109] Roger Dingledine and Nick Mathewson. 2006. *Design of a blocking-resistant anonymity system*. Technical Report, Tor Project.
- [110] Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. Tor: The Second-Generation Onion Router. *13th USENIX Security Symposium* (2004).
- [111] Lucas Dixon, Thomas Ristenpart, and Thomas Shrimpton. 2016. Network Traffic Obfuscation and Automated Internet Censorship. *IEEE Secur. Privacy* 14, 6 (November 2016), 43–53. DOI:<https://doi.org/10.1109/MSP.2016.121>
- [112] Ayhan Dolunay, Fevzi Kasap, and Gökçe Keçeci. 2017. Freedom of Mass Communication in the Digital Age in the Case of the Internet: “Freedom House” and the USA Example. *Sustainability* 9, 10 (October 2017), 1739. DOI:<https://doi.org/10.3390/su9101739>
- [113] Jason Donenfeld. 2018. WireGuard - Fast, Modern, Secure VPN Tunnel. In *Black Hat USA*. Black Hat USA. Retrieved from <https://i.blackhat.com/us-18/Wed-August-8/us-18-Donenfeld-WireGuard-Next-Generation-Secure-Network-Tunnel.pdf>
- [114] Jason A Donenfeld. 2020. WireGuard: Next Generation Kernel Network Tunnel. *Distributed System Security Symposium NDSS 2017*, (2020). Retrieved from <https://www.wireguard.com/papers/wireguard.pdf>
- [115] Maximillian Dornseif. 2003. Government mandated blocking of foreign Web content. In *DFN-Arbeitstagung über Kommunikationsnetze*, Gesellschaft für Informatik, 617–647. Retrieved from <https://censorbib.nymity.ch/pdf/Dornseif2003a.pdf>
- [116] Haixin Duan, Nicholas Weaver, Zongxu Zhao, Meng Hu, Jinjin Liang, Jian Jiang, Kang Li, and Vern Paxson. 2012. Hold-On: Protecting Against On-Path DNS Poisoning. In

Securing and Trusting Internet Names, National Physical Laboratory. Retrieved from <https://www.icsi.berkeley.edu/pubs/networking/dns poisoning12.pdf>

- [117] Arun Dunna, Ciarán O'Brien, and Phillipa Gill. 2018. Analyzing China's Blocking of Unpublished Tor Bridges. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/conference/foci18/foci18-paper-dunna.pdf>
- [118] Josiah Dykstra, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. 2022. The Economics of Sharing Unclassified Cyber Threat Intelligence by Government Agencies and Departments. *JIS* 13, 03 (2022), 85–100. DOI:<https://doi.org/10.4236/jis.2022.133006>
- [119] Dynamic Internet Technology. 2014. Freegate: Gateway to free Internet. *DIT*. Retrieved from <http://dit-inc.us/freegate.html>
- [120] Sabrina Earle. 2016. The battle against geo-blocking: the consumer strikes back. *Richmond journal of global law and business* 15, (2016).
- [121] Peter Eckersley. 2010. How Unique Is Your Web Browser? In *Privacy Enhancing Technologies*, Mikhail J. Atallah and Nicholas J. Hopper (eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 1–18. DOI:https://doi.org/10.1007/978-3-642-14527-8_1
- [122] Tariq Elahi and Ian Goldberg. 2012. CORDON - A Taxonomy of Internet Censorship Resistance Strategies. Retrieved from <https://cacr.uwaterloo.ca/techreports/2012/cacr2012-33.pdf>
- [123] Tariq Elahi, Colleen Swanson, and Ian Goldberg. 2015. *Slipping Past the Cordon: A Systematization of Internet Censorship Resistance*. Technical Report.
- [124] Kathrin Elmenhorst, Bertram Schütz, Nils Aschenbruck, and Simone Basso. 2021. Web censorship measurements of HTTP/3 over QUIC. In *Proceedings of the 21st ACM Internet Measurement Conference*, ACM, Virtual Event, 276–282. DOI:<https://doi.org/10.1145/3487552.3487836>
- [125] Paul Emmanuel. 2020. These African countries have various forms of Internet censorship. *Techpoint Africa*. Retrieved from <https://techpoint.africa/2020/05/21/african-countries-censor-internet/>
- [126] T. Enghardt, T. Pauly, C. Perkins, K. Rose, and C. Wood. 2020. RFC 8922: A Survey of the Interaction between Security Protocols and Transport Services. *Internet Engineering Task Force (IETF)*. Retrieved from <https://www.rfc-editor.org/rfc/rfc8922.html>
- [127] Roya Ensafi, David Fifield, Philipp Winter, Nick Feamster, Nicholas Weaver, and Vern Paxson. 2015. Examining How the Great Firewall Discovers Hidden Circumvention Servers. In *Proceedings of the 2015 Internet Measurement Conference*, ACM, Tokyo Japan, 445–458. DOI:<https://doi.org/10.1145/2815675.2815690>

- [128] Roya Ensafi, Philipp Winter, Abdullah Mueen, and Jedidiah R. Crandall. 2015. Analyzing the Great Firewall of China Over Space and Time. *Proceedings on Privacy Enhancing Technologies* 2015, 1 (April 2015), 61–76. DOI:<https://doi.org/10.1515/popets-2015-0005>
- [129] Golnaz Esfandiari. 2013. Iran Admits Throttling Internet To “Preserve Calm” During Election. *Radio Free Europe/Radio Liberty*. Retrieved from <https://www.rferl.org/a/iran-internet-disruptions-election/25028696.html>
- [130] B Evers, J Hols, E Kula, J Schouten, and J A Pouwelse. 2016. *Thirteen Years of Tor Attacks*. Retrieved from <https://github.com/Attacks-on-Tor/Attacks-on-Tor>
- [131] Oliver Farnan, Alexander Darer, and Joss Wright. 2016. Poisoning the Well – Exploring the Great Firewall’s Poisoned DNS Responses. In *Workshop on Privacy in the Electronic Society*, ACM. Retrieved from <https://dl.acm.org/authorize?N25517>
- [132] FCC. 2000. Children’s Internet Protection Act (CIPA). *Federal Communications Commission (FCC)*. Retrieved from <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>
- [133] Federal Court of Australia. 2020. Roadshow Films vs Telstra Corporation. *FCA Digital Library*. Retrieved from <https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2020/2020fca0507>
- [134] Federal Ministry of Justice. 1998. Strafgesetzbuch (German Criminal Code). *Federal Law Gazette I*. Retrieved from https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html
- [135] Steven Feldstein. 2021. *The rise of digital repression: how technology is reshaping power, politics, and resistance*. Oxford University Press, New York, NY.
- [136] Steven Feldstein. 2022. Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond? *Carnegie Endowment for International Peace*. Retrieved from <https://carnegieendowment.org/2022/03/31/government-internet-shutdowns-are-changing.-how-should-citizens-and-democracies-respond-pub-86687>
- [137] Edward W Felten and Michael A Schneider. 2000. Timing Attacks on Web Privacy. *CCS ’00: Proceedings of the 7th ACM conference on Computer and Communications Security* (November 2000).
- [138] Ellis Fenske and Aaron Johnson. 2023. Security Notions for Fully Encrypted Protocols. In *Free and Open Communications on the Internet*, Proceedings on Privacy Enhancing Technologies. Retrieved from <https://www.petsymposium.org/foci/2023/foci-2023-0004.pdf>
- [139] Peter Fettke and Peter Loos (Eds.). 2007. *Reference modeling for business systems analysis*. Idea Group Publishing, Saarbrücken, Germany.

- [140] David Fifield. 2017. Threat modeling and circumvention of Internet censorship. University of California, Berkeley.
- [141] David Fifield, Chang Lan, Rod Hynes, Percy Wegmann, and Vern Paxson. 2015. Blocking-resistant communication through domain fronting. *Proceedings on Privacy Enhancing Technologies* 2015, 2 (June 2015), 46–64. DOI:<https://doi.org/10.1515/popets-2015-0009>
- [142] David Fifield and Lynn Tsai. 2016. Censors’ Delay in Blocking Circumvention Proxies. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/conference/foci16/foci16-paper-fifield.pdf>
- [143] Arturo Filastò and Jacob Appelbaum. 2012. OONI: Open Observatory of Network Interference. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/conference/foci12/foci12-final12.pdf>
- [144] Arturo Filastò, Arthur Gwagwa, and Maria Xynou. 2016. The Gambia: Internet Shutdown during 2016 Presidential Election. *OONI Reports*. Retrieved from <https://ooni.org/post/gambia-internet-shutdown/>
- [145] Eric Filiol, Maxence Delong, and J. Nicolas. 2020. Statistical and combinatorial analysis of the TOR routing protocol: structural weaknesses identified in the TOR network. *J Comput Virol Hack Tech* 16, 1 (March 2020), 3–18. DOI:<https://doi.org/10.1007/s11416-019-00334-x>
- [146] Arlene Fink. 2005. *Conducting research literature reviews: from the Internet to paper* (2nd ed ed.). Sage Publications, Thousand Oaks, CA.
- [147] FireninjaDD. 2017. Will using a VPN prevent ISP throttling due to the removal of Net Neutrality? *Reddit*. Retrieved from https://www.reddit.com/r/technology/comments/6c1kck/will_using_a_vpn_prevent_isp_throttling_due_to/
- [148] Eric Fish. 2009. Is Internet Censorship Compatible with Democracy? Legal Restrictions of Online Speech in South Korea. *Asia-Pacific Journal on Human Rights and the Law* 10, 2 (2009), 43–96. DOI:<https://doi.org/10.1163/138819010X12647506166519>
- [149] Terry Fletcher and Andria Hayes-Birchler. 2020. Comparing Measures of Internet Censorship: Analyzing the Tradeoffs between Expert Analysis and Remote Measurement. *Data For Policy* 2020 (July 2020). DOI:<https://doi.org/10.5281/ZENODO.3967397>
- [150] Andrea Di Florio, Nino Vincenzo Verde, Antonio Villani, Domenico Vitali, and Luigi Vincenzo Mancini. 2014. Bypassing Censorship: A Proven Tool against the Recent Internet Censorship in Turkey. In *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, IEEE, Naples, Italy, 389–394. DOI:<https://doi.org/10.1109/ISSREW.2014.93>

- [151] Forcepoint. 2023. Protocol Agents on NGFW Engines. *NGFW 7.0 Online Help*. Retrieved February 15, 2023 from <https://help.forcepoint.com/ngfw/en-us/7.0.0/GUID-8A8FD672-D113-4D47-945A-46298F96C0F9.html>
- [152] Fortinet. FortiOS 7.0.1 Administration Guide. *Blocking applications with custom signatures*. Retrieved February 15, 2023 from <https://docs.fortinet.com/document/fortigate/7.0.1/administration-guide/233445/blocking-applications-with-custom-signatures>
- [153] France 24. 2010. 5,000 arrested in China for Internet pornography last year. *France 24*. Retrieved from <https://www.france24.com/en/20100101-5000-arrested-china-internet-pornography-last-year>
- [154] Nana Fredua-Agyeman. 2012. #BannedAfricanBooks: List of Banned African Books. *ImageNations - Promoting African Literature*. Retrieved from <https://freduagyeman.blogspot.com/2012/11/bannedafricanbooks-list-of-banned.html>
- [155] Freedom House. 2021. Freedom on the Net 2021 - The Gambia. *freedomhouse.org*. Retrieved from <https://freedomhouse.org/country/gambia/freedom-net/2021>
- [156] Freedom House. 2021. Freedom on the Net 2021 - Venezuela. *freedomhouse.org*. Retrieved from <https://freedomhouse.org/country/venezuela/freedom-net/2021>
- [157] Freedom House. 2021. Freedom on the Net 2021 - Russia. *freedomhouse.org*. Retrieved from <https://freedomhouse.org/country/russia/freedom-net/2021>
- [158] Freedom House. 2021. Freedom on the Net 2021 - Singapore. *freedomhouse.org*. Retrieved from <https://freedomhouse.org/country/singapore/freedom-net/2021>
- [159] Freedom House. 2021. Freedom on the Net 2021 - Kenya. *freedomhouse.org*. Retrieved from <https://freedomhouse.org/country/kenya/freedom-net/2021>
- [160] Freedom House. 2021. Freedom on the Net 2021 - United Kingdom. *freedomhouse.org*. Retrieved from <https://freedomhouse.org/country/united-kingdom/freedom-net/2021>
- [161] Freedom House. 2021. Freedom on the Net 2021 - Germany. *freedomhouse.org*. Retrieved from <https://freedomhouse.org/country/germany/freedom-net/2021>
- [162] Freedom House. 2021. Freedom on the Net 2021 - Canada. *freedomhouse.org*. Retrieved from <https://freedomhouse.org/country/canada/freedom-net/2021>
- [163] Freedom House. Freedom on the Net - Annual Report. *Freedom House*. Retrieved from <https://freedomhouse.org/report/freedom-net>
- [164] Freedom House. Freedom on the Net 2021 - China. *Freedom House*. Retrieved from <https://freedomhouse.org/country/china/freedom-net/2021>

