Digital Control: National Tactics of Internet Censorship

Julia Lenz[1], Simon Volpert[1], Sebastian Zillien[1],
Philip Rünz[2], Luca Caviglione[3], Steffen Wendzel[1]

[1] University of Ulm, Ulm, Germany
name.surname@uni-ulm.de
https://www.uni-ulm.de/en/in/omi/
[2] FernUniversität in Hagen, Hagen, Germany
[3] CNR - IMATI, Genova, Italy
name.surname@ge.imati.cnr.it

Abstract. Internet censorship has evolved from simple content blocking to complex socio-technical control systems. While prior surveys primarily focus on techniques such as DNS poisoning or deep packet inspection, they rarely examine how national contexts shape deployments. This paper presents a comparative analysis of 20 countries, conceptualizing censorship as a four-dimensional architecture comprising legal regulation, technical filtering, information flooding and infrastructural denial. Synthesizing existing research across regime types, we identify a systematic "sliding scale" in the dominant locus of control: democratic systems rely mainly on regulatory mechanisms, hybrid regimes combine filtering with narrative manipulation, and highly restrictive states block physical access. Our findings show that censorship adapts to political and institutional contexts, often shifting its control across domains calling for broader measurement approaches beyond the network layer.

Keywords: Internet Censorship · Censorship Measurement · Free Internet Access · TCP/IP · DNS · Internet Technology

1 Introduction

This is a pre-print. The published version appeared in Proc. European Interdisciplinary Cybersecurity Conference (EICC 2026), Springer, 2026.
https://doi.org/10.1007/978-3-032-28957-5_5.

The Internet enables large-scale connectivity and access to vast amounts of information and services. At the same time, governments, corporate, institutional, and non-governmental organizations may deem certain interactions or content inappropriate due to political, religious, cultural, legal, or security-related concerns. Internet censorship therefore aims to restrict access to and exchange of information considered undesirable by a censor [32].

Given the growing importance of digital communication infrastructures, a substantial body of research examines the technical mechanisms used to enforce

censorship. Recent surveys such as [90] review network-level filtering techniques and detection methods, complementing previous research in [51], which surveyed censorship trends across 70 countries. The resulting snapshot is somewhat alarming, since advanced techniques ranging from deep packet inspection (DPI) to per-protocol manipulation are nowadays prevalent. Other notable research includes the seminal work in [6] providing a comprehensive but now outdated view of Internet censorship and the work in [87] analyzing real-world censorship behaviors. Together, these studies offer detailed information on *which* techniques are deployed and *where* they occur. However, existing research focuses on identifying the *presence* of specific filtering capabilities (e.g., DNS tampering or TLS filtering) [51] rather than examining how these mechanisms are embedded within broader political, legal, and infrastructural systems. Censorship is not merely a technical intervention, but a multi-dimensional system of control shaped by differences in institutional design, regulatory frameworks, and state capacity. Consequently, systematic comparison of these socio-political architectures across regime types remains limited [4,90,91].

This paper addresses this gap through a comparative and country-focused analysis of Internet censorship. Drawing on the annual "Freedom on the Net" (FOTN) report [32] and complementary sources, we examine how national actors implement and operate censorship. Rather than cataloging individual techniques, we identify distinct *models of control* and conceptualize censorship as a multidimensional architecture. Accordingly, this paper asks: *How do national Internet censorship architectures vary across regime types, and which control mechanisms emerge as dominant within different political contexts?* To answer this question, we identify recurring patterns, overlaps, and singularities across countries to synthesize evidence into a four-dimensional analytical framework capturing legal, technical, informational, and infrastructural dimensions of censorship. Our contributions are threefold: (i) we introduce a structured model for describing national censorship architectures beyond technique-level inventories; (ii) we provide a cross-country mapping of these dimensions; (iii) we propose a novel "sliding scale" model for linking dominant control mechanisms to political contexts. Our paper is accompanied by a project website: https://atlas.omi.uni-ulm.de/

The remainder of this paper is structured as follows. Sect. 2 describes the methodology and sampling strategy. Sect. 3 presents the country-specific findings. Sect. 4 discusses commonalities, trends, and shifts as well as overall implications, limitations and future research directions. Lastly, Sect. 5 concludes the paper.

2 Methodology

To enable structured cross-country comparison while preserving analytical depth, we do not cover all countries worldwide. Instead, we analyze 20 countries through a stratified random sampling approach based on the categorization of the 2025 FOTN report [32]. Four sampling strata were constructed. Three correspond to the FOTN categories: "not-free", "partially free", "free", from which five countries were randomly selected each. The fourth stratum consists of countries

"not covered" by FOTN, from which five additional cases were drawn. Although these countries lack an Internet-specific FOTN rating, Freedom House assesses them in its separate annual report "Freedom in the World" [31], providing a broader "World" Freedom Score measuring political rights and civil liberties. Accordingly, Tab. 1 reports both the FOTN "Internet" score (where available) and the "World" score of our final sample, also highlighted in Fig. 1. For "not covered" countries, only the latter exists. Within each stratum, eligible countries were randomly sampled with a uniform probability. No geographic quotas were imposed, as the primary analytical variable is regime type rather than regional distribution (e.g., continent-based balancing). Furthermore, each country is analyzed using the following four-dimensional framework:

(i) **Legal/regulatory controls** (•): Restrictive laws and regulations making undesired topics illegal.
(ii) **Technical filtering** (•): Rule-based filtering of undesired content.
(iii) **Information flooding** (•): Propaganda through bot/troll armies, narrative manipulation, and fake news.
(iv) **Infrastructure denial** (•): (Near) total Internet shutdowns, infrastructure-level disconnects.

These dimensions are not mutually exclusive but provide a structured lens for comparing censorship architectures across national contexts. Throughout the paper, color-coded markers annotate text and tables: a solid bullet (•) denotes a primary censorship mechanism and an open circle (○) indicates a secondary or occasional application. Country assessments are based on qualitative synthesis of peer-reviewed studies, reports from established digital rights organizations, regulatory documents, and reputable news outlets. Sources were identified through academic database queries, citation snowballing, and web searches.

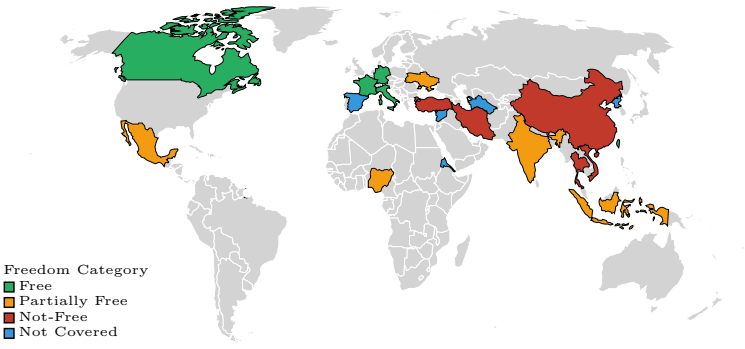

Fig. 1. Geographical distribution of the 20 selected countries. Highlighted regions indicate the nations included in our analysis across the various FOTN categories.

