CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

MARCH 2022

Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?

Steven Feldstein

Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?

Steven Feldstein

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Summary

Governments worldwide continue to deploy internet shutdowns and 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 show that incidences of global shutdowns have remained steadily high: 196 documented incidents in 2018, 213 incidents in 2019, and 155 in 2020. The first five months of 2021 recorded fifty shutdown incidents.[1] 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. As Clément Voule, the United Nations special rapporteur on the rights to freedom of peaceful assembly and of association, pointedly observes: "Shutdowns are lasting longer, becoming harder to detect and targeting particular social media and messaging applications and specific localities and communities."[2]

Events in Russia have put a finer point on internet shutdown trends. On March 4, 2022, Roskomnadzor, the Russian internet regulator, announced that it would block Facebook and Twitter and would ban new uploads to TikTok.[3] On March 14, it added Instagram to the banned list.[4] Russian authorities have also restricted access to a slew of news websites, including the BBC, Deutsche Welle, Radio Free Europe/Radio Liberty, and Voice of America. Roskomnadzor claimed these measures were enacted in response to new limits imposed by platforms on Russian propaganda outlets—accusing Facebook of "discrimination."[5] The Kremlin's crackdown is an ominous signal about where the shutdown struggle is headed in authoritarian countries.

Despite these bleak trends, there is a growing international consensus—at least among liberal democracies—that protecting internet access is integrally linked to freedoms of expression and association and forms a crucial part of the global democracy and human rights agenda. This paper picks up on this emerging norm and probes several key questions: What can citizens do to evade authoritarian controls and regain internet access? How can democratic governments support these efforts and push back against governments that shut down and block the internet?

The short answer is that there is a multitude of responses available to democracies and civil society organizations to push back against internet blackouts and network disruptions. Democracies can exert meaningful pressure against repressive governments to ease internet blocks, and citizens are able to exercise creative options to circumvent internet controls. The paper walks through different tools available to citizens to evade internet controls. It examines where internet shutdown trends are headed and incentives for particular regimes to adopt new modes of censorship. It then presents a multifaceted strategy for democracies, civil society organizations, and technology developers and companies to counter internet shutdowns.

Key Insights

- Internet shutdowns exist on a spectrum and include everything from complete blackouts (where online connectivity is fully severed) or disruptions of mobile service to throttling or slowing down connections to selectively blocking certain platforms. Some internet shutdowns last a few days or weeks, while others persist for months or even years.

- Inherent in the definition of internet shutdowns is that they are timebound and contain fixed start and end dates. But in many countries, short-term internet disruptions are morphing into longer-term controls, bringing definitional confusion as to whether these restrictions still qualify as shutdowns or whether they are more properly understood as permanent limitations on internet access.

- This underlines a growing trend: internet blackouts, where governments order internet service providers (ISPs) to fully disconnect online access for a particular geographic region or throughout a country, will become decreasingly common in the future. Instead, governments will use more precise blocking methods to deny access to specific websites, internet services, or communications platforms, while avoiding widespread service disruptions.

- Activists and politicians have called for the United States to deploy satellite internet or floating Wi-Fi balloons to restore internet access during other countries' shutdowns, such as during Cuba's 2021 internet blackout. Unfortunately, these tools are rarely practical nor workable for both technical and political reasons. But other tools are available to citizens that bring a high degree of effectiveness:

  — *Virtual private networks (VPNs