- [165] Sergey Frolov. 2020. Practical Countermeasures against Network Censorship. Dissertation. University of Colorado, Boulder, CO. Retrieved from <https://scholar.colorado.edu/downloads/mg74qn240>
- [166] Sergey Frolov, Jack Wampler, and Eric Wustrow. 2020. Detecting Probe-resistant Proxies. In *Network and Distributed System Security*, The Internet Society. Retrieved from <https://www.ndss-symposium.org/wp-content/uploads/2020/02/23087.pdf>
- [167] Sergey Frolov and Eric Wustrow. 2019. The use of TLS in Censorship Circumvention. In *Network and Distributed System Security*, The Internet Society. Retrieved from <https://tlsfingerprint.io/static/frolov2019.pdf>
- [168] Sergey Frolov and Eric Wustrow. 2020. HTTPPT: A Probe-Resistant Proxy. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/foci20-paper-frolov.pdf>
- [169] FTC. 1998. Children’s Online Privacy Protection Rule (“COPPA”). *Federal Trade Commission (FTC)*. Retrieved from <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>
- [170] Christian Fuchs and Daniel Trottier. 2017. Internet surveillance after Snowden: A critical empirical study of computer experts’ attitudes on commercial and state surveillance of the Internet and social media post-Edward Snowden. *JICES* 15, 4 (December 2017), 412–444. DOI:<https://doi.org/10.1108/JICES-01-2016-0004>
- [171] Iginio Gagliardone and Frederick Golooba-Mutebi. 2016. The Evolution of the Internet in Ethiopia and Rwanda: Towards a “Developmental” Model? *Stability: International Journal of Security and Development* 5, 1 (August 2016), 8. DOI:<https://doi.org/10.5334/sta.344>
- [172] Raphael Garcia. 2019. Internet Censorship is Part of South Korea’s Democracy Package. *The News Lens*. Retrieved from <https://international.thenewslens.com/article/122579>
- [173] Frank Gardner. 2000. Saudis “defeating” internet porn. *British Broadcasting Corporation (BBC)*. Retrieved from http://news.bbc.co.uk/2/hi/middle_east/742798.stm
- [174] Richard Gartner. 2016. *Metadata*. Springer International Publishing, University of London, UK. DOI:<https://doi.org/10.1007/978-3-319-40893-4>
- [175] Jodesz Gavilan. 2022. Cyberattack hits CNN Philippines on day of presidential debate. *Rappler*. Retrieved from <https://www.rappler.com/nation/cyberattack-hits-cnn-philippines-presidential-debate-february-27-2022/>
- [176] Genevieve Gebhart and Tadayoshi Kohno. 2017. Internet Censorship in Thailand: User Practices and Potential Threats. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, Paris, 417–432. DOI:<https://doi.org/10.1109/EuroSP.2017.50>

- [177] Arzu Geybullayeva, Maria Xynou, and Arturo Filastò. 2021. Media censorship in Azerbaijan through the lens of network measurement. *OONI Reports*. Retrieved from <https://ooni.org/post/2021-azerbaijan/>
- [178] Alessandro Ghedini. 2018. Encrypt it or lose it: how encrypted SNI works. *The Cloudflare Blog*. Retrieved from <https://blog.cloudflare.com/encrypted-sni/>
- [179] Phillipa Gill, Masashi Crete-Nishihata, Jakub Dalek, Sharon Goldberg, Adam Senft, and Greg Wiseman. 2015. Characterizing Web Censorship Worldwide: Another Look at the OpenNet Initiative Data. *ACM Transactions on the Web* 9, 1 (2015). Retrieved from <https://censorbib.nymity.ch/pdf/Gill2015a.pdf>
- [180] Ian Goldberg. 2000. A pseudonymous communications infrastructure for the Internet. PhD Dissertation. University of California, Berkley.
- [181] Paul Goldstein. 2008. Fair use in context. *The Columbia journal of law & the arts* 31, 4 (2008).
- [182] GoodbyeDPI. GoodbyeDPI — Deep Packet Inspection circumvention utility. *Github*. Retrieved from <https://github.com/ValdikSS/GoodbyeDPI>
- [183] Google. 2017. HTTPS encryption on the web. *Google Transparency Report*. Retrieved from [HTTPS encryption on the web](https://transparencyreport.google.com/https-encryption)
- [184] Devashish Gosain, Anshika Agarwal, Sahil Shekhawat, H. B. Acharya, and S. Chakravarty. 2018. Mending Wall: On the Implementation of Censorship in India. *arXiv:1806.06518 [cs]* (June 2018). Retrieved October 13, 2021 from <http://arxiv.org/abs/1806.06518>
- [185] Devashish Gosain, Mayank Mohindra, and Sambuddho Chakravarty. 2021. Too Close for Comfort: Morasses of (Anti-) Censorship in the Era of CDNs. *Proceedings on Privacy Enhancing Technologies* 2021, 2 (April 2021), 173–193. DOI:<https://doi.org/10.2478/popets-2021-0023>
- [186] James A. Green (Ed.). 2015. *Cyber warfare: a multidisciplinary analysis*. Routledge, Abingdon, Oxon ; New York, NY.
- [187] Glenn Greenwald. 2014. Exclusive: Snowden Docs Show UK Spies Attacked Anonymous, Hackers. *NBC News*. Retrieved from <https://www.nbcnews.com/feature/edward-snowdeninterview/exclusive-snowden-docs-show-uk-spies-attacked-anonymous-hackers-n21361>
- [188] Giovanni De Gregorio. 2020. Internet Shutdowns and the Limits of Law. *International Journal of Communication* (2020). Retrieved from <https://ijoc.org/index.php/ijoc/article/view/13752/3183>

- [189] Gurshabad Grover and Kushagra Singh. 2019. Reliance Jio is using SNI inspection to block websites. *The Center for Internet & Society, India*. Retrieved from <https://cis-india.org/internet-governance/blog/reliance-jio-is-using-sni-inspection-to-block-websites>
- [190] Brynjólfur Þór Guðmundsson. 2015. Gangi ekki upp nema of langt sé gengið [Doesn't work unless you go too far]. *RÚV*. Retrieved from <https://www.ruv.is/frettir/innlent/gangi-ekki-upp-nema-of-langt-se-gengid>
- [191] Peter Guest. 2022. “It’s like being under siege”: How DDoS became a censorship tool. *Rest of World: Reporting Global Tech Stories*. Retrieved from <https://restofworld.org/2022/blackouts-ddos/>
- [192] Hacker Target. 2022. WHOIS ASN IP Lookup Tool. *Hacker Target*. Retrieved from <https://hackertarget.com/as-ip-lookup/>
- [193] Hall et al. 2022. A Survey of Worldwide Censorship Techniques (Draft in progress). *Internet Engineering Task Force (IETF)*. Retrieved December 1, 2022 from <https://datatracker.ietf.org/doc/draft-irtf-pearg-censorship/08/>
- [194] Alexis Hancock. 2021. HTTPS Is Actually Everywhere. *Electronic Frontier Foundation (EFF)*. Retrieved from <https://www.eff.org/deeplinks/2021/09/https-actually-everywhere>
- [195] Michael Harrity, Kevin Bock, Frederick Sell, and Dave Levin. 2022. GET /out: Automated Discovery of Application-Layer Censorship Evasion Strategies. *USENIX Security Symposium (2022)*. Retrieved from <https://www.usenix.org/system/files/sec22-harrity.pdf>
- [196] Shaddi Hasan, Yahel Ben-David, Giulia Fanti, Eric Brewer, and Scott Shenker. 2013. Building Dissent Networks: Towards Effective Countermeasures against Large-Scale Communications Blackouts. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://censorbib.nymity.ch/pdf/Hasan2013a.pdf>
- [197] Jamie Hayes. 2016. Traffic Confirmation Attacks Despite Noise. *arXiv:1601.04893 [cs]* (February 2016). Retrieved October 24, 2021 from <http://arxiv.org/abs/1601.04893>
- [198] Gaofeng He, Ming Yang, Junzhou Luo, and Xiaodan Gu. 2015. A novel application classification attack against Tor: A novel application classification attack against Tor. *Concurrency and Computation: Practice and Experience* 27, 18 (December 2015), 5640–5661. DOI:<https://doi.org/10.1002/cpe.3593>
- [199] Rebecca Hersher. 2015. Meet Mafiaboy, The “Bratty Kid” Who Took Down The Internet. *NPR: All Tech Considered*. Retrieved from <https://www.npr.org/sections/alltechconsidered/2015/02/07/384567322/meet-mafiaboy-the-bratty-kid-who-took-down-the-internet>
- [200] Andrew Hintz. 2003. Fingerprinting Websites Using Traffic Analysis. In *Privacy Enhancing Technologies*, Roger Dingledine and Paul Syverson (eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 171–178. DOI:https://doi.org/10.1007/3-540-36467-6_13

- [201] Ming-Syuan Ho. 2018. *Taiwan Internet Transparency Report*. Taiwan Association for Human Rights, Taiwan. Retrieved from http://transparency.tahr.org.tw/TITR_Report_2018_en.pdf
- [202] Nguyen Phong Hoang, Arian Akhavan Niaki, Jakub Dalek, Jeffrey Knockel, Pellaeon Lin, Bill Marczak, Masashi Crete-Nishihata, Phillipa Gill, and Michalis Polychronakis. 2007. *How Great is the Great Firewall? Measuring China's DNS Censorship*. New York University, Technical Report, New York University. Retrieved from <https://www.usenix.org/system/files/sec21-hoang.pdf>
- [203] Nguyen Phong Hoang, Arian Akhavan Niaki, Jakub Dalek, Jeffrey Knockel, Pellaeon Lin, Bill Marczak, Masashi Crete-Nishihata, Phillipa Gill, and Michalis Polychronakis. 2021. How Great is the Great Firewall? Measuring China's DNS Censorship. In *USENIX Security Symposium*, USENIX. Retrieved from <https://www.usenix.org/system/files/sec21-hoang.pdf>
- [204] Nguyen Phong Hoang, Michalis Polychronakis, and Phillipa Gill. 2022. Measuring the Accessibility of Domain Name Encryption and Its Impact on Internet Filtering. In *Passive and Active Measurement Conference*, Springer, 518–536. Retrieved from <https://www3.cs.stonybrook.edu/~mikepo/papers/dneye.pam22.pdf>
- [205] John Holowczak and Amir Houmansadr. 2015. CacheBrowser: Bypassing Chinese Censorship without Proxies Using Cached Content. In *Computer and Communications Security*, ACM. Retrieved from <https://people.cs.umass.edu/~amir/papers/CacheBrowser.pdf>
- [206] John Horton. 2011. Self-Censorship. *Res Publica* 17, 1 (February 2011), 91–106. DOI:<https://doi.org/10.1007/s11158-011-9145-3>
- [207] A. Houmansadr, C. Brubaker, and V. Shmatikov. 2013. The Parrot Is Dead: Observing Unobservable Network Communications. In *2013 IEEE Symposium on Security and Privacy*, IEEE, Berkeley, CA, 65–79. DOI:<https://doi.org/10.1109/SP.2013.14>
- [208] Jinling Hua and Rajib Shaw. 2020. Corona Virus (COVID-19) “Infodemic” and Emerging Issues through a Data Lens: The Case of China. *IJERPH* 17, 7 (March 2020), 2309. DOI:<https://doi.org/10.3390/ijerph17072309>
- [209] Diana L. Huete Trujillo and Antonio Ruiz-Martínez. 2021. Tor Hidden Services: A Systematic Literature Review. *Journal of Cybersecurity and Privacy* 1, 3 (September 2021), 496–518. DOI:<https://doi.org/10.3390/jcp1030025>
- [210] Human Rights Council, United Nations. 2020. *General comment No. 37 (2020) on the right of peaceful assembly (article 21)*. Retrieved from <https://digitallibrary.un.org/record/3884725?ln=en>
- [211] Human Rights Council, United Nations. 2021. *Ending Internet shutdowns: a path forward*. Retrieved from <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/149/66/PDF/G2114966.pdf?OpenElement>