Table 1. Random selection of five countries per category. "World" and "Internet" denote Freedom in the World and Freedom on the Net scores, respectively. Cell colors map a continuous scale from 0 (Red/Worst) to 100 (Green/Best).

Country	World	Internet	Country	World	Internet
Not-Free			**Free**		
China	9	9.0	Canada	97	85.0
Iran	11	13.0	France	89	76.0
Thailand	34	39.0	Germany	95	74.0
Turkey	33	31.0	Italy	89	74.0
Vietnam	20	22.0	Taiwan	94	79.0
Partially Free			**Not Covered**		
India	63	51.0	Eritrea	3	N/A
Indonesia	56	48.0	North Korea	3	N/A
Mexico	59	61.0	Spain	90	N/A
Nigeria	44	59.0	Syria	5	N/A
Ukraine	51	62.0	Turkmenistan	1	N/A

3 Censorship Deployments in Selected Countries

This section presents country-specific analyses of Internet censorship. As most governments rarely disclose official blocklists or filtering infrastructure, our insights rely mostly on indirect evidence, such as long-term measurement studies that track blocking and traffic alternations across time and locations [90].

3.1 FOTN Non-free Countries

China One of the most sophisticated censorship systems worldwide is operated by China, integrating technical censorship measures with a rigid legal framework. Through intermediary liability, the state delegates censorship duties to private platforms, compelling them to police content under threat of heavy fines or license revocation [24] •. The network-level censorship is primarily implemented through the *Great Firewall* (GFW), a large-scale filtering system designed to detect and block undesirable traffic, particularly encrypted protocols which are critical for censorship circumvention [92] •. The GFW also employs *residual censorship* [13], whereby once a connection attempt has been flagged, the same traffic tuple may remain blocked for 120 to 180 seconds, effectively suppressing repeated connection attempts. Beyond filtering, coordinated "information flooding" shapes online discourse •. Han highlights the role of the "Fifty Cent Army" (*wumaodang*), whose members engage in "discourse competition" by posting pro-government narratives and diverting discussions away from critical topics [38]. During politically sensitive periods, China occasionally resorts to infrastructural interventions such as temporary Internet shutdowns and DNS tampering [51] ○. Although less common, these measures illustrate its ability to escalate censorship through direct network disruptions.

Iran Among the most repressive Internet environment worldwide is Iran •. Authorities regularly intensify restrictions around elections, including criminalizing regime-critical content [10,32]. Censorship practices date back to at least 2002, when roughly 50% of the most visited websites were blocked and over 95% of adult content filtered [10] •. Since then, DPI, DNS tampering, and HTTP keyword filtering are used to target political, social, and security-related content.[14,40]. In 2020, additional protocol-based filtering that inspects the first two client packets of DNS, HTTP, and HTTPS traffic were introduced. If protocol fingerprints do not match expected patterns, flows are dropped for 60 seconds [14]. Encrypted DNS, including DoT, is also blocked [11], while measurement studies show inconsistencies in protocol-level enforcement, such as the continued accessibility of unencrypted HTTP/2 traffic [47]. The state promotes a curated information environment through the "National Internet", prioritizing domestic services and enabling stronger narrative control •. During nationwide protests in 2019, authorities used this infrastructure to substitute global connectivity and have since pursued a more isolated and potentially religiously framed "Halal Internet" [40]. Beyond filtering, throttling and connectivity disruptions have also been widely used •. Mainly SSH and other encrypted flows have been degraded via TCP packet drops [29]. During the most recent protests, which began in late December 2025, authorities have blocked Internet access while also intensifying forceful suppression of demonstrations [5].Following the escalation on 28 Feb 2026, Iran reimposed a near-total wartime "international kill-switch and whitelisting" model. External connectivity dropped to near-zero (∼98% traffic loss) [22,58], while domestic intranet access persisted and politically vetted "white-SIM / tiered access" channels expanded alongside coercive enforcement (SMS prosecution threats targeting circumvention attempts) [30].

Thailand The censorship system of Thailand relies on *lèse-majesté* laws and the expanded 2017 Computer Crime Act, which are used as primary tools to prosecute online speech •. Enforcement is bolstered by the 2010 Cyber Scout program and the "Social Sanction" network mobilizing citizens to report dissent. Together, these mechanisms create a climate of self-censorship, illustrated by the 2024 arrest of two Prachatai journalists covering anti-monarchy graffiti [32]. Technical filtering is less documented, although studies report blocking related to religious debates and pornography [1] •. Proposals for a centralized "single gateway" architecture (resembling the GFW) have been discussed, but doubts remain regarding their political feasibility and implementation [48]. Monitoring also occurs at the ISP level, where active probing techniques are used to identify infected user machines and suspicious traffic patterns, which can subsequently inform blocking decisions or the detection of circumvention tools [15]. Studies of circumvention practices further indicate that most users adopt standard VPNs or Tor, while a minority resorts to manual workarounds like RSS feeds [33]. Evidence also points to coordinated information manipulation, including large-scale fabricated Tweets to make the regime appear more popular [79] •. The government has additionally employed targeted infrastructural controls ○. In mid-

2025, authorities ordered telecom providers to shutdown broadband and mobile Internet links to Cambodia near the border region, officially citing cybersecurity concerns [83]. Although framed as an anti-scammer measure, this restriction reflects the willingness to enforce disruptions during geopolitical disputes.

Turkey A robust legal censorship regime is maintained by Turkey, frequently issuing content takedown requests under vague laws, restricting criticism of political leadership [81,88] •. For example, large volumes of such requests were directed at Twitter in 2015, and internationally operating platforms often comply with such country-specific removal mechanisms [81,88]. Moreover, in 2014, the government attempted to block access to both Twitter and YouTube by acting over DNS. To prevent users from circumventing these blocks through alternative DNS services, Turkish ISPs began advertising a "bogus" BGP route to divert traffic intended for OpenDNS and Google DNS servers [81]. At the technical level, censorship includes DNS tampering, BGP hijacking, TLS-based filtering and DPI deployed by ISPs to enable user profiling and the blocking of selected keywords or destinations [51] •. Turkey also relies on a decentralized online propaganda network known as "AKTrolls", who harasses dissidents and floods platforms with pro-regime content [72] •. Furthermore, authorities have occasionally resorted to infrastructural interventions ○. Internet throttling and regional shutdowns have been observed during politically sensitive periods, including protests and the 2016 coup attempt [51].

Vietnam Internet censorship in Vietnam follows a "bamboo diplomacy" approach characterized by flexibility and pragmatism [60] •. Rather than deploying a centralized firewall, the Communist Party allows Western platforms like Facebook and Google to operate while simultaneously pressuring them to comply with domestic content removal requests [49]. This strategy of "platform coercion" allows the state to harness the economic benefits of global connectivity while maintaining control over "toxic" content. Under fear-based control, effectively summarized by the proverb "kill one to warn one hundred" [19], high-profile arrests target users who cross vague "red lines", such as criticizing key leaders, reinforcing a climate of self-censorship [49]. Technically, censorship relies on a combination of DNS tampering, IP blocking, and firewall-based filtering, with inconsistencies observed across ISPs (e.g., FPT vs VNPT), suggesting that enforcement varies across the national network infrastructure [49] •. Complementing these technical measures, "Force 47", a military cyber-unit of over 10,000 agents, and "public opinion shapers" (*Dư Luận Viên*) flood social media with pro-state narratives and counter critical voices [60] •. Moreover, authorities utilize "prior restraint" as cultural control by vetting musical and artistic works before release, reinforcing broader patterns of self-censorship [62]. In addition to account-based access restrictions, bloggers and activists have reported being cut off from Internet services, placed under surveillance, or denied access to mobile networks, showcasing the selective use of connectivity restrictions [32] ○.