- [212] Human Rights Watch. 2006. “*Race to the Bottom*” *Corporate Complicity in Chinese Internet Censorship*. Technical Report. Retrieved from <https://www.hrw.org/reports/2006/china0806/china0806webwcover.pdf>
- [213] Chris Hunt and Micah Rankin. 2015. R. v. Spencer: Anonymity, the Rule of Law, and the Shrivelling of the Biographical Core. *McGill Law Journal* 61, 1 (September 2015). Retrieved from <https://lawjournal.mcgill.ca/article/r-v-spencer-anonymity-the-rule-of-law-and-the-shrivelling-of-the-biographical-core/>
- [214] Troy Hunt and Scott Helme. 2021. Why No HTTPS? *Why No HTTPS?* Retrieved November 14, 2022 from <https://whynohttps.com/>
- [215] ICMEC. 2021. The Growing Global Threat of Child Sexual Abuse Material (CSAM). *International Centre for Missing & Exploited Children*. Retrieved from <https://icmec.org.au/blog/the-growing-global-threat-of-child-sexual-abuse-material-csam/>
- [216] Internet Security Research Group. Let’s Encrypt. *Let’s Encrypt*. Retrieved from <https://letsencrypt.org/>
- [217] Internet Society. Internet Society Pulse - Internet Shutdown Tracker 2020-2021. *Internet Society*. Retrieved from <https://pulse.internetsociety.org/shutdowns>
- [218] INVISV. 2022. INVISV Relay. *INVISV*. Retrieved from <https://invisv.com/relay/>
- [219] Gunnar Eyal Wolf Iszaevich. 2019. Distributed Detection of Tor Directory Authorities Censorship in Mexico. In *International Conference on Networks*, IARIA. Retrieved from https://tics.site/proceedings/2019a/icn_2019_6_20_38010.pdf
- [220] Kevin Jacobs. 2021. Encrypted Client Hello: the future of ESNI in Firefox. *Mozilla Security Blog*. Retrieved from <https://blog.mozilla.org/security/2021/01/07/encrypted-client-hello-the-future-of-esni-in-firefox/>
- [221] Sune K. Jakobsen and Claudio Orlandi. 2016. How To Bootstrap Anonymous Communication. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science*, ACM, Cambridge Massachusetts USA, 333–344. DOI:<https://doi.org/10.1145/2840728.2840743>
- [222] Markus Jakobsson. 1998. A practical mix. In *Advances in Cryptology - EUROCRYPT’98*, Kaisa Nyberg (ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 448–461. DOI:<https://doi.org/10.1007/BFb0054145>
- [223] Santosh Janardhan. 2021. More details about the October 4 outage. *Engineering at Meta*. Retrieved from <https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/>
- [224] Andrea Januta and Minami Funakoshi. 2021. Myanmar’s internet suppression. *Reuters*. Retrieved from <https://www.reuters.com/graphics/MYANMAR-POLITICS/INTERNET-RESTRICTION/rlgpdbreepo/>

- [225] Kalervo Järvelin and T.D. Wilson. 2003. On conceptual models for information seeking and retrieval research. *Information Research* 9, 1 (2003). Retrieved from <https://informationr.net/ir/9-1/paper163.html>
- [226] Jill Jermyn and Nicholas Weaver. 2017. Autosonda: Discovering Rules and Triggers of Censorship Devices. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/conference/foci17/foci17-paper-jermyn.pdf>
- [227] JHU. 2014. The Johns Hopkins Foreign Affairs Symposium Presents: The Price of Privacy: Re-Evaluating the NSA. *YouTube*. Retrieved from <https://youtu.be/kV2HDM86XgI?t=1072>
- [228] Yaoqi Jia, Xinshu Dong, Zhenkai Liang, and Prateek Saxena. 2015. I Know Where You've Been: Geo-Inference Attacks via the Browser Cache. *IEEE Internet Comput.* 19, 1 (January 2015), 44–53. DOI:<https://doi.org/10.1109/MIC.2014.103>
- [229] Lin Jin, Shuai Hao, Haining Wang, and Chase Cotton. 2021. Understanding the Practices of Global Censorship through Accurate, End-to-End Measurements. *Proc. ACM Meas. Anal. Comput. Syst.* 5, 3 (December 2021), 1–25. DOI:<https://doi.org/10.1145/3491055>
- [230] Ansong Joana. 2020. Pooling samples boosts Ghana's COVID-19 testing. *World Health Organization (Who) Africa*. Retrieved from <https://www.afro.who.int/news/pooling-samples-boosts-ghanas-covid-19-testing>
- [231] Ben Jones, Roya Ensafi, Nick Feamster, Vern Paxson, and Nick Weaver. 2015. Ethical Concerns for Censorship Measurement. In *Proceedings of the 2015 ACM SIGCOMM Workshop on Ethics in Networked Systems Research*, ACM, London United Kingdom, 17–19. DOI:<https://doi.org/10.1145/2793013.2793015>
- [232] Ben Jones and Nick Feamster. 2015. Can Censorship Measurements Be Safe(r)? In *HotNets '15*, ACM. Retrieved from <http://conferences.sigcomm.org/hotnets/2015/papers/jones.pdf>
- [233] Ben Jones, Tzu-Wen Lee, Nick Feamster, and Phillipa Gill. 2014. Automated Detection and Fingerprinting of Censorship Block Pages. In *Proceedings of the Internet Measurement Conference 2014*, ACM, Vancouver BC Canada, 299–304. DOI:<https://doi.org/10.1145/2663716.2663722>
- [234] Kadak. 2018. How to Block Traffic Based on Application Filters with an Exception. *Palo Alto Networks: Customer Support Portal*. Retrieved from <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIXfCAK>
- [235] Cecilia Kang, Davey Alba, and Adam Satariano. 2020. Surging Traffic Is Slowing Down Our Internet. *The New York Times*. Retrieved from <https://www.nytimes.com/2020/03/26/business/coronavirus-internet-traffic-speed.html>

- [236] David Kanouse. 1984. Explaining Negativity Biases in Evaluation and Choice Behavior: Theory and Research. *Advances in Consumer Research* 11, (1984), 703–708. Retrieved from <https://www.acrwebsite.org/volumes/6335/>
- [237] Nikolaos Karapanos and Srdjan Capkun. 2014. On the Effective Prevention of TLS Man-In-The-Middle Attacks in Web Applications. *USENIX Security Symposium* (2014). Retrieved from <https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-karapanos.pdf>
- [238] Simin Kargar and Keith McManamen. 2018. Censorship and Collateral Damage: Analyzing the Telegram Ban in Iran. *SSRN Journal* (2018). DOI:<https://doi.org/10.2139/ssrn.3244046>
- [239] Ishan Karunanayake, Nadeem Ahmed, Robert Malaney, Rafiqul Islam, and Sanjay K. Jha. 2021. De-Anonymisation Attacks on Tor: A Survey. *IEEE Commun. Surv. Tutorials* 23, 4 (2021), 2324–2350. DOI:<https://doi.org/10.1109/COMST.2021.3093615>
- [240] Lukas Kawerau, Nils B. Weidmann, and Alberto Dainotti. 2023. Attack or Block? Repertoires of Digital Censorship in Autocracies. *Journal of Information Technology & Politics* 20, 1 (January 2023), 60–73. DOI:<https://doi.org/10.1080/19331681.2022.2037118>
- [241] David Kaye. 2015. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. United Nations. Retrieved from <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf>
- [242] Alexander Kentikelenis and Erik Voeten. 2021. Legitimacy challenges to the liberal world order: Evidence from United Nations speeches, 1970–2018. *The Review of International Organizations* 16, 4 (October 2021), 721–754. DOI:<https://doi.org/10.1007/s11558-020-09404-y>
- [243] James Khan. 2017. A Study in Protocol Obfuscation Techniques and their Effectiveness. Masters Thesis. University of Oxford. Retrieved July 15, 2022 from <https://doi.org/10.13140/RG.2.2.14167.32165>
- [244] Mohammad Taha Khan, Joe DeBlasio, Geoffrey M. Voelker, Alex C. Snoeren, Chris Kanich, and Narseo Vallina-Rodriguez. 2018. An Empirical Analysis of the Commercial VPN Ecosystem. In *Proceedings of the Internet Measurement Conference 2018*, ACM, Boston MA USA, 443–456. DOI:<https://doi.org/10.1145/3278532.3278570>
- [245] Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M. Swanson, Steven J. Murdoch, and Ian Goldberg. 2016. SoK: Making Sense of Censorship Resistance Systems. *Proceedings on Privacy Enhancing Technologies* 2016, 4 (October 2016), 37–61. DOI:<https://doi.org/10.1515/popets-2016-0028>
- [246] Sheharbano Khattak, David Fifield, Sadia Afroz, Mobin Javed, Srikanth Sundaresan, Vern Paxson, Steven J. Murdoch, and Damon McCoy. 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.
DOI:<https://doi.org/10.14722/ndss.2016.23342>
- [247] Sheharbano Khattak, Mobin Javed, Syed Ali Khayam, Zartash Afzal Uzmi, and Vern Paxson. 2014. A Look at the Consequences of Internet Censorship Through an ISP Lens. In *Internet Measurement Conference*, ACM. Retrieved from <http://conferences2.sigcomm.org/imc/2014/papers/p271.pdf>
- [248] Aminollah Khormali, Jeman Park, Hisham Alasmay, Afsah Anwar, Muhammad Saad, and David Mohaisen. 2021. Domain name system security and privacy: A contemporary survey. *Computer Networks* 185, (February 2021), 107699. DOI:<https://doi.org/10.1016/j.comnet.2020.107699>
- [249] Gary King, Jennifer Pan, and Margaret E. Roberts. 2012. How Censorship in China Allows Government Criticism but Silences Collective Expression. *American Political Science Review* (2012). Retrieved from <https://gking.harvard.edu/files/censored.pdf>
- [250] Gary King, Jennifer Pan, and Margaret E. Roberts. 2014. Reverse-engineering censorship in China: Randomized experimentation and participant observation. *Science* 345, 6199 (2014). Retrieved from <http://cryptome.org/2014/08/reverse-eng-cn-censorship.pdf>
- [251] Francesca Klug, Keir Starmer, and Stuart Weir. 1996. *The three pillars of liberty: political rights and freedoms in the United Kingdom*. New York : Routledge, London.
- [252] Jeffrey Knockel, Masashi Crete-Nishihata, Jason Q. Ng, Adam Senft, and Jedidiah R. Crandall. 2015. Every Rose Has Its Thorn: Censorship and Surveillance on Social Video Platforms in China. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/conference/foci15/foci15-paper-knockel.pdf>
- [253] Jeffrey Knockel and Lotus Ruan. 2021. Measuring QQMail’s Automated Email Censorship in China. In *Free and Open Communications on the Internet*, ACM. Retrieved from <https://doi.org/10.1145/3473604.3474560>
- [254] Jeff Kosseff. 2019. *The twenty-six words that created the Internet*. Cornell University Press, Ithaca, New York.
- [255] Jeff Kosseff. 2022. *The United States of Anonymous: How the First Amendment Shaped Online Speech*. Cornell University Press, Ithaca, New York.
- [256] Zhanna Kozhamberdiyeva. 2008. Freedom of Expression on the Internet: A Case Study of Uzbekistan. *Review of Central and East European Law* 33, 1 (2008). DOI:<https://doi.org/10.1163/092598808X262542>
- [257] Carmen Kwan, Paul Janiszewski, Shela Qiu, Cathy Wang, and Cecylia Bocovich. 2021. Exploring Simple Detection Techniques for DNS-over-HTTPS Tunnels. In *Free and Open Communications on the Internet*, ACM. Retrieved from <https://doi.org/10.1145/3473604.3474563>

- [258] Lantern. Get Lantern. *Lantern*. Retrieved from https://getlantern.org/en_US/index.html
- [259] Pierre Laperdrix, Nataliia Bielova, Benoit Baudry, and Gildas Avoine. 2020. Browser Fingerprinting: A Survey. *ACM Trans. Web* 14, 2 (May 2020), 1–33. DOI:<https://doi.org/10.1145/3386040>
- [260] Christopher S. Leberknight, Mung Chiang, and Felix Ming Fai Wong. 2012. A Taxonomy of Censors and Anti-Censors: Part I-Impacts of Internet Censorship. *International Journal of E-Politics* 3, 2 (2012), 52–64. DOI:<https://doi.org/10.4018/jep.2012040104>
- [261] Christopher S. Leberknight, Mung Chiang, and Felix Ming Fai Wong. 2012. A Taxonomy of Censors and Anti-Censors Part II: Anti-Censorship Technologies. *International Journal of E-Politics* 3, 4 (2012), 20–35. DOI:<https://doi.org/10.4018/jep.2012100102>
- [262] Douglas J. Leith. 2021. Web Browser Privacy: What Do Browsers Say When They Phone Home? *IEEE Access* 9, (March 2021), 41615–41627. DOI:<https://doi.org/10.1109/ACCESS.2021.3065243>
- [263] Let’s Encrypt. 2021. Let’s Encrypt Statistics. *Firefox Telemetry*. Retrieved from <https://letsencrypt.org/stats/>
- [264] Wilson Lian, Eric Rescorla, Hovav Shacham, and Stefan Savage. 2013. Measuring the practical impact of DNSSEC Deployment. *USENIX Security Symposium* (August 2013).
- [265] Patrick Lincoln, Ian Mason, Phillip Porras, Vinod Yegneswaran, Zachary Weinberg, Jeroen Massar, William Simpson, Paul Vixie, and Dan Boneh. 2012. Bootstrapping Communications into an Anti-Censorship System. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/conference/foci12/foci12-final7.pdf>
- [266] Natasha Lomas. 2020. Germany tightens online hate speech rules to make platforms send reports straight to the feds. *TechCrunch*. Retrieved from <https://techcrunch.com/2020/06/19/germany-tightens-online-hate-speech-rules-to-make-platforms-send-reports-straight-to-the-feds/>
- [267] G. Loukas and G. Oke. 2010. Protection Against Denial of Service Attacks: A Survey. *The Computer Journal* 53, 7 (September 2010), 1020–1037. DOI:<https://doi.org/10.1093/comjnl/bxp078>
- [268] Graham Lowe, Patrick Winters, and Michael L Marcus. 2007. *The Great DNS Wall of China*. New York University, Technical Report, New York University. Retrieved from <https://censorbib.nymity.ch/pdf/Lowe2007a.pdf>
- [269] Zhen Lu, Zhenhua Li, Jian Yang, Tianyin Xu, Ennan Zhai, Yao Liu, and Christo Wilson. 2017. Accessing Google Scholar under Extreme Internet Censorship: A Legal Avenue. In *Middleware*, ACM. Retrieved from <https://censorbib.nymity.ch/pdf/Lu2017a.pdf>

- [270] Philipp M. Lutscher, Nils B. Weidmann, Margaret E. Roberts, Mattijs Jonker, Alistair King, and Alberto Dainotti. 2020. At Home and Abroad: The Use of Denial-of-service Attacks during Elections in Nondemocratic Regimes. *Journal of Conflict Resolution* 64, 2–3 (February 2020), 373–401. DOI:<https://doi.org/10.1177/0022002719861676>
- [271] J. Lyengar and M. Thomson. 2021. RFC 9000: A UDP-Based Multiplexed and Secure Transport. *Internet Engineering Task Force (IETF)*. Retrieved from <https://doi.org/10.17487/RFC9000>
- [272] Ryan Macasero. 2020. Signal shutdown to proceed during Sinulog 2020 events. *Rappler*. Retrieved from <https://www.rappler.com/nation/249581-signal-shutdown-sinulog-2020/>
- [273] Tasnuva Mahjabin, Yang Xiao, Guang Sun, and Wangdong Jiang. 2017. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks* 13, 12 (December 2017), 155014771774146. DOI:<https://doi.org/10.1177/1550147717741463>
- [274] Imran Makhdoom, Mehran Abolhasan, and Justin Lipman. 2022. A comprehensive survey of covert communication techniques, limitations and future challenges. *Computers & Security* 120, (September 2022). DOI:<https://doi.org/10.1016/j.cose.2022.102784>
- [275] Michael Malakata. 2011. Malawi blocks social media networks to quell protests. *Computer World*. Retrieved from <https://web.archive.org/web/20110726185847/http://news.idg.no/cw/art.cfm?id=3DFADEBE-1A64-67EA-E44251D79A4C6F57>
- [276] Mousa Taghizadeh Manavi. 2018. Defense mechanisms against Distributed Denial of Service attacks : A survey. *Computers & Electrical Engineering* 72, (November 2018), 26–38. DOI:<https://doi.org/10.1016/j.compeleceng.2018.09.001>
- [277] Antonio Mangino and Elias Bou-Harb. 2021. A Multidimensional Network Forensics Investigation of a State-Sanctioned Internet Outage. In *2021 International Wireless Communications and Mobile Computing (IWCMC)*, IEEE, Harbin City, China, 813–818. DOI:<https://doi.org/10.1109/IWCMC51323.2021.9498743>
- [278] Eleanor Marchant and Nicole Stremmlau. 2020. The Changing Landscape of Internet Shutdowns in Africa. *International Journal of Communication* 14, (2020). Retrieved from <https://ijoc.org/index.php/ijoc/article/view/11490/3182>
- [279] Bill Marczak, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ron Deibert, and Vern Paxson. 2015. An Analysis of China’s “Great Cannon.” In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/conference/foci15/foci15-paper-marczak.pdf>
- [280] Samvel Martirosyan. 2021. The main issues of Internet freedom in Armenia (in Armenian). *Media.am*. Retrieved from <https://media.am/hy/critique/2021/01/18/25891/>

- [281] L. Masinter and M. McCahill. 1994. RFC 1738: Uniform Resource Locators (URL). *Internet Engineering Task Force (IETF)*. Retrieved from <https://datatracker.ietf.org/doc/html/rfc1738>
- [282] Alexander Master. 2022. Threat Modeling Internet Censorship: Towards Evaluation of Managed Attribution Software. In *AvengerCon VII*. Fort Meade, MD. Retrieved from <https://www.dvidshub.net/video/870218/avengercon-vii-threat-modeling-internet-censorship-towards-evaluation-managed-attribution-software>
- [283] Alexander Master. 2023. Modeling and Characterization of Internet Censorship Technologies. Dissertation. Purdue University, West Lafayette, IN.
- [284] Alexander Master and Christina Garman. 2021. *A WireGuard Exploration*. Purdue University, West Lafayette, IN. DOI:<https://doi.org/10.5703/1288284317610>
- [285] Alexander Master and Christina Garman. 2023. Investigating Nation-state Internet Censorship Methods. In *Purdue CERIAS Security Symposium*. West Lafayette, IN. Retrieved from <https://www.cerias.purdue.edu/symposium/index.php/posters/year/2023/E29-885>
- [286] Alexander Master and Christina Garman. 2023. A Worldwide View of Nation-state Internet Censorship. In *Free and Open Communications on the Internet*, Proceedings on Privacy Enhancing Technologies. Retrieved from <https://www.petsymposium.org/foci/2023/foci-2023-0008.pdf>
- [287] Alexander Master, George Hamilton, and J. Eric Dietz. 2022. Optimizing Cybersecurity Budgets with AttackSimulation. IEEE, Boston, MA, USA. DOI:<https://doi.org/10.1109/HST56032.2022.10024984>
- [288] Dan McDevitt. 2017. Rwanda censors critical, independent media in targeted fashion: report. *Open Technology Fund*. Retrieved from <https://www.opentech.fund/news/new-report-investigates-internet-censorship-during-rwandas-2017-presidential-election/>
- [289] Allison McDonald, Matthew Bernhard, Luke Valenta, Benjamin VanderSloot, Will Scott, Nick Sullivan, J. Alex Halderman, and Roya Ensafi. 2018. 403 Forbidden: A Global View of CDN Geoblocking. In *Internet Measurement Conference*, ACM. Retrieved from <http://delivery.acm.org/10.1145/3280000/3278552/p218-McDonald.pdf>
- [290] Brian E. McGarry, Ashvin D. Gandhi, and Michael L. Barnett. 2023. Covid-19 Surveillance Testing and Resident Outcomes in Nursing Homes. *N Engl J Med* 388, 12 (March 2023), 1101–1110. DOI:<https://doi.org/10.1056/NEJMoa2210063>
- [291] Molly McHugh. 2011. Burma bans Skype, severing global communication. *digitaltrends*. Retrieved from <https://www.digitaltrends.com/computing/burma-bans-skype-severing-global-communication/>
- [292] Iain McLean and Alistair McMillan (Eds.). 2009. *The concise Oxford dictionary of politics* (3rd ed ed.). Oxford University Press, Oxford ; New York.

- [293] Joe McNamee. 2011. The Slide from “Self-Regulation” to Corporate Censorship. In *European Digital Rights*. Retrieved from https://www.edri.org/files/EDRI_selfreg_final_20110124.pdf
- [294] Damian Menscher. 2020. Exponential growth in DDoS attack volumes. *Google Cloud Blog*. Retrieved from <https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks>
- [295] Merriam-Webster. censor. *Merriam-Webster*. Retrieved July 14, 2022 from <https://www.merriam-webster.com/dictionary/censor>
- [296] Merriam-Webster. attribution. *Merriam-Webster.com Dictionary*. Retrieved from <https://www.merriam-webster.com/dictionary/attribution>
- [297] Mohsen Minaei, Pedro Moreno-Sanchez, and Aniket Kate. 2020. MoneyMorph: Censorship Resistant Rendezvous using Permissionless Cryptocurrencies. *Proceedings on Privacy Enhancing Technologies* 2020, 3 (July 2020), 404–424. DOI:<https://doi.org/10.2478/popets-2020-0058>
- [298] Ming Song, Gang Xiong, Zhenzhen Li, Junrui Peng, and Li Guo. 2013. A de-anonymize attack method based on traffic analysis. In *2013 8th International Conference on Communications and Networking in China (CHINACOM)*, IEEE, Guilin, China, 455–460. DOI:<https://doi.org/10.1109/ChinaCom.2013.6694639>
- [299] Jelena Mirkovic and Peter Reiher. 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. *SIGCOMM Comput. Commun. Rev.* 34, 2 (April 2004), 39–53. DOI:<https://doi.org/10.1145/997150.997156>
- [300] Asya Mitseva, Andriy Panchenko, and Thomas Engel. 2018. The state of affairs in BGP security: A survey of attacks and defenses. *Computer Communications* 124, (June 2018), 45–60. DOI:<https://doi.org/10.1016/j.comcom.2018.04.013>
- [301] Hooman Mohajeri Moghaddam, Baiyu Li, Mohammad Derakhshani, and Ian Goldberg. 2012. SkypeMorph: protocol obfuscation for Tor bridges. In *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12*, ACM Press, Raleigh, North Carolina, USA, 97. DOI:<https://doi.org/10.1145/2382196.2382210>
- [302] David Moher, Alessandro Liberati, Jennifer Tetzlaff, Douglas G. Altman, and The PRISMA Group. 2009. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLoS Med* 6, 7 (July 2009), e1000097. DOI:<https://doi.org/10.1371/journal.pmed.1000097>
- [303] Daniel L. Moody. 2005. Theoretical and practical issues in evaluating the quality of conceptual models: current state and future directions. *Data & Knowledge Engineering* 55, 3 (December 2005), 243–276. DOI:<https://doi.org/10.1016/j.datak.2004.12.005>

- [304] Lennart Mühlenmeier. 2020. Jordan does not block, it throttles internet access. *Netspolitik.org*. Retrieved from <https://netzpolitik.org/2020/jordan-throttles-not-blocks-internet-access-shutdowns-keepit/#netzpolitik-pw>
- [305] Steven J. Murdoch and Piotr Zielinski. 2007. Sampled Traffic Analysis by Internet-Exchange-Level Adversaries. *Privacy Enhancing Technologies* (2007). DOI:https://doi.org/10.1007/978-3-540-75551-7_11
- [306] Zubair Nabi. 2013. The Anatomy of Web Censorship in Pakistan. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/conference/foci13/foci13-nabi.pdf>
- [307] Elisa Yumi Nakagawa, Flavio Oquendo, and Martin Becker. 2012. RAModel: A Reference Model for Reference Architectures. In *2012 Joint Working IEEE/IFIP Conference on Software Architecture and European Conference on Software Architecture*, IEEE, Helsinki, Finland, 297–301. DOI:<https://doi.org/10.1109/WICSA-ECSA.2012.49>
- [308] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *Independent* (2008). DOI:<https://doi.org/10.2139/ssrn.3440802>
- [309] Arvind Narayanan and Bendert Zevenbergen. 2015. No Encore for Encore? Ethical Questions for Web-Based Censorship Measurement. *Technology Science* (2015). Retrieved from <https://censorbib.nymity.ch/pdf/Narayanan2015a.pdf>
- [310] Milad Nasr, Hadi Zolfaghari, Amir Houmansadr, and Amirhossein Ghafari. 2020. MassBrowser: Unblocking the Censored Web for the Masses, by the Masses. In *Proceedings 2020 Network and Distributed System Security Symposium*, Internet Society, San Diego, CA. DOI:<https://doi.org/10.14722/ndss.2020.24340>
- [311] Jose Nazario. *Politically Motivated Denial of Service Attacks*.
- [312] NetBlocks. 2019. Iraq introduces nightly internet curfew. *NetBlocks.org*. Retrieved from <https://netblocks.org/reports/iraq-introduces-nightly-internet-curfew-JAp1DKBd>
- [313] NetBlocks. 2020. Facebook Live streams restricted in Jordan during Teachers’ Syndicate protests. *NetBlocks.org*. Retrieved from <https://netblocks.org/reports/facebook-live-streams-restricted-in-jordan-during-teachers-syndicate-protests-XB7K1xB7>
- [314] NetBlocks. 2021. Internet disrupted in Colombia amid anti-government protests. *NetBlocks.org*. Retrieved from <https://netblocks.org/reports/internet-disrupted-in-colombia-amid-anti-government-protests-YAEvMvB3>
- [315] Lily Hay Newman. 2019. How the Iranian Government Shut Off the Internet. *WIRED*. Retrieved from <https://www.wired.com/story/iran-internet-shutoff/>
- [316] Arian Akhavan Niaki, Shinyoung Cho, Zachary Weinberg, Nguyen Phong Hoang, Abbas Razaghpanah, Nicolas Christin, and Phillipa Gill. 2020. ICLab: A Global, Longitudinal Internet Censorship Measurement Platform. In *2020 IEEE Symposium on Security and*