3.2 FOTN Partially Free Countries

India Censorship in India is legally grounded in Section 69A of the Information Technology Act, allowing the government to order takedowns of online content and block websites deemed a threat to sovereignty, public order or national security [43] •. These provisions enable the restriction of access to selected Internet destinations [61]. At the technical level, blocking is typically implemented through DNS and HTTP filtering, although enforcement varies considerably across ISPs [78] •. Some providers block only subsets of targeted sites or apply their own filtering policies, while others leave content accessible, highlighting a decentralized and sometimes arbitrary system [78]. The network topology further shapes censorship: roughly ∼1% of autonomous systems (AS) carry around 95% of the traffic to blocked sites, creating a centralized structure that could support large-scale filtering [36]. For mobile apps, blocking is typically enforced directly by service providers rather than through network-level interception [36]. These technical efforts are reinforced by extensive social manipulation •. Party-affiliated IT cells and "cyber troops" use social media platforms such as WhatsApp to spread disinformation, deploy bot networks, and amplify partisan narratives, particularly during elections [20]. Simultaneously, studies report growing levels of self-censorship among content creators on streaming platforms, who may voluntarily restrict expression to maintain access to the domestic large "unfettered" digital market [53]. Uncommonly among democracies, the state frequently resorts to regional Internet shutdowns to control unrest, as seen during the Kashmir lockdown and protests surrounding the Citizenship Amendment Act [56] ○.

Indonesia The censorship regime of Indonesia is described as an emerging "digital authoritarianism" [77], and grounded in the Electronic Information and Transactions Law and Ministerial Regulation 5 •. These regulations require platforms to register with the government and grant authorities broad powers to order content takedowns deemed illegal or harmful [50]. Enforcement is decentralized: the Ministry of Communication and Informatics maintains the *TrustPositif* blocklist, while implementation is carried out by individual ISPs. The censorship is mainly implemented through DNS hijacking, where ISPs redirect requests for blacklisted domains to warning pages such as "Internet Positif" •. The decentralized enforcement model often leads to inconsistent blocking and collateral damage [74]. Monitoring technologies such as DPI systems and automated "Cyber Crawling" programs complement these filtering mechanisms by detecting and tracking undesirable content, thereby enabling more targeted blocking [69].Coordinated information manipulation also occurs through government-aligned influencers and so-called "buzzers" who amplify pro-government narratives and harass critics on social media [77] •. Instead of total connectivity blackouts, the government utilizes tactical bandwidth throttling during crises ○. During the 2019 post-election riots, authorities slowed upload speeds on platforms like WhatsApp and Facebook to curb viral image and video sharing while preserving text functionality [74].

Mexico While Mexico formally prohibits state-mandated Internet shutdowns under the 2021 IFT Guidelines, Article 190 of the 2014 Telecommunications Law allows authorities to suspend telecommunication services to prevent criminal activity, granting the state conditional power over connectivity infrastructure [2] ○. Technical censorship is relatively rare and often driven by economic motivations ○. In 2006, a major national provider blocked access to `www.skype.com` to protect revenue from long-distance calls [28]. Measurements of Tor connectivity between 2010 and 2019 also suggest that some ISPs intermittently blocked routes to Tor directory authorities, although disruptions may also stem from misconfigurations, NAT behavior, or DPI-based filtering [44]. Some content control also occurs outside the network layer. For instance, a recent work addresses how distributed media such as anime is often "sanitized" before release, though users frequently bypass restrictions through P2P file sharing of uncensored versions [46]. The authors highlight the difficulty of enforcing blockages due to the ability of P2P to route data beyond national borders [46]. Lastly, coordinated information campaigns have been observed •. As an example, the government shaped the discussion on the COVID-19 pandemic performed via Twitter [66].

Nigeria Online censorship in Nigeria is primarily enforced through legal instruments such as the 2015 Cybercrime Act and various regulatory provisions, including anti-blasphemy statutes •. These laws have been used to prosecute journalists and social media users, encouraging self-censorship and fostering a chilling effect online. Authorities have also invoked Section 146 of the 2003 Communications Act, to compel ISPs to block websites, often without transparent procedures [32]. Although studies document the proliferation of laws restricting online contents as well as movies and games, a comprehensive technical evaluation of the censorship infrastructure remains limited [37]. Technical filtering approaches include DNS manipulation, TCP injection, and blockpage delivery, as observed during the 2017-2018 measurement campaign by ICLab [61] •. Nonetheless, these mechanisms appear to be implemented inconsistently and with limited oversight. Political actors also employ troll networks and disinformation campaigns to shape public opinion during elections and protests, using bots, fake accounts, and state-linked influencers [3] •. Authorities have additionally resorted to infrastructural restrictions during periods of political tension, including regional Internet and mobile network shutdowns in 2021 and a nationwide Twitter-ban after the platform removed a presidential tweet [8] ○.

Ukraine The censorship model in Ukraine reflects the country's defensive response to Russian "hybrid warfare" and military aggression conducted through digital disinformation on the "online battlefield" [17]. Rather than suppressing domestic dissent, restrictions focus on countering foreign influence and safeguarding the national information space. Prior to the invasion, the 2017 Law "On Sanctions" enabled the blocking of major Russian platforms (e.g., Odnoklassniki, Yandex), creating what Golovchenko [35] terms a "friction-based" model that increased the "cost" of access (e.g., forcing VPN use) rather than imposing a complete

blockade, encouraging migration toward domestic and Western alternatives •. Since 2022, censorship has intensified under martial law through the 2022 Law "On Media" and amendments to the Criminal Code (Article 436-2), criminalizing pro-Russian narratives and effectively merging network-level filtering with punitive legal restrictions [17]. Technically, the National Centre for Operations and Technology Management of Telecommunications Networks issues direct blocking orders to network operators, resulting in the blocking of over 48 million Russian IP addresses and numerous AS associated with Russian infrastructure [17] •. Wartime information management also includes centralized broadcasting through the nationwide "Unified News" telethon, designed to counter disinformation and maintain a consistent public narrative [70] ○. Systematic Internet shutdowns have not been used as a censorship tool. Most connectivity disruptions during the war result from Russian attacks on infrastructure and ISP-level rerouting in occupied territories [70]. Internationally, similar restrictions have been adapted by the EU against Russian state media such as RT and Sputnik [73].

3.3 FOTN Free Countries

Canada Internet governance in Canada is increasingly shifting toward a model of "soft censorship" based on regulatory control rather than large-scale technical filtering. Judicial site-blocking orders and platform mandates have introduced limited forms of network-level intervention [26] •. In the *GoldTV* case, courts authorized ISPs to block IPTV piracy services, establishing a precedent for court-mandated blocking and filtering under copyright enforcement [25]. Recent legislation further expands regulatory influence. Bill C-11 (Online Streaming Act), grants authorities indirect influence over platform algorithmic "discoverability", manipulating what users see in their feeds based on national criteria rather than user preference [39]. Similarly, the *Online News Act* (Bill C-18), intending to support the Canadian news industry by forcing dominant digital platforms to pay the domestic organizations, triggered major platform responses. Meta decided to block news content for users, significantly altering the country's information ecosystem, affecting accessibility [82]. Additional proposals such as Bill C-63 aim to regulate "legal but harmful" speech, intensifying debates about platform liability and potential self-censorship [23,42]. While such filtering remains limited in scope, the government has also used DNS tampering in exceptional cases, such as blocking COVID-19–related content during the pandemic [45] •.

France The regulation of online content in France primarily relies on legal and regulatory mechanisms. A notable example is the "graduated response" system introduced through the HADOPI framework, which allows authorities to identify users distributing copyrighted material via peer-to-peer networks and report their IP addresses to law enforcement agencies [54] •. These measures focus on deterrence and enforcement of intellectual property law rather than broad content blocking. Although relatively limited in scope, technical filtering mechanisms have also been documented ○. Measurement studies indicate the use of DNS

and HTTP/keyword filtering [51], mainly to mitigate child pornography or as a reaction against the 2001 terrorism wave [16]. However, even if some works hint at the use of filtering techniques, to the best of our knowledge there is no prior literature analyzing used techniques or their pervasiveness.

Germany In Germany, online regulation relies primarily on legal enforcement and content removal rather than systematic network-level filtering [32]. The state briefly employed technical blocking through the *Zugangserschwerungsgesetz* (2010-2011), targeting websites hosting child exploitation material via DNS-based filtering [51] • ○. After its repeal, policy shifted toward content removal and platform liability. A central pillar is the *Network Enforcement Act* (NetzDG), which requires large social media platforms to remove illegal content within strict timeframes, strengthening enforcement of existing criminal law while raising concerns about potential overblocking and chilling effects on expression [85]. Today, enforcement focuses on removing illegal content, including extremist material (e.g., Holocaust denial) and copyright violations. Takedown procedures are coordinated through the *Clearingstelle Urheberrecht im Internet*, facilitating cooperation between rights holders, regulators, and ISPs.

Italy State-mandated content filtering has increased in Italy, primarily targeting copyright violations •. The national telecom regulator AGCOM operates the "Piracy Shield" system, which allows domain and IP-level blocking of services associated with illegal streaming. Internet and VPN providers must enforce these blocking orders, typically triggered through a ticket-based reporting system that flags IPv4/v6 addresses or domain names responsible for copyright violations or illegal activities. Critics argue that the system lacks sufficient oversight and may lead to overblocking and collateral damage. In fact, endpoints are blocked after a ticket is submitted, but "Piracy Shield" cannot handle the presence of shared IP addresses or DNS entries. A notable incident in October 2024 showed how a misclassification led to the blocking of `drive.usercontent.google.com`, disrupting access to Google Drive and YouTube for many users [7] •. Measurement studies also show inconsistent enforcement and frequent circumvention via open or foreign DNS resolvers [64]. In addition to DNS filtering, some operators deploy TCP and HTTP tampering, for instance, Vodafone applies HTTP proxy inspection for more targeted filtering [4].

Taiwan As a digitally open democracy, Taiwan faces asymmetric threats from China, including attempts at "extraterritorial censorship" and cognitive warfare campaigns targeting its public discourse [75]. Censorship often arises indirectly through economic and political pressure rather than direct state control •. Media outlets with business ties to China often self-censor, a form of "outsourced" control described as part of the "3 Is" of China's strategy: propaganda *Initiation*, media *Investment* in local media outlets, and *Ideological* polarization [80,75]. As a direct countermeasure to the "Investment" strategy, the National

Communications Commission revoked the broadcast license of the pro-China television channel *CtiTV* in 2020, citing repeated misinformation violations [75]. Rather than relying on extensive technical filtering, Taiwan focuses on countering disinformation campaigns ○. Malicious foreign-linked accounts amplify polarizing narratives online [59], while a "whole-of-society" response involving journalists, civil society, and academic institutions works to collaboratively detect and debunk disinformation [71]. Technical blocking remains minimal ○. In a few national security cases, authorities have restricted certain Chinese streaming platforms (OTT services). The state also promotes "digital democracy" through platforms such as *vTaiwan*, which use algorithms to visualize public consensus and facilitate deliberative policymaking rather than manipulate information visibility [55].

3.4 FOTN Non-covered Countries

Eritrea As an extreme case of "stable authoritarianism", Eritrea enforces censorship primarily through infrastructure denial and systemic information control [65]. Control is embedded in the broader political and institutional system: from physical surveillance to an educational curriculum that restricts digital literacy ○. Some argue that the state employs a strategy of "mis-education", in which the curriculum is designed to produce docile students to secure obedience and discourage political mobilization [76]. Information control is reinforced by a state monopoly on media ○. Since banning independent outlets in 2001, domestic news has been tightly controlled through government-driven channels [18], with occasional shutdowns during unrest [65]. Traditional network-level filtering is minimal, as the regime largely prevents widespread Internet use ○. Thus, Internet penetration remains extremely low (approx. 1.3%),with access tightly controlled by the state-owned monopoly *EriTel* [76] ●. Mobile data services are virtually nonexistent, and most users rely on state-monitored Internet cafés with slow speeds, high costs and physical surveillance [34].

North Korea Near-total isolation from the global Internet characterizes information control in North Korea, which is largely enforced via strict legal and punitive measures. Unauthorized access to foreign information sources is criminalized, and citizens attempting to connect to the Internet risk severe penalties, including imprisonment [9] ○. Traditional filtering is largely unnecessary because only a few government-approved institutions and elites can access the outside Internet ○. Consequently, domestic information flows are tightly controlled through state-run media and the highly curated national intranet "Kwangmyong", which hosts only government-approved websites and services ○. Thus, propaganda exists but is embedded in infrastructural isolation. By preventing physical connectivity to the global Internet, the regime avoids needing sophisticated filtering systems ●. This isolation hinders Internet measurement efforts, as there is almost no traffic to or from the outside world.

Spain A recent analysis identified multiple censorship measures in response to political conflicts [88], most notably during the 2017 Catalan independence

referendum •. Authorities ordered the blocking of websites and applications associated with the referendum, providing a legal basis for subsequent network-level interventions. ISPs used technical filtering such as DNS manipulation, CDN node seizures, HTTP blocking with DPI, and additional TLS-layer censorship •. For example, Vodafone deployed SNI blocking, which aimed to alter the TLS extension used to route data through HTTPS-reachable destinations hosted on the same physical machine. Other blockages against TLS traffic have been inferred by considering the presence of many certificate verification failures plaguing some AS, suggesting the presence of TLS intercept attempts [52].