- Privacy (SP)*, IEEE, San Francisco, CA, USA, 135–151.
DOI:<https://doi.org/10.1109/SP40000.2020.00014>
- [317] Aqib Nisar, Aqsa Kashaf, Ihsan Ayyub Qazi, and Zartash Afzal Uzmi. 2018. Incentivizing Censorship Measurements via Circumvention. In *SIGCOMM*, ACM. Retrieved from <https://dl.acm.org/authorize?N666961>
- [318] Leif Nixon. 2011. Some observations on the Great Firewall of China. *Linköping University*. Retrieved from <https://www.nsc.liu.se/~nixon/sshprobes.html>
- [319] Daiyuu Nobori and Yasushi Shinjo. 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. Retrieved from <https://www.usenix.org/system/files/conference/nsdi14/nsdi14-paper-nobori.pdf>
- [320] Helmi Noman. 2019. Internet Censorship and the Intraregional Geopolitical Conflicts in the Middle East and North Africa. *SSRN Journal* (2019). DOI:<https://doi.org/10.2139/ssrn.3315708>
- [321] Dawn C Nunziato. 2014. The Beginning of the End of Internet Freedom. *Georgetown Journal of International Law* (2014). Retrieved from <http://ssrn.com/abstract=2995714>
- [322] Jonathan Oakley, Lu Yu, Xingsi Zhong, Ganesh Kumar Venayagamoorthy, and Richard Brooks. 2020. Protocol Proxy: An FTE-based covert channel. *Computers & Security* 92, (2020). Retrieved from <https://censorbib.nymity.ch/pdf/Oakley2020a.pdf>
- [323] OASIS-RM Technical Committee. 2014. OASIS SOA Reference Model. *OASIS Open*. Retrieved from <https://www.oasis-open.org/committees/soa-rm/faq.php>
- [324] Katherine Ognyanova, David Lazer, Ronald Robertson, and Christo Wilson. 2020. Misinformation in action: Fake news exposure is linked to lower trust in media, higher trust in government when your side is in power. *The Harvard Kennedy School Misinformation Review* 1, 4 (June 2020). DOI:<https://doi.org/10.37016/mr-2020-024>
- [325] Chitu Okoli and Kira Schabram. 2010. A Guide to Conducting a Systematic Literature Review of Information Systems Research. *SSRN Journal* (2010). DOI:<https://doi.org/10.2139/ssrn.1954824>
- [326] Babatunde Okunoye, Maria Xynou, Arturo Filastò, and Gabreal Odunsi. 2019. Nigeria’s 2019 elections through the lens of network measurements. *OONI Reports*. Retrieved from <https://ooni.org/post/2019-nigeria-internet-censorship/>
- [327] Karl Olson, Jack Wampler, and Eric Keller. 2023. Doomed to Repeat with IPv6? Characterization of NAT-centric Security in SOHO Routers. *ACM Computing Surveys* (March 2023). DOI:<https://doi.org/10.1145/3586007>

- [328] ONI Team. 2014. Looking Forward: A Note of Appreciation and Closure on a Decade of Research. *OpenNet Initiative*. Retrieved from <https://opennet.net/blog/2014/12/looking-forward-note-appreciation-and-closure-decade-research>
- [329] Amanda Onion, Missy Sullivan, Matt Mullen, and Christian Zapata. Arab Spring. *History.com*. Retrieved November 1, 2022 from <https://www.history.com/topics/middle-east/arab-spring>
- [330] OONI. 2021. Estonia blocking gambling sites query. *OONI Explorer*. Retrieved from https://explorer.ooni.org/search?since=2020-06-01&until=2021-05-31&failure=true&probe_cc=EE&test_name=web_connectivity&only=anomalies&category_code=GMB
- [331] OONI. Open Observatory of Network Interference: Global community measuring Internet censorship since 2012. *OONI*. Retrieved from <https://ooni.org/>
- [332] OONI. OONI Research Reports Blog. *Open Observatory of Network Interference*. Retrieved from <https://ooni.org/reports/>
- [333] OONI. OONI Probe Data Set 20200601-20210531. Retrieved from <https://ooni.org/data/>
- [334] OONI. Argentina blocking Uber website and app. *OONI Explorer*. Retrieved from https://explorer.ooni.org/search?since=2017-01-01&until=2021-05-31&failure=false&probe_cc=AR&test_name=web_connectivity&domain=www.uber.com&only=anomalies
- [335] OpenNet Initiative. 2009. *Internet Filtering in China*. OpenNet Initiative, Technical Report. Retrieved from http://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf
- [336] OpenNet Initiative. Country profile: Kazakhstan, 2010. Retrieved from <https://opennet.net/research/profiles/kazakhstan>
- [337] Juan Ortiz Freuler. 2022. The weaponization of private corporate infrastructure: Internet fragmentation and coercive diplomacy in the 21st century. *Global Media and China* (November 2022). DOI:<https://doi.org/10.1177/20594364221139729>
- [338] Barbara Ortutay, Frank Bajak, and Tali Arbel. 2021. Cuba's internet cutoff: A go-to tactic to suppress dissent. *Associated Press*. Retrieved from <https://apnews.com/article/business-technology-cuba-ca1ae7975e04481e8cbd56d62a7fb30e>
- [339] Oxford English Dictionary. Liberalism. *OED*. Retrieved from <https://www.oed.com/view/Entry/107864?redirectedFrom=liberalism>
- [340] Oxford English Dictionary. Authoritarianism. *OED*. Retrieved from <https://www.oed.com/view/Entry/13344>
- [341] Oxford Union. 2017. Michael Hayden | Full Q&A | Oxford Union. *YouTube*. Retrieved from https://www.youtube.com/watch?v=exw9HpK_ytl

- [342] Ramakrishna Padmanabhan, Arturo Filastò, Maria Xynou, Ram Sundara Raman, Kennedy Middleton, Mingwei Zhang, Doug Madory, Molly Roberts, and Alberto Dainotti. 2021. A multi-perspective view of Internet censorship in Myanmar. In *Free and Open Communications on the Internet*, ACM, Virtual Event, USA. DOI:<https://doi.org/10.1145/3473604.3474562>
- [343] Palo Alto Networks. 2018. How to Block a Specific HTTPS Site with URL Filtering. *Palo Alto Networks: Customer Support Portal*. Retrieved from <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIIPCA0>
- [344] Palo Alto Networks. 2018. How to Block Tor (The Onion Router). *Palo Alto Networks: Customer Support Portal*. Retrieved from <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRtCAK>
- [345] Jong Chun Park and Jedidiah R. Crandall. 2010. Empirical Study of a National-Scale Distributed Intrusion Detection System: Backbone-Level Filtering of HTML Responses in China. In *Distributed Computing Systems*, IEEE, 315–326. Retrieved from <https://www.cs.unm.edu/~crandall/icdcs2010.pdf>
- [346] Christopher Patton. 2020. Good-bye ESNI, hello ECH! *Cloudflare Blog*. Retrieved from <https://blog.cloudflare.com/encrypted-client-hello/>
- [347] Katy Pearce. 2020. While Armenia and Azerbaijan fought over Nagorno-Karabakh, their citizens battled on social media. *The Washington Post*. Retrieved from <https://www.washingtonpost.com/politics/2020/12/04/while-armenia-azerbaijan-fought-over-nagorno-karabakh-their-citizens-battled-social-media/>
- [348] Paul Pearce, Roya Ensafi, Frank Li, Nick Feamster, and Vern Paxson. 2017. Augur: Internet-Wide Detection of Connectivity Disruptions. In *Symposium on Security & Privacy*, IEEE. Retrieved from <https://www.ieee-security.org/TC/SP2017/papers/586.pdf>
- [349] Paul Pearce, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. 2017. Global Measurement of DNS Manipulation. *Proceedings of the 26th USENIX Security Symposium* (2017). Retrieved from <https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-pearce.pdf>
- [350] Andreas Pfitzmann and Marit Köhntopp. 2001. Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In *Designing Privacy Enhancing Technologies*. Springer Berlin Heidelberg, Berlin, Heidelberg. DOI:https://doi.org/10.1007/3-540-44702-4_1
- [351] Chris Phiri. 2014. Zambia Reports, Watchdog ‘Unblocked.’ *Zambia Reports*. Retrieved from <https://web.archive.org/web/20190424160446/https://zambiareports.com/2014/04/04/zambia-reports-watchdog-unblocked/>

- [352] Louis Poinsignon. 2018. BGP leaks and cryptocurrencies. *Cloudflare Blog*. Retrieved from <https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/>
- [353] PowerTunnel. PowerTunnel - Powerful and extensible proxy server. *Github*. Retrieved from <https://github.com/krlvm/PowerTunnel>
- [354] Matthew Prince. 2019. Introducing WARP: Fixing Mobile Internet Performance and Security. *Cloudflare Blog*. Retrieved from <https://blog.cloudflare.com/1111-warp-better-vpn/>
- [355] Psiphon. 2020. A Technical Description of Psiphon. *Psiphon*. Retrieved from <https://web.archive.org/web/20201027205044/https://psiphon.ca/en/blog/psiphon-a-technical-description>
- [356] Andrea Purdeková. 2011. ‘Even if I am not here, there are so many eyes’: surveillance and state reach in Rwanda. *J. Mod. Afr. Stud.* 49, 3 (September 2011), 475–497. DOI:<https://doi.org/10.1017/S0022278X11000292>
- [357] Ram Sundara Raman, Leonid Evdokimov, Eric Wurstrow, J. Alex Halderman, and Roya Ensafi. 2020. Investigating Large Scale HTTPS Interception in Kazakhstan. In *Proceedings of the ACM Internet Measurement Conference*, ACM, 125–132. DOI:<https://doi.org/10.1145/3419394.3423665>
- [358] Ram Sundara Raman, Adrian Stoll, Jakub Dalek, Reethika Ramesh, Will Scott, and Roya Ensafi. 2020. Measuring the Deployment of Network Censorship Filters at Global Scale. In *Proceedings 2020 Network and Distributed System Security Symposium*, Internet Society, San Diego, CA. DOI:<https://doi.org/10.14722/ndss.2020.23099>
- [359] Ram Sundara Raman, Apurva Virkud, Sarah Laplante, Vinicius Fortuna, and Roya Ensafi. 2023. Advancing the Art of Censorship Data Analysis. In *Free and Open Communications on the Internet*, Proceedings on Privacy Enhancing Technologies. Retrieved from <https://petsymposium.org/foci/2023/foci-2023-0003.pdf>
- [360] Ram Sundara Raman, Mona Wang, Jakub Dalek, Jonathan Mayer, and Roya Ensafi. 2022. Network Measurement Methods for Locating and Examining Censorship Devices. In *Emerging Networking Experiments and Technologies*, ACM. Retrieved from <https://dl.acm.org/doi/pdf/10.1145/3555050.3569133>
- [361] Reethika Ramesh, Leonid Evdokimov, Diwen Xue, and Roya Ensafi. 2022. VPNalyzer: Systematic Investigation of the VPN Ecosystem. In *Proceedings 2022 Network and Distributed System Security Symposium*, Internet Society, San Diego, CA, USA. DOI:<https://doi.org/10.14722/ndss.2022.24285>
- [362] Reethika Ramesh, Ram Sundara Raman, Matthew Bernhard, Victor Ongkowijaya, Leonid Evdokimov, Anne Edmundson, Steven Sprecher, Muhammad Ikram, and Roya Ensafi. 2020. Decentralized Control: A Case Study of Russia. In *Proceedings 2020 Network and Distributed System Security Symposium*, Internet Society, San Diego, CA. DOI:<https://doi.org/10.14722/ndss.2020.23098>

- [363] Tuomo Rautakivi. 2022. *Critical Evaluation of Individualism, Collectivism and Collective Action*.
- [364] Michael K. Reiter and Aviel D. Rubin. 1999. Anonymous Web transactions with Crowds. *Communications of the ACM* 42, 2 (February 1999), 32–48. DOI:<https://doi.org/10.1145/293411.293778>
- [365] Representative. 2019. Media Release: Taking action against illegal offshore gambling websites. *Paul Fletcher MP*. Retrieved from <https://www.paulfletcher.com.au/media-releases/media-release-taking-action-against-illegal-offshore-gambling-websites>
- [366] Eric Rescorla, Kazuho Oku, Nick Sullivan, and Christopher Wood. 2022. *TLS Encrypted Client Hello, Internet-Draft RFC*. Internet Engineering Task Force (IETF). Retrieved from <https://datatracker.ietf.org/doc/draft-ietf-tls-esni/15>
- [367] Reuters. 2022. Russia blocks access to BBC and Voice of America websites. *Reuters*. Retrieved from <https://www.reuters.com/business/media-telecom/russia-restricts-access-bbc-russian-service-radio-liberty-ria-2022-03-04/>
- [368] Reuters Staff. 2018. Businesses, consumers uncertain ahead of China VPN ban. *Reuters*. Retrieved from <https://www.reuters.com/article/us-china-vpns/businesses-consumers-uncertain-ahead-of-china-vpn-ban-idUSKBN1H612F>
- [369] Roland van Rijswijk-Deij, Anna Sperotto, and Aiko Pras. 2015. Making the Case for Elliptic Curves in DNSSEC. *SIGCOMM Comput. Commun. Rev.* 45, 5 (September 2015), 13–19. DOI:<https://doi.org/10.1145/2831347.2831350>
- [370] Jenn Riley. 2017. *Understanding Metadata: What is metadata, and what is it for?* National Information Standards Organization, Baltimore, MD. Retrieved from <https://www.niso.org/publications/understanding-metadata-2017>
- [371] RIPE NCC. 2008. YouTube Hijacking: A RIPE NCC RIS case study. *RIPE NCC*. Retrieved from <https://web.archive.org/web/20080405030750/http://www.ripe.net/news/study-youtube-hijacking.html>
- [372] Hal Roberts, Ethan Zuckerman, and John G. Palfrey. 2011. 2011 Circumvention Tool Evaluation. *Berkman Center Research Publication No. 2011-08* (2011). Retrieved October 18, 2021 from https://cyber.harvard.edu/sites/cyber.harvard.edu/files/2011_Circumvention_Tool_Evaluation_1.pdf
- [373] Hal Roberts, Ethan Zuckerman, Jillian York, Robert Faris, and John Palfrey. 2010. Circumvention Tool Usage Report. *Berkman Center Research Publication No. 2010-*. Retrieved from https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf

- [374] Margaret E. Roberts. 2020. *Censored: distraction and diversion inside China's great firewall*. Princeton University Press, Princeton.
- [375] Adi Robertson. 2014. Putin signs law forcing bloggers to register with Russian media office. *The Verge*. Retrieved from <https://www.theverge.com/2014/5/7/5690410/putin-signs-law-forcing-bloggers-to-register-with-russian-media-office>
- [376] Florentin Rochet and Olivier Pereira. 2018. Dropping on the Edge: Flexibility and Traffic Confirmation in Onion Routing Protocols. *Proceedings on Privacy Enhancing Technologies* 2018, 2 (April 2018). DOI:<https://doi.org/10.1515/popets-2018-0011>
- [377] Marc B. Rosen, James Parker, and Alex J. Malozemoff. 2021. Balboa: Bobbing and Weaving around Network Censorship. In *USENIX Security Symposium*, USENIX. Retrieved from <https://www.usenix.org/system/files/sec21-rosen.pdf>
- [378] Roskomnadzor. 2021. Roskomnadzor takes measures to protect russian citizens from the influence of illegal content. *Roskomnadzor*. Retrieved from <https://rkn.gov.ru/news/rsoc/news73464.htm>
- [379] Malise Ruthven. 2016. How to Understand ISIS. *The New York Review*. Retrieved from <https://www.nybooks.com/articles/2016/06/23/how-to-understand-isis/>
- [380] Julia Ryng, Guillemette Guicherd, Judy Al Saman, Priyanka Choudhury, and Angharad Kellett. 2022. Internet Shutdowns: A Human Rights Issue. *The RUSI Journal* 167, 4–5 (July 2022), 50–63. DOI:<https://doi.org/10.1080/03071847.2022.2156234>
- [381] Denham Sadler. 2019. Arbitrary site blocks a ‘slippery slope.’ *InnovationAUS*. Retrieved from <https://www.innovationaus.com/arbitrary-site-blocks-a-slippery-slope/>
- [382] Nicholas Michael Sambaluk and Eugene Spafford. 2020. *Myths and realities of cyber warfare: conflict in the digital realm*. Praeger Security International, Santa Barbara, CA.
- [383] Ferry Astika Saputra, Isbat Uzzin Nadhori, and Balighani Fathul Barry. 2016. Detecting and blocking onion router traffic using deep packet inspection. In *2016 International Electronics Symposium (IES)*, IEEE, Denpasar, Indonesia, 283–288. DOI:<https://doi.org/10.1109/ELECSYM.2016.7861018>
- [384] Adam Satariano. 2022. How Russia Took Over Ukraine’s Internet in Occupied Territories. *The New York Times*. Retrieved from <https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html>
- [385] Sambhav Satija and Rahul Chatterjee. 2021. BlindTLS: Circumventing TLS-Based HTTPS Censorship. In *Free and Open Communications on the Internet*, ACM. Retrieved from <https://doi.org/10.1145/3473604.3474564>

- [386] Molly Sauter. 2014. *The Coming Swarm: DDoS Actions, Hactivism, and Civil Disobedience on the Internet* (1st ed.). Bloomsbury Publishing Inc. DOI:<https://doi.org/10.5040/9781628926705>
- [387] Jared Schroeder. 2022. Meet the EU Law That Could Reshape Online Speech in the U.S. *Slate*. Retrieved from <https://slate.com/technology/2022/10/digital-services-act-european-union-content-moderation.html>
- [388] Christoph Ludwig Schuba. 1997. On the modeling, design, and implementation of firewall technology. Purdue University.
- [389] C.L. Schuba and E.H. Spafford. 1997. A reference model for firewall technology. In *Proceedings 13th Annual Computer Security Applications Conference*, IEEE, San Diego, CA, USA, 133–145. DOI:<https://doi.org/10.1109/CSAC.1997.646183>
- [390] Will Scott, Thomas Anderson, Tadayoshi Kohno, and Arvind Krishnamurthy. 2016. Satellite: Joint Analysis of CDNs and Network-Level Interference. *Proceedings of the 2016 USENIX Annual Technical Conference* (June 2016). Retrieved from https://www.usenix.org/system/files/conference/atc16/atc16_paper-scott.pdf
- [391] Wendy Seltzer. 2011. Infrastructures of Censorship and Lessons from Copyright Resistance. *Free and Open Communications on the Internet* (2011). Retrieved from https://www.usenix.org/legacy/events/foci11/tech/final_files/Seltzer.pdf
- [392] Ryan Serabian and Daniel Kapellmann Zafra. 2022. Pro-PRC “HaiEnergy” Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites. *Mandiant*. Retrieved from <https://www.mandiant.com/resources/blog/pro-prc-information-operations-campaign-haienergy>
- [393] Serbia. 2020. Zakon o igrama na sreću [The Law about Gambling]. Retrieved from https://www.paragraf.rs/propisi/zakon_o_igrama_na_srecu.html
- [394] Andreas Sfakianakis, Elias Athanasopoulos, and Sotiris Ioannidis. 2011. CensMon: A Web Censorship Monitor. In *Free and Open Communications on the Internet*, USENIX. Retrieved from https://www.usenix.org/legacy/events/foci11/tech/final_files/Sfakianakis.pdf
- [395] Nishant Shah. 2021. (Dis)information Blackouts: Politics and Practices of Internet Shutdowns. *International Journal of Communication* 15, (2021).
- [396] Adrian Shahbaz and Allie Funk. 2021. *Freedom on the Net 2021 - The Global Drive to Control Big Tech*. Annual Report, Freedom House. Retrieved from https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

- [397] Sima L. Sharara and Souha S. Kanj. 2014. War and Infectious Diseases: Challenges of the Syrian Civil War. *PLoS Pathogens* 10, 11 (November 2014), e1004438. DOI:<https://doi.org/10.1371/journal.ppat.1004438>
- [398] Y. Shavitt and N. Zilberman. 2012. Arabian Nights: Measuring the Arab Internet during the 2011 Events. *IEEE Network* 26, 6 (November 2012), 75–80. DOI:<https://doi.org/10.1109/MNET.2012.6375897>
- [399] Xiaoxiao Shen and Rory Truex. 2021. In Search of Self-Censorship. *Brit. J. Polit. Sci.* 51, 4 (October 2021), 1672–1684. DOI:<https://doi.org/10.1017/S0007123419000735>
- [400] Justine Sherry, Chang Lan, Raluca Ada Popa, and Sylvia Ratnasamy. 2015. BlindBox: Deep Packet Inspection over Encrypted Traffic. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, ACM, London United Kingdom, 213–226. DOI:<https://doi.org/10.1145/2785956.2787502>
- [401] Sandra Siby, Marc Juarez, Claudia Diaz, Narseo Vallina-Rodriguez, and Carmela Troncoso. 2020. Encrypted DNS --> Privacy? A Traffic Analysis Perspective. In *Proceedings 2020 Network and Distributed System Security Symposium*, Internet Society, San Diego, CA. DOI:<https://doi.org/10.14722/ndss.2020.24301>
- [402] Singapore IMDA. 2020. Internet Regulatory Framework. *Singapore IMDA*. Retrieved from <https://web.archive.org/web/20220925231358/https://www.imda.gov.sg/regulations-and-licensing-listing/content-standards-and-classification/standards-and-classification/internet>
- [403] Kushagra Singh, Gurshabad Grover, and Varun Bansal. 2020. How India Censors the Web. In *12th ACM Conference on Web Science*, ACM, Southampton United Kingdom, 21–28. DOI:<https://doi.org/10.1145/3394231.3397891>
- [404] Rachee Singh, Rishab Nithyanand, Sadia Afroz, Paul Pearce, Michael Carl Tschantz, Phillipa Gill, and Vern Paxson. 2017. Characterizing the Nature and Dynamics of Tor Exit Blocking. In *USENIX Security Symposium*, USENIX. Retrieved from <https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-singh.pdf>
- [405] Charlie Smith. 2015. We are under attack. *GreatFire.org*. Retrieved from <https://en.greatfire.org/blog/2015/mar/we-are-under-attack>
- [406] Software Freedom Law Centre. 2020. Internet shutdowns. *SFLC.in*. Retrieved from <https://internetshutdowns.in/>
- [407] Daniel J Solove. 2009. *Understanding Privacy*. Harvard University Press.
- [408] Jonghyuk Song, Sangho Lee, and Jong Kim. 2016. Inference Attack on Browsing History of Twitter Users Using Public Click Analytics and Twitter Metadata. *IEEE Transactions on Dependable and Secure Computing* 13, 3 (May 2016). DOI:<https://doi.org/10.1109/TDSC.2014.2382577>

- [409] Eugene H. Spafford. 2023. Personal communication.
- [410] Eugene H Spafford and Annie I Antón. 2008. The Balance of Privacy and Security. In *Controversies in Science and Technology*. Retrieved from <https://home.liebertpub.com/publications/controversies-in-science-and-technology-volume-2-from-climate-to-chromosomes/254/toc>
- [411] Raphael Spreitzer, Veelasha Moonsamy, Thomas Korak, and Stefan Mangard. 2018. Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Commun. Surv. Tutorials* 20, 1 (2018), 465–488. DOI:<https://doi.org/10.1109/COMST.2017.2779824>
- [412] Yixin Sun, Anne Edmundson, Laurent Vanbever, Oscar Li, Jennifer Rexford, Mung Chiang, and Prateek Mittal. 2015. RAPTOR: Routing Attacks on Privacy in Tor. *24th USENIX Security Symposium* (March 2015). Retrieved December 17, 2021 from <https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-sun.pdf>
- [413] Ram Sundara Raman, Prerana Shenoy, Katharina Kohls, and Roya Ensafi. 2020. Censored Planet: An Internet-wide, Longitudinal Censorship Observatory. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ACM, Virtual Event USA, 49–66. DOI:<https://doi.org/10.1145/3372297.3417883>
- [414] Tailscale. Tailscale makes networking easy. Retrieved April 24, 2021 from <https://tailscale.com/>
- [415] Rima Tanash, Zhouhan Chen, Dan Wallach, and Melissa Marschall. 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. Retrieved from <https://www.usenix.org/system/files/conference/foci17/foci17-paper-tanash.pdf>
- [416] Rima S. Tanash, Zhouhan Chen, Tanmay Thakur, Dan S. Wallach, and Devika Subramanian. 2015. Known Unknowns: An Analysis of Twitter Censorship in Turkey. In *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society*, ACM, Denver Colorado USA, 11–20. DOI:<https://doi.org/10.1145/2808138.2808147>
- [417] Tax and Customs Board. 2020. Blokeeritud hasartmängu internetileheküljed ["Blocked gambling websites"]. *Maksu-Ja Tolliamet*. Retrieved from <https://web.archive.org/web/20201204203801/https://www.emta.ee/et/eraklient/maa-soiduk-mets-hasartmang/blokeeritud-hasartmangu-internetilehekuljed>
- [418] Berhan Taye, Maria Xynou, Leonid Evdokimov, and Moses Karanja. 2018. Ethiopia: Verifying the unblocking of websites. *OONI Reports*. Retrieved from <https://ooni.org/post/ethiopia-unblocking/>
- [419] Tbilisi. 2015. Georgia Blocks Access to Pro-Islamic State Websites. *Civil.ge*. Retrieved from <https://old.civil.ge/eng/article.php?id=28801?id=28801>