Syria Internet censorship in Syria has a long history closely tied to regime stability and political control. Since the late 1990s, authorities have restricted access to email, FTP, and blocked foreign political content using centralized infrastructure, proxies and imported filtering tools [41] •. Technical censorship includes blocking IP subnets (e.g., those linked to Israel), keyword filtering, and disabling access to instant messaging services and Facebook plugins [21] •. Analyses of leaked proxy logs reveal extensive HTTP filtering and countermeasures against VPNs and circumvention tools. By 2012, popular VPN protocols such as PPTP and L2TP had largely been rendered ineffective [27]. Despite these restrictions, users appear to be aware of the censorship tactics and frequently attempt to access blocked content via Tor, VPNs, and cached versions of blocked websites. In addition, pro-regime cyber groups such as the "Syrian Electronic Army", have conducted coordinated disinformation campaigns and harassment against opposition voices online [12] •. Political changes following the leadership transition in December 2024 have introduced uncertainty regarding the future of the censorship system, with some reports suggesting a possible loosening of controls, although the long-term trajectory remains unclear [84] ○.

Turkmenistan The Internet environment in Turkmenistan ranks among the most restrictive worldwide. Although official legislation promotes digital development, in practice the state tightly controls connectivity, monopolizes access, enforces pervasive censorship and opaque cybersecurity controls [67] •. Most VPN use is prohibited, with violations punishable by imprisonment, reflecting the regimes punitive approach [89]. Authorities justify these restrictions as part of the "Golden Age" ideology, emphasizing national unity through informational isolation [68]. Technical filtering is extensive, including DNS tampering, HTTPS blocking, port-agnostic filtering, and large-scale IP/domain bans [57] •. Measurement campaigns identified more than 122,000 blocked domains from a sample of 15.5 million, often due to overly broad filtering rules causing substantial collateral damage [63]. Port filtering is also severe: in one measured AS, only ∼1,150 of 65,535 ports remained accessible [63]. These policies vary across networks and IP prefixes, reflecting an inconsistent enforcement architecture. Authorities have also periodically deployed shutdowns for preemptive censorship, collective punishment, or protest suppression rather than genuine emergency response [86] •. In April 2023, access to roughly 75% of global IP addresses was reportedly blocked.

4 Discussion: The Sliding Scale of Control

This section synthesizes the cross-country findings and develops a comparative interpretation of the identified censorship architectures. Building on data presented in Tab. 2, we highlight recurring patterns across regime types and derive the proposed "sliding scale" model. Moreover, we discuss limitations and future directions.

Table 2. Global Spectrum of Control: Censorship Mechanisms by FOTN Status

Country	FOTN Status	Infrastructure (Shutdowns/Intranet)	Tech Filtering (DNS/IP/DPI)	Info Flooding (Trolls/Bots)	Legal/Reg (Fines/Orders)
China	Not Free	○	•	•	•
Iran	Not Free	•	•	•	•
Thailand	Not Free	○	•	•	•
Turkey	Not Free	○	•	•	•
Vietnam	Not Free	○	•	•	•
India	Partially Free	○	•	•	•
Indonesia	Partially Free	○	•	•	•
Mexico	Partially Free	-	○	•	○
Nigeria	Partially Free	○	•	•	•
Ukraine	Partially Free	-	•	○	•
Canada	Free	-	•	-	•
France	Free	-	○	-	•
Germany	Free	-	○	-	•
Italy	Free	-	•	-	•
Taiwan	Free	-	○	○	•
Eritrea	Not Covered	•	○	○	○
North Korea	Not Covered	•	○	○	○
Spain	Not Covered	-	•	-	•
Syria	Not Covered	○	•	○	•
Turkmenistan	Not Covered	•	•	-	•

• = Primary Mechanism, ○ = Secondary/Occasional, - = Not Observed/Evidence Missing

4.1 Commonalities: A Spectrum of Intervention

Tab. 2 categorizes the censorship mechanisms of our selected countries, sorted by their FOTN status. Rather than a binary divide between "Free" and "Not Free," the data shows a diagonal progression in control strategies from the physical to the legal domain. We therefore combine the four intervention dimensions from our framework into three overarching models of censorship behavior, defined by their primary operating domain and freedom (Fig. 2).

Model 1: Regulatory Defense (The Legal Domain): Countries classified as "Free" (e.g., Canada, Taiwan, Germany) primarily exert control through the **Legal/Regulatory** dimension. Technical blocking is either absent or limited to specific judicial orders (e.g., Canada's *GoldTV* case or Italy's *Piracy Shield*). Here, the focus is on content regulation and platform liability rather than network interference.

Model 2: Filter & Flood (The Network Domain): As we move to "Partially Free" and "Not Free" nations like Indonesia and Vietnam, the primary mechanisms consolidate around **Technical Filtering** and **Information Flooding**. These regimes maintain connectivity for economic reasons but rely on network-level blocking (e.g., DNS poisoning) and state-sponsored narrative manipulation (e.g., Vietnam's Force 47) to curate the online environment.

Model 3: Infrastructural Denial (The Physical Domain): At the bottom of the spectrum, highly restrictive regimes like Eritrea and North Korea resort to the **Infrastructure** dimension as their primary tool. The main mechanism is preventing physical access to the global Internet entirely, creating a domestic intranet or maintaining a digital void.

Fig. 2 visualizes the synthesis of the four dimensions into three models as a "diagonal shift" in censorship strategies. As countries move from "Free" to "Not Free", control shifts from the Legal/Application (Model 1) to the Network (Model 2) and Physical dimension (Model 3). While depicted as a progression, shifts may also occur in reverse as countries liberalize and reduce reliance on infrastructural or network-level controls. Suggesting that while techniques vary, the intent to control remains constant, adapting to technological and legal capacity.

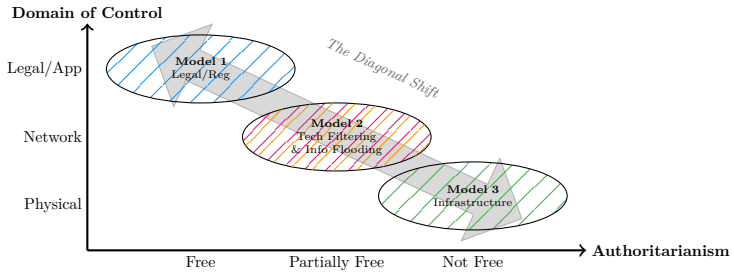

Fig. 2. Sliding Scale of Control: As authoritarianism grows, censorship shifts from legal tools to physical infrastructure.

4.2 Architectural Trade-offs in Censorship Design

Beyond regime differences, our inductive analysis reveals recurring design trade-offs in how states balance costs, precision, and collateral damage.

High Cost, High Precision. Regimes with high state capacity pursue "Engineering Maximalism." **China** pairs advanced DPI with human flooding to maintain granular control while limiting economic impact [92], whereas **Iran** relies on centralized protocol filtering for "Ideological Whitelisting," often trading usability for strict compliance [14]. These high-investment models allow states to filter dissent without severing global connectivity.

Coarse-grained Enforcement. Conversely, other nations rely on decentralized or automated blocking where collateral damage is an accepted operational

cost. In **Indonesia**, filtering is inconsistent across regions due to fragmented ISP infrastructure, while in **Italy**, the "Piracy Shield" platform prioritizes speed over accuracy, causing automated, mistaken bans of legitimate services. As noted in the recent review in [90], these policy-driven or cost-saving shortcuts often result in significant inconsistency and overblocking.