- [420] Technical Working Group, BITAG. 2013. Port Blocking. *SSRN Journal* (2013). DOI:<https://doi.org/10.2139/ssrn.2701485>
- [421] The Citizen Lab. Free Expression Online. *The Citizen Lab - University of Toronto*. Retrieved from <https://citizenlab.ca/category/research/free-expression-online/>
- [422] The Guardian. 2016. Record number of journalists in jail globally after Turkey crackdown. *The Guardian*. Retrieved from <https://www.theguardian.com/media/greenslade/2016/dec/13/turkey-has-81-of-the-worlds-259-jailed-journalists-behind-bars>
- [423] The Korea Communications Commission. 2019. Press Release.
- [424] The World Bank. Individuals using the Internet (% of population) - Myanmar. *International Telecommunication Union (ITU) World Telecommunication/ICT Indicators Database*. Retrieved December 12, 2022 from <https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=MM>
- [425] Eneken Tikk, Kadri Kaska, Kristel Rännimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul. 2008. Cyber Attacks Against Georgia: Legal Lessons Identified. (2008). Retrieved from <http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf>
- [426] Adam Tinworth. 2018. Happy GDPR day! *Twitter*. Retrieved from <https://twitter.com/adders/status/999976701089189890/photo/1>
- [427] Tor. Tor usage statistics during Invasion of Ukraine 2022. *metrics.torproject.org*. Retrieved from https://web.archive.org/web/20230105232136/https://web.ics.purdue.edu/~amaster/anticensorship/Tor_usage_Ukraine_invasion.png
- [428] Tor. Tor Relays and Bridges. *Tor Metrics*. Retrieved July 16, 2022 from <https://metrics.torproject.org/networksize.html>
- [429] Tor. Tor Project | Anonymity Online. *Tor Project*. Retrieved from <https://www.torproject.org/>
- [430] Mark Trevelyan. 2022. Russians' demand for VPNs skyrockets after Meta block. *Reuters*. Retrieved from <https://www.reuters.com/technology/russians-demand-vpns-skyrockets-after-meta-block-2022-03-14/>
- [431] Nikhil Tripathi and Neminath Hubballi. 2021. Application Layer Denial-of-Service Attacks and Defense Mechanisms: A Survey. *ACM Comput. Surv.* 54, 4 (April 2021), 1–33. DOI:<https://doi.org/10.1145/3448291>
- [432] Anton Troianovski and Valeriya Safronova. 2022. Russia Takes Censorship to New Extremes, Stifling War Coverage. *The New York Times*. Retrieved from <https://www.nytimes.com/2022/03/04/world/europe/russia-censorship-media-crackdown.html>

- [433] Michael Carl Tschantz, Sadia Afroz, Anonymous, and Vern Paxson. 2016. SoK: Towards Grounding Censorship Circumvention in Empiricism. In *2016 IEEE Symposium on Security and Privacy (SP)*, IEEE, San Jose, CA, 914–933. DOI:<https://doi.org/10.1109/SP.2016.59>
- [434] Michael Carl Tschantz, Sadia Afroz, Shaarif Sajid, Shoaib Asif Qazi, Mobin Javed, and Vern Paxson. 2018. A Bestiary of Blocking: The Motivations and Modes behind Website Unavailability. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/conference/foci18/foci18-paper-tschantz.pdf>
- [435] Ultrasurf. Ultrasurf Downloads. *Ultrasurf*. Retrieved from <https://ultrasurf.us/download/>
- [436] Todd Underwood. 2005. Internet-wide Catastrophe - Last Year. *renesys | blog*. Retrieved from https://web.archive.org/web/20080228131639/http://www.renesys.com/blog/2005/12/internetwide_nearcatastrophela.shtml
- [437] Nik Unger, Sergej Dechand, Joseph Bonneau, Sascha Fahl, Henning Perl, Ian Goldberg, and Matthew Smith. 2015. SoK: Secure Messaging. In *2015 IEEE Symposium on Security and Privacy*, IEEE, San Jose, CA, USA, 232–249. DOI:<https://doi.org/10.1109/SP.2015.22>
- [438] United Nations. 1948. Universal Declaration of Human Rights: Article 19. *United Nations*. Retrieved from <https://www.un.org/en/about-us/universal-declaration-of-human-rights>
- [439] United Nations. 2021. Right to freedom of expression in Myanmar must be guaranteed, UN expert urges military coup leader. *United Nations News*. Retrieved from <https://news.un.org/en/story/2021/04/1090742>
- [440] United Nations. UN Member States. *United Nations*. Retrieved November 1, 2022 from <https://www.un.org/en/about-us/member-states>
- [441] Unknown. 2021. Dozens detained at Kazakhstan political prisoner protest. *Aljazeera*. Retrieved from <https://www.aljazeera.com/news/2021/2/28/dozens-detained-at-kazakhstan-political-prisoner-protest>
- [442] US Army. 2020. *ATP 7-100.2 North Korean Tactics*.
- [443] US Army. *FM 3-12 Cyberspace and Electronic Warfare Operations*. Retrieved from https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3089_FM%203-12%20FINAL%20WEB%201.pdf
- [444] US Department of Justice. 2022. Press Release: United States Leads Seizure of One of the World’s Largest Hacker Forums and Arrests Administrator. *Office of Public Affairs*. Retrieved from <https://www.justice.gov/opa/pr/united-states-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator>

- [445] US Strategic Command. 2009. *The Cyber Warfare Lexicon*. USSTRATCOM. Retrieved from <https://info.publicintelligence.net/USSTRATCOM-CyberWarfareLexicon.pdf>
- [446] Brian Van Leeuwen, Jason Gao, Haikuo Yin, Benjamin Anthony, and Vincent Urias. 2019. *Networked-based Cyber Analysis using Deep Packet Inspection (DPI) for High-Speed Networks*. Sandia National Lab, U.S. Department of Energy. DOI:<https://doi.org/10.2172/1863848>
- [447] Benjamin VanderSloot, Allison McDonald, Will Scott, J Alex Halderman, and Roya Ensafi. 2018. Quack: Scalable Remote Measurement of Application-Layer Censorship. *USENIX Security Symposium (2018)*, 16.
- [448] Joana Varon, Rebecca Gomperts, Maria Xynou, Federico Ceratto, and Arturo Filastò. 2019. On the blocking of abortion rights websites: Women on Waves & Women on Web. *OONI Reports*. Retrieved from <https://ooni.org/post/2019-blocking-abortion-rights-websites-women-on-waves-web/#brazil>
- [449] Petr Velan, Milan Čermák, Pavel Čeleda, and Martin Drašar. 2015. A Survey of Methods for Encrypted Traffic Classification and Analysis. *Int. J. Network Mgmt* 25, 5 (September 2015), 355–374. DOI:<https://doi.org/10.1002/nem.1901>
- [450] Pieter Velghe. 2019. “Reading China”: The Internet of Things, Surveillance, and Social Management in the PRC. *chinaperspectives* 2019, 1 (March 2019), 85–89. DOI:<https://doi.org/10.4000/chinaperspectives.8874>
- [451] John-Paul Verkamp and Minaxi Gupta. 2012. Inferring Mechanics of Web Censorship Around the World. In *Free and Open Communications on the Internet*, USENIX, Bellevue, WA. Retrieved from <https://www.usenix.org/conference/foci12/workshop-program/presentation/Verkamp>
- [452] Vasilis Ververis, Marios Isaakidis, Chrystalleni Loizidou, and Benjamin Fabian. 2017. Internet Censorship Capabilities in Cyprus: An Investigation of Online Gambling Blocklisting. In *E-Democracy – Privacy-Preserving, Secure, Intelligent E-Government Services*, Sokratis K. Katsikas and Vasilios Zorkadis (eds.). Springer International Publishing, Cham, 136–149. DOI:https://doi.org/10.1007/978-3-319-71117-1_10
- [453] Vasilis Ververis, George Kargiotakis, Arturo Filastò, Benjamin Fabian, and Afentoulis Alexandros. 2015. Understanding Internet Censorship Policy: The Case of Greece. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/conference/foci15/foci15-paper-ververis-updated-2.pdf>
- [454] Vasilis Ververis, Maria Xynou, Tawanda Mugari, and Will Scott. 2016. OONI Data Reveals How WhatsApp Was Blocked (Again) in Brazil. *OONI Reports*. Retrieved from <https://ooni.org/post/brazil-whatsapp-block/>
- [455] James Vincent. 2019. UK police shut off Wi-Fi in London Tube stations to deter climate protestors. *The Verge*. Retrieved from

<https://www.theverge.com/2019/4/17/18411820/london-underground-tube-wi-fi-down-shut-off-protests-extinction-rebellion>

- [456] Anjali Vyas, Ram Sundara Raman, Nick Ceccio, Philipp M. Lutscher, and Roya Ensafi. 2021. Lost in Transmission: Investigating Filtering of COVID-19 Websites. In *Financial Cryptography and Data Security* (Lecture Notes in Computer Science), Springer Berlin Heidelberg, Berlin, Heidelberg, 417–436. DOI:https://doi.org/10.1007/978-3-662-64331-0_22
- [457] Ben Wagner. 2014. The Politics of Internet Filtering: The United Kingdom and Germany in a Comparative Perspective. *Politics* 34, 1 (February 2014), 58–71. DOI:<https://doi.org/10.1111/1467-9256.12031>
- [458] Marc Waldman, Aviel D Rubin, and T Labs. 2000. Publius: A robust, tamper-evident, censorship-resistant web publishing system. *USENIX Security Symposium* (2000).
- [459] Christopher Walker and Robert W. Orttung. 2014. Breaking the News: The Role of State-Run Media. *Journal of Democracy* 25, 1 (2014), 71–85. DOI:<https://doi.org/10.1353/jod.2014.0015>
- [460] Liang Wang, Kevin P. Dyer, Aditya Akella, Thomas Ristenpart, and Thomas Shrimpton. 2015. Seeing through Network-Protocol Obfuscation. In *Computer and Communications Security*, ACM. Retrieved from <http://pages.cs.wisc.edu/~liangw/pub/ccsf653-wangA.pdf>
- [461] Qiyang Wang, Xun Gong, Giang T.K. Nguyen, Amir Houmansadr, and Nikita Borisov. 2012. CensorSpoof: 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, 121. DOI:<https://doi.org/10.1145/2382196.2382212>
- [462] Zhongjie Wang, Yue Cao, Zhiyun Qian, Chengyu Song, and Srikanth V. Krishnamurthy. 2017. Your State is Not Mine: A Closer Look at Evading Stateful Internet Censorship. In *Internet Measurement Conference*, ACM. Retrieved from <http://www.cs.ucr.edu/~krish/imc17.pdf>
- [463] Zhongjie Wang, Shitong Zhu, Yue Cao, Zhiyun Qian, Chengyu Song, Srikanth V. Krishnamurthy, Kevin S. Chan, and Tracy D. Braun. 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. DOI:<https://doi.org/10.14722/ndss.2020.24083>
- [464] Barney Warf. 2011. Geographies of global Internet censorship. *GeoJournal* 76, 1 (February 2011), 1–23. DOI:<https://doi.org/10.1007/s10708-010-9393-3>
- [465] Murdoch Watney. 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 (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), 130–143.
DOI:https://doi.org/10.1007/978-3-319-14289-0_10