Strategic Outsourcing. A middle path is observed in **Vietnam**, which employs "Platform Coercion" to outsource censorship to foreign tech giants [49]. By pressuring companies to remove content under threat of law, the state balances economic openness with political control without assuming the massive infrastructure costs of building a domestic firewall.

4.3 Limitations and Future Directions

Our study has several limitations. First, the sample includes only about 10% of global states; although stratified by regime type, it may miss distinctive architectures in unexamined regions such as South America. Second, the analysis relies on secondary rather than primary data, consistent with the paper's goal of synthesizing existing findings into a comparative framework, but this may reduce depth for closed regimes where reliable data are scarce. The proposed four-dimensional framework should therefore be understood as a foundation rather than a definitive taxonomy. Future studies can apply these dimensions to new countries, refine coding criteria, or empirically test the regime-dependent patterns. An accompanying interactive exhibit is being developed as a continuously updated resource to map and explain global Internet censorship practices: https://atlas.omi.uni-ulm.de/.

5 Conclusion

This paper compared Internet censorship in 20 countries, focusing on national control architectures rather than technical details. We identified three distinct models: infrastructural denial in closed autocracies, filter & flood in mixed regimes, and regulatory defense in democracies. Our findings show that censorship adapts to political and institutional contexts, shifting its primary locus of control. While authoritarian regimes invest in technical firewalls to block dissent, democratic nations increasingly adopt similar mechanics under the guise of copyright protection or national security. This convergence suggests that future censorship research should move beyond traffic metrics to auditing the legal and algorithmic systems that govern information visibility. The proposed framework provides a structured baseline for systematically comparing national approaches and guiding future empirical research on evolving censorship.

Acknowledgments. We like to thank Saskia Imhof for her supportive work regarding the investigation of multiple countries.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Abdulmana, S., Saleh, B.: Coordinate negative content filtering and threat detection in Thailand on the Internet infrastructure. In: The 5th Int. Conf. on Information and Communication Technology for the Muslim World (ICT4M). IEEE (2014)
2. Access Now: Mexico: New guidelines jeopardize net neutrality and empower surveillance. https://www.accessnow.org/press-release/mexico-guidelines-jeopardize-net-neutrality/ (2021)
3. Access Now: #KeepItOn: Authorities in Nigeria must reconnect people in Zamfara North now. https://www.accessnow.org/press-release/keepiton-authorities-in-nigeria-must-reconnect-people-in-zamfara-north-now/ (2025)
4. Aceto, G., Montieri, A., Pescapé, A.: Internet censorship in Italy: An analysis of 3G/4G networks. In: 2017 IEEE Int. Conf. on Communications (ICC). IEEE (2017)
5. Aceto, G., Persico, V., Pescapè, A.: Iran's january 2026 internet shutdown (2026), https://arxiv.org/abs/2603.28753
6. Aceto, G., Pescapé, A.: Internet Censorship detection: A survey. Computer Networks **83** (2015). https://doi.org/10.1016/j.comnet.2015.03.008
7. Agenzia Nazionale Stampa Associata (ANSA): Anti-piracy shield halts google drive. https://www.ansa.it/english/news/general_news/2024/10/20/anti-piracy-shield-halts-google-drive_2e7b137e-361d-4026-a704-9895c798e65a.html (2024)
8. Al Jazeera: Twitter restricted in Nigeria after government decree. https://www.aljazeera.com/news/2021/6/5/twitter-restricted-in-nigeria-after-government-decree (2021)
9. Amnesty International: North Korea, the surveillance state. https://www.amnesty.org.uk/north-korea-surveillance-state-prison-camp-internet-phone-technology (2025)
10. Aryan, S., Aryan, H., Halderman, J.A.: Internet censorship in Iran: A first look. In: 3rd USENIX FOCI (2013)
11. Basso, S.: DNS over TLS blocked in Iran. https://ooni.org/post/2020-iran-dot/ (2020)
12. Bertram, S.K.: 'Close enough' – The link between the Syrian Electronic Army and the Bashar al-Assad regime, and implications for the future development of nation-state cyber counter-insurgency strategies. Contemporary Voices: St Andrews Journal of International Relations **8**(1) (2017). https://doi.org/10.15664/jtr.1294
13. Bock, K., Bharadwaj, P., Singh, J., Levin, D.: Your censor is my censor: Weaponizing censorship infrastructure for availability attacks. In: 2021 Ieee SPW. IEEE (2021). https://doi.org/10.1109/SPW53761.2021.00059
14. Bock, K., Fax, Y., Reese, K., Singh, J., Levin, D.: Detecting and evading Censorship-in-Depth: A case study of Iran's protocol whitelister. In: 10th USENIX Worksh. on Free and Open Communications on the Internet (FOCI 20) (2020)
15. Bou-Harb, E., Debbabi, M., Assi, C.: A novel cyber security capability: Inferring Internet-scale infections by correlating malware and probing activities. Computer Networks **94** (2016)
16. Breindl, Y., Wright, J.: Internet filtering trends in western liberal democracies: French and German regulatory debates. FOCI **12** (2012)
17. Burdiak, P.: Online Battlefield: The Legal Landscape of Ukraine's Internet Censorship Before and After the 2022 Russian Invasion. Modern Historical and Political Issues **47** (2023). https://doi.org/10.31861/mhpi2023.47.195-205
18. C S. H. N. Murthy: State-owned media and democratization in Eritrea: An analytical study. Global Media Journal African Edition **6**(2) (2013). https://doi.org/10.5789/6-2-108