- [466] Zachary Weinberg. 2018. Toward Automated Worldwide Monitoring of Network-level Censorship. Dissertation. Carnegie Mellon University.
- [467] Zachary Weinberg, Diogo Barradas, and Nicolas Christin. 2021. Chinese Wall or Swiss Cheese? Keyword filtering in the Great Firewall of China. In *Proceedings of the Web Conference 2021*, ACM, Ljubljana Slovenia, 472–483.
DOI:<https://doi.org/10.1145/3442381.3450076>
- [468] Zachary Weinberg, Mahmood Sharif, Janos Szurdi, and Nicolas Christin. 2017. Topics of Controversy: An Empirical Analysis of Web Censorship Lists. *Privacy Enhancing Technologies 2017*, 1 (2017), 42–61. Retrieved from <https://petsymposium.org/2017/papers/issue1/paper06-2017-1-source.pdf>
- [469] Zachary Weinberg, Jeffrey Wang, Vinod Yegneswaran, Linda Briesemeister, Steven Cheung, Frank Wang, and Dan Boneh. 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, 109.
DOI:<https://doi.org/10.1145/2382196.2382211>
- [470] Zack Whittaker. 2021. Apple’s CSAM detection tech is under fire — again. *TechCrunch*. Retrieved from <https://techcrunch.com/2021/08/18/apples-csam-detection-tech-is-under-fire-again/>
- [471] Brandon Wiley. *Dust: A Blocking-Resistant Internet Transport Protocol*. School of Information, University of Texas at Austin.
- [472] Philipp Winter. 2014. Measuring and circumventing Internet censorship. PhD Dissertation. Karlstad University. Retrieved from <https://www.diva-portal.org/smash/get/diva2:758124/FULLTEXT01.pdf>
- [473] Philipp Winter. NullHypothesis / censorbib. *GitHub*. Retrieved from <https://github.com/NullHypothesis/censorbib>
- [474] Philipp Winter. CensorBib: Selected Research Papers in Internet Censorship. *CensorBib*. Retrieved from <https://censorbib.nymity.ch/>
- [475] Philipp Winter and Stefan Lindskog. 2012. How the Great Firewall of China is Blocking Tor. In *Free and Open Communications on the Internet*, USENIX. Retrieved from <https://www.usenix.org/system/files/conference/foci12/foci12-final2.pdf>
- [476] Philipp Winter, Tobias Pulls, and Juergen Fuss. 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, 213–224.
DOI:<https://doi.org/10.1145/2517840.2517856>

- [477] Sebastian Wolfgarten. 2006. *Investigating large-scale Internet content filtering*. Technical Report, Dublin City University, Dublin, Ireland. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.133.5778&rep=rep1&type=pdf>
- [478] Alexander Wong. 2020. Malaysian authorities start blocking servers that stream pirated content. *Soyacincanau*. Retrieved from <https://soyacincanau.com/2020/02/28/malaysia-block-server-ip-illegal-copyright-streaming-android-tv/>
- [479] Bill Woodcock. 2011. Overview of the Egyptian Internet Shutdown. In *DHS Infosec Technology Transition Council*. Packet Clearing House. Retrieved from <https://web.archive.org/web/20120125051846/http://www.pch.net/resources/misc/Egypt-PCH-Overview.pdf>
- [480] Samuel Woodhams and Simon Migliano. 2022. Cost of Internet Shutdowns Report 2021. *Top10VPN Research*. Retrieved from <https://www.top10vpn.com/research/cost-of-internet-shutdowns/2021/>
- [481] Joss Wright. 2012. *Regional Variation in Chinese Internet Filtering*. University of Oxford. Retrieved from https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2265775_code1448244.pdf?abstractid=2265775&mirid=3
- [482] Robin B. Wright. 2011. *Rock the Casbah: rage and rebellion across the Islamic world* (1st ed.). Simon & Schuster, New York.
- [483] Tim Wu. 2003. Network neutrality, broadband discrimination. *Journal on telecommunications & high technology law* 2, 1 (2003).
- [484] Yinglian Xie, Fang Yu, Kannan Achan, Eliot Gillum, Moises Goldszmidt, and Ted Wobber. 2007. How dynamic are IP addresses? In *Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications*, ACM, Kyoto Japan, 301–312. DOI:<https://doi.org/10.1145/1282380.1282415>
- [485] Ruohan Xiong and Jeffrey Knockel. 2019. An Efficient Method to Determine which Combination of Keywords Triggered Automatic Filtering of a Message. In *Free and Open Communications on the Internet*, USENIX. Retrieved from https://www.usenix.org/system/files/foci19-paper_xiong.pdf
- [486] Xueyang Xu, Z. Morley Mao, and J. Alex Halderman. 2011. Internet Censorship in China: Where Does the Filtering Occur? In *Passive and Active Measurement*, Neil Spring and George F. Riley (eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 133–142. DOI:https://doi.org/10.1007/978-3-642-19260-9_14
- [487] Diwen Xue, Benjamin Mixon-Baca, ValdikSS, Anna Ablove, Beau Kujath, Jedidiah R. Crandall, and Roya Ensafi. 2022. TSPU: Russia’s decentralized censorship system. In *Proceedings of the 22nd ACM Internet Measurement Conference*, ACM, Nice France, 179–194. DOI:<https://doi.org/10.1145/3517745.3561461>

- [488] Diwen Xue, Reethika Ramesh, Arham Jain, Michalis Kallitsis, J. Alex Halderman, Jedidiah R. Crandall, and Roya Ensafi. 2022. OpenVPN is Open to VPN Fingerprinting. In *USENIX Security Symposium*, USENIX. Retrieved from <https://www.usenix.org/system/files/sec22-xue-diwen.pdf>
- [489] Diwen Xue, Reethika Ramesh, Valdik S S, Leonid Evdokimov, Andrey Viktorov, Arham Jain, Eric Wustrow, Simone Basso, and Roya Ensafi. 2021. Throttling Twitter: an emerging censorship technique in Russia. In *Proceedings of the 21st ACM Internet Measurement Conference*, ACM, Virtual Event, 435–443. DOI:<https://doi.org/10.1145/3487552.3487858>
- [490] Maria Xynou, Simone Basso, Ramakrishna Padmanabhan, and Arturo Filastò. 2021. Uganda: Data on internet blocks and nationwide internet outage amid 2021 general election. *OONI Reports*. Retrieved from <https://ooni.org/post/2021-uganda-general-election-blocks-and-outage/>
- [491] Maria Xynou and Arturo Filastò. 2016. How Uganda blocked social media, again. *OONI Reports*. Retrieved from <https://ooni.org/post/uganda-social-media-blocked/>
- [492] Maria Xynou and Arturo Filastò. 2020. Belarus protests: From internet outages to pervasive website censorship. *Open Observatory of Network Interference*. Retrieved from <https://ooni.org/post/2020-belarus-internet-outages-website-censorship/>
- [493] Maria Xynou and Arturo Filastò. 2021. Zambia: Social media blocked amid 2021 general elections. *OONI Reports*. Retrieved from <https://ooni.org/post/2021-zambia-social-media-blocks-amid-elections/>
- [494] Maria Xynou and Arturo Filastò. 2021. How countries attempt to block Signal Private Messenger App around the world. *Open Observatory of Network Interference*. Retrieved from <https://ooni.org/post/2021-how-signal-private-messenger-blocked-around-the-world/>
- [495] Maria Xynou, Arturo Filastò, and Moses Karanja. 2019. Ethiopia: From internet blackouts to the blocking of WhatsApp and Telegram. *OONI Reports*. Retrieved from <https://ooni.org/post/ethiopia-whatsapp-telegram/>
- [496] Maria Xynou, Arturo Filastò, Tawanda Mugari, and Natasha Msonza. 2019. Zimbabwe protests: Social media blocking and internet blackouts. *OONI Reports*. Retrieved from <https://ooni.org/post/venezuela-internet-censorship/>
- [497] Tarun Kumar Yadav, Akshat Sinha, Devashish Gosain, Piyush Kumar Sharma, and Sambuddho Chakravarty. 2018. Where The Light Gets In: Analyzing Web Censorship Mechanisms in India. In *Internet Measurement Conference*, ACM. DOI:<https://doi.org/10.1145/3278532.3278555>
- [498] Stephanie Yang. 2021. China Appears to Block Popular Encrypted Messaging App Signal. *The Wall Street Journal*. Retrieved from <https://www.wsj.com/articles/china-appears-to-block-signal-one-of-last-popular-encrypted-messaging-apps-11615883434>

- [499] Bilge Yesil, Efe Kerem Sozeri, and Emad Khazraee. 2017. *Turkey's Internet Policy after the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance*. University of Pennsylvania, Philadelphia, PA. Retrieved from <https://repository.upenn.edu/internetpolicyobservatory/22/>
- [500] Your Freedom. *Your Freedom*. Retrieved from <https://www.your-freedom.net/>
- [501] Savvas Zannettou, Tristan Caulfield, Emiliano De Cristofaro, Michael Sirivianos, Gianluca Stringhini, and Jeremy Blackburn. 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, 218–226. DOI:<https://doi.org/10.1145/3308560.3316495>
- [502] Saman Taghavi Zargar, James Joshi, and David Tipper. 2013. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials* 15, 4 (2013), 2046–2069. DOI:<https://doi.org/10.1109/SURV.2013.031413.00127>
- [503] Aaron Zelinsky. 2011. Misunderstanding the Anti-Federalist Papers: The Dangers of Availability. *Alabama Law Review* 63, (2011). Retrieved from <https://www.law.ua.edu/pubs/lrarticles/Volume%2063/Issue%205/4%20Zelinsky%201067%20-%201113.pdf>
- [504] Kim Zetter. 2016. The Sony Hackers Were Causing Mayhem Years Before They Hit the Company. *WIRED*. Retrieved from <https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company/>
- [505] Pengxiong Zhu, Keyu Man, Zhongjie Wang, Zhiyun Qian, Roya Ensafi, J. Alex Halderman, and Haixin Duan. 2020. Characterizing Transnational Internet Performance and the Great Bottleneck of China. *Measurement and Analysis of Computing Systems* 4, 1 (2020). Retrieved from <https://dl.acm.org/doi/pdf/10.1145/3379479>
- [506] Tao Zhu, David Phipps, Adam Pridgen, Jedidiah R. Crandall, and Dan S. Wallach. 2013. The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions. In *USENIX Security Symposium*, USENIX. Retrieved from <https://www.cs.unm.edu/~crandall/usenix13.pdf>
- [507] Jonathan Zittrain and Benjamin Edelman. 2002. *Documentation of Internet filtering in Saudi Arabia*. Berkman Center for Internet & Society, Harvard Law School. Retrieved from <https://cyber.harvard.edu/filtering/saudi-arabia/>
- [508] Jonathan Zittrain and Benjamin Edelman. 2003. Internet Filtering in China. *IEEE Internet Computing* 7, 2 (2003). DOI:<https://doi.org/10.1109/MIC.2003.1189191>
- [509] Jonathan L. Zittrain, Robert Faris, Helmi Noman, Justin Clark, Casey Tilton, and Ryan Morrison-Westphal. 2017. The Shifting Landscape of Global Internet Censorship. *SSRN Journal* (2017). DOI:<https://doi.org/10.2139/ssrn.2993485>

- [510] Hadi Zolfaghari and Amir Houmansadr. 2016. Practical Censorship Evasion Leveraging Content Delivery Networks. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, Vienna Austria, 1715–1726. DOI:<https://doi.org/10.1145/2976749.2978365>
- [511] First Amendment. *United States Constitution*. Retrieved from <https://constitution.congress.gov/constitution/amendment-1/>
- [512] Satellite Visualization. *Censored Planet*. Retrieved August 10, 2020 from <https://censoredplanet.org/data/visualizations/>
- [513] Transparent DNS Proxies. *dnsleaktest.com*. Retrieved from <https://dnsleaktest.com/what-is-transparent-dns-proxy.html>
- [514] nDPI - Open and Extensible LGPLv3 Deep Packet Inspection Library. *ntop.org*. Retrieved from <https://www.ntop.org/products/deep-packet-inspection/ndpi/>
- [515] Pluggable Transports. *Obfuscation collaboration web presence*. Retrieved from <https://obfuscation.github.io/>

VITA

Alexander Master earned a Bachelor of Science degree in Computer and Information Technology from Purdue University in 2013, a Master of Engineering in Cybersecurity from the University of Maryland in 2020, and a Doctor of Philosophy in Information Security degree from Purdue University in 2023. His research interests focus primarily on Internet censorship, privacy, and digital operational security (OPSEC). He has also contributed to work related to election security and published articles educating the general public about online cybersecurity and privacy practices.

Alex was commissioned as a U.S. Army field artillery officer in 2013 and transitioned to become a cyber officer in 2016. He deployed in support of the NATO mission Operation Resolute Support in 2015 as part of the conflict in Afghanistan. Afterwards he assisted in the planning and conduct of cyberspace operations for several years as a member of U.S. Cyber Command. Alex spent three years as a graduate researcher at Purdue University under the Center for Education and Research in Information Assurance and Security (CERIAS) and contributed to efforts within the Purdue Homeland Security Institute (PHSI).

Starting in the fall of 2023, Alex will serve as a Research Scientist with the Army Cyber Institute, located at the United States Military Academy in West Point, New York, USA.