19. Cain, G.: Kill One to Warn One Hundred: The Politics of Press Censorship in Vietnam. The International Journal of Press/Politics **19**(1) (2014). https://doi.org/10.1177/1940161213508814
20. Campbell-Smith, U., Bradshaw, S.: Global cyber troops country profile: India. Project on Computational Propaganda (2019)
21. Chaabane, A., Chen, T., Cunche, M., De Cristofaro, E., Friedman, A., Kaafar, M.A.: Censorship in the wild: Analyzing internet filtering in Syria. In: Proc. 2014 Conf. on Internet Measurement Conf. ACM (2014). https://doi.org/10.1145/2663716.2663720
22. Cloudflare: Traffic volume in iran. https://radar.cloudflare.com/traffic/ir?dateRange=1d (2026)
23. Coe, P.: The Draft Online Safety Bill and the regulation of hate speech: Have we opened Pandora's box? Journal of Media Law **14**(1) (2022). https://doi.org/10.1080/17577632.2022.2083870
24. Creemers, R.: China's social credit system: An evolving practice of control. Available at SSRN 3175792 (2018)
25. Crowne, E.: All that glitters: Federal Court of Canada issues Canada's first website blocking order against GoldTV. Journal of Intellectual Property Law & Practice **15**(2) (2020). https://doi.org/10.1093/jiplp/jpaa002
26. Deibert, R.: Canada and the Challenges of Cyberspace Governance and Security. The School of Public Policy Publications **6** (2013). https://doi.org/10.55016/ojs/sppp.v6i1.42426
27. Eissa, T., Cho, G.h.: Internet anonymity in Syria, challenges and solution. In: IT Convergence and Security 2012. Springer (2012)
28. Erixon, F., Hindley, B., Lee-Makiyama, H.: Protectionism online: Internet censorship and international trade law. Tech. rep., ECIPE Working Paper (2009)
29. Fifield, D.: Threat Modeling and Circumvention of Internet Censorship. Ph.D. thesis, UC Berkeley EECS (2017)
30. Filter Watch: Wartime digital isolation: Iran's strategic internet shutdown. https://filter.watch/english/2026/03/10/investigative-report-irans-strategic-internet-shutdown-of-february-28/ (2026)
31. Freedom House: Freedom in the world 2025: The uphill battle to safeguard rights. https://freedomhouse.org/report/freedom-world (2025)
32. Freedom House: Freedom of the net 2025. https://freedomhouse.org/report/freedom-net/2025/uncertain-future-global-internet (2025)
33. Gebhart, G., Kohno, T.: Internet censorship in Thailand: User practices and potential threats. In: 2017 IEEE Eur. Symp. on Security and Privacy (EuroS&P). IEEE (2017). https://doi.org/10.1109/EUROSP.2017.50
34. Ghebregiorgis, F., Mihreteab, H.T.: Determinants of Internet Use and Internet Penetration in Eritrea: Evidences from the City of Asmara. Journal of Economics and Management Sciences **1**(1) (2018). https://doi.org/10.30560/jems.v1n1p28
35. Golovchenko, Y.: Fighting Propaganda with Censorship: A Study of the Ukrainian Ban on Russian Social Media. The Journal of Politics **84**(2) (2022). https://doi.org/10.1086/716949
36. Gosain, D., Singh, K., Sharma, R., Suresh Babu, J., Chakravaty, S.: Out in the open: On the implementation of mobile app filtering in india. In: Int. Conf. on Passive and Active Network Measurement. Springer (2024)
37. Gumede, W.: Rise in censorship of the Internet and social media in Africa. Journal of African Media Studies **8**(3) (2016)
38. Han, R.: Defending the Authoritarian Regime Online: China's "Voluntary Fifty-cent Army". The China Quarterly **224** (2015). https://doi.org/10.1017/S0305741015001216

39. Hannaford, N.: Death by a thousand clicks: The rise of internet censorship and control in Canada. https://www.jccf.ca/wp-content/uploads/2025/12/Death-by-a-thousand-clicks_Final.pdf (2025)
40. Hashemzadegan, A., Gholami, A.: Internet Censorship in Iran: An Inside Look. Journal of Cyberspace Studies **6**(2), 183–204 (2022). https://doi.org/10.22059/JCSS.2022.349715.1080
41. Helwani, I.: Cyberactivism in [Syria: Emergence, transformation, potentials, and limitations. Güvenlik Stratejileri Dergisi **20**(48) (2024)
42. Hu, W., Barradas, D.: Work in Progress: A Glance at Social Media Self-Censorship in North America. In: 2023 IEEE Eur. Symp. on Security and Privacy Worksh. (EuroS&PW) (2023). https://doi.org/10.1109/EuroSPW59978.2023.00072
43. Indian Gov: Section 69a Of It Act 2 | Ministry of Electronics and Information Technology. https://www.meity.gov.in/documents/act-and-policies/section-69a-of-it-act-2-YjNxgTMtQWa (2008)
44. Iszaevich, G.E.W.: Distributed Detection of Tor Directory Authorities Censorship in Mexico. In: The Eighteenth Int. Conf. on Networks (2019)
45. Jin, L., Hao, S., Wang, H., Cotton, C.: Understanding the Practices of Global Censorship through Accurate, End-to-End Measurements. Proceedings of the ACM on Measurement and Analysis of Computing Systems **5**(3) (2021). https://doi.org/10.1145/3491055
46. Josephy-Hernández, D.E.: A brief history of anime censorship in the United States, México and Costa Rica: Reception and adverse reactions. In: Routledge Handbook of East Asian Translation. Routledge (2025)
47. Lange, F., Niere, N., Jonathan von Niessen: Censors ignore unencrypted HTTP/2 traffic. https://upb-syssec.github.io/blog/2024/http2/ (2024)
48. Laungaramsri, P.: Mass surveillance and the militarization of cyberspace in post-coup Thailand. Advances in Southeast Asian Studies **9**(2) (2016)
49. Luong, D.N.A.: A Study of Vietnam's Control over Online Anti-state Content. In: A Study of Vietnam's Control over Online Anti-state Content, pp. 1–27. Trends in Southeast Asia, ISEAS–Yusof Ishak Institute (2023)
50. Manullang, S.O.: The Legality of Devious Cyber Practices: Readiness of Indonesia's Cyber Laws. Society **10**(2) (2022). https://doi.org/10.33019/society.v10i2.482
51. Master, A., Garman, C.: A Worldwide View of Nation-state Internet Censorship. In: Free and Open Communications on the Internet (FOCI'23) (2023)
52. Medina, M.: Governmental Censorship of the Internet: Spanish vs. Catalans Case Study. Library Trends **68**(4) (2020)
53. Mehta, S.N., Amit-Danhi, E.R.: The road to censorship: The case of digital audio-visual industries in India. International Journal of Cultural Policy **31**(7) (2025)
54. Meyer, T.: Graduated response in France: The clash of copyright and the Internet. Journal of Information Policy **2** (2012)
55. Moats, D., Tseng, Y.S.: Using quali-quantitative methods to interrogate the role of algorithms in digital democracy platforms. Information, Communication & Society **27**(5) (2024). https://doi.org/10.1080/1369118X.2023.2230286
56. Momen, M.N., S., H., Das, D.: Mediated democracy and internet shutdown in India. Journal of Information, Communication and Ethics in Society **19**(2) (2021). https://doi.org/10.1108/JICES-07-2020-0075
57. Net4People: Bidirectional DNS, HTTPS, HTTP injection in Turkmenistan. https://github.com/net4people/bbs/issues/80 (2021)
58. NetBlocks: Mapping internet freedom in real time. https://netblocks.org/ (2026)

59. Nguyen, N.L., Wang, M.H., Dai, Y.C., Dow, C.R.: Understanding Malicious Accounts in Online Political Discussions: A Multilayer Network Approach. Sensors (Basel, Switzerland) **21**(6) (2021). https://doi.org/10.3390/s21062183
60. Nguyen-Pochan, T.T.P.: State Management of Social Media in Vietnam. The Russian Journal of Vietnamese Studies **5**(1S) (2021). https://doi.org/10.54631/VS.2021.S-23-33
61. Niaki, A.A., Cho, S., Weinberg, Z., Hoang, N.P., Razaghpanah, A., Christin, N., Gill, P.: ICLab: A global, longitudinal Internet censorship measurement platform. In: 2020 IEEE Symp. on Security and Privacy (SP). IEEE (2020). https://doi.org/10.1109/SP.2020.00014
62. Norton, B.: Music and Censorship in Vietnam since 1954. In: Hall, P. (ed.) The Oxford Handbook of Music Censorship. Oxford University Press (2017). https://doi.org/10.1093/oxfordhb/9780199733163.013.29
63. Nourin, S., Tran, V., Jiang, X., Bock, K., Feamster, N., Hoang, N.P., Levin, D.: Measuring and Evading Turkmenistan's Internet Censorship: A Case Study in Large-Scale Measurements of a Low-Penetration Country. In: Proc. ACM Web Conf. 2023. ACM (2023). https://doi.org/10.1145/3543507.3583189
64. Park, J., Jang, R., Mohaisen, M., Mohaisen, D.: A large-scale behavioral analysis of the open DNS resolvers on the Internet. IEEE/ACM Transactions on Networking **30**(1) (2022). https://doi.org/10.1109/TNET.2021.3105599
65. Piskunova, N.: Small, stable, authoritarian? Assessing Eritrea's consistency in abusing media freedoms. In: Saqib, F., Wlodarczyk, M. (eds.) Authoritarian and Populist Influences in the New Media. IGI Global (2017). https://doi.org/10.4018/978-1-5225-2187-7.ch014
66. Piña-García, C.A., Espinoza, A.: Coordinated campaigns on Twitter during the coronavirus health crisis in Mexico. Tapuya: Latin American Science, Technology and Society **5**(1) (2022). https://doi.org/10.1080/25729861.2022.2035935
67. progres: The regulation of the Internet in Turkmenistan. https://progres.online/reports/internet-freedom/the-regulation-of-the-internet-in-turkmenistan/ (2024)
68. Qurim: Turkmenistan and their "Golden DPI". https://www.qurium.org/alerts/turkmenistan-and-their-golden-dpi/ (2019)
69. Rama, B.G.A.: Press Freedom in The Digital Era in Indonesia: A Human Rights Perspective. JIHAD : Jurnal Ilmu Hukum dan Administrasi **6**(4) (2024). https://doi.org/10.58258/jihad.v6i4.7543
70. Ramesh, R., Raman, R.S., Virkud, A., Dirksen, A., Huremagic, A., Fifield, D., Rodenburg, D., Hynes, R., Madory, D., Ensafi, R.: Network responses to Russia's invasion of Ukraine in 2022: A cautionary tale for internet freedom. In: Proc. 32nd USENIX Conf. on Security Symp. USENIX Association (2023)
71. Rauchfleisch, A., Tseng, T.H., Kao, J.J., Liu, Y.T.: Taiwan's Public Discourse About Disinformation: The Role of Journalism, Academia, and Politics. Journalism Practice **17**(10) (2023). https://doi.org/10.1080/17512786.2022.2110928
72. Saka, E.: Social Media in Turkey as a Space for Political Battles: AKTrolls and other Politically motivated trolling. Middle East Critique **27**(2) (2018). https://doi.org/10.1080/19436149.2018.1439271
73. Santos Okholm, C., Ebrahimi Fard, A., Ten Thij, M.: Blocking the information war? Testing the effectiveness of the EU's censorship of Russian state propaganda among the fringe communities of Western Europe. Internet Policy Review **13**(3) (2024). https://doi.org/10.14763/2024.3.1788

74. Satriawan, I., Elven, T.M.A., Lailam, T.: Internet Shutdown in Indonesia: An Appropriate Response or A Threat to Human Rights? Sriwijaya Law Review (2023). https://doi.org/10.28946/slrev.Vol7.Iss1.1018.pp19-46
75. Shen, P.: How China Initiates Information Operations Against Taiwan. Taiwan Strategists **12** (2021)
76. Shiker, Z.R., Tsegay, S.M.: (Mis)Education in Authoritarian Regimes: The Case of Eritrea. Education Sciences **15**(7) (2025). https://doi.org/10.3390/educsci15070801
77. Sihidi, I.T.: The Rise of Symptoms of Digital Authoritarianism: Lesson from Indonesia. Internasional Journal of Politics and Public Policy **2**(1) (2025). https://doi.org/10.70214/28vg6e57
78. Singh, K., Grover, G., Bansal, V.: How India censors the web. In: Proc. 12th ACM Conf. on Web Science. ACM (2020). https://doi.org/10.1145/3394231.3397891
79. Sirikupt, C.: Drowning Out Dissent: The Thai Military's Quest to Fabricate Popular Support on Twitter. The International Journal of Press/Politics **31**(1) (2026). https://doi.org/10.1177/19401612241279158
80. Skrzypczak, J.: The Effect of the 'China Factor' on Taiwan's Media System Security as an Example of the 'Privatization and Outsourcing' of Censorship and Propaganda in the Digital Age. Przegląd Strategiczny **9**(12) (2019). https://doi.org/10.14746/ps.2019.1.22
81. Tanash, R.S., Chen, Z., Thakur, T., Wallach, D.S., Subramanian, D.: Known unknowns: An analysis of twitter censorship in Turkey. In: Proc. 14th ACM WPES. ACM (2015). https://doi.org/10.1145/2808138.2808147
82. Tenenboim, O.: Under-the-radar engagement: How and why news users limit their public expression. Journal of Computer-Mediated Communication **30**(1) (2025). https://doi.org/10.1093/jcmc/zmae024
83. The Internet Monitor: Internet Monitor. https://thenetmonitor.org/ (2026)
84. The New Arab Staff: New Syria government unblocks websites banned by Assad regime. https://www.newarab.com/news/new-syria-government-unblocks-websites-banned-assad-regime (2025)
85. Theil, S.: The German NetzDG: A Risk Worth Taking? Verfassungsblog: On Matters Constitutional (2018). https://doi.org/10.17176/20180208-184652
86. Thumfart, J.: Digital Rights and the State of Exception. Internet Shutdowns from the Perspective of Just Securitization Theory. Journal of Global Security Studies **9**(1) (2024). https://doi.org/10.1093/jogss/ogad024
87. Tschantz, M.C., Afroz, S., Name Withheld On Request, Paxson, V.: SoK: Towards Grounding Censorship Circumvention in Empiricism. In: 2016 IEEE Symp. on Security and Privacy (S&P). IEEE (2016). https://doi.org/10.1109/SP.2016.59
88. Ververis, V., Marguel, S., Fabian, B.: Cross-Country comparison of Internet censorship: A literature review. Policy & Internet **12**(4) (2020)
89. Watch, H.R.: Turkmenistan events 2023. https://www.hrw.org/world-report/2024/Country-chapters/turkmenistan (2024)
90. Wendzel, S., Volpert, S., Zillien, S., Lenz, J., Rünz, P., Caviglione, L.: A Survey of Internet Censorship and its Measurement: Methodology, Trends, and Challenges. Computers & Security **164** (2025). https://doi.org/10.1016/j.cose.2025.104732
91. Winter, P.: Measuring and Circumventing Internet Censorship. Ph.D. thesis, Karlstads universitet (2014)
92. Wu, M., Sippe, J., Sivakumar, D., Burg, J., Anderson, P., Wang, X., Bock, K., Houmansadr, A., Levin, D., Wustrow, E.: How the Great Firewall of China detects and blocks fully encrypted traffic. In: Proc. 32nd Usenix Security Symp. USENIX (2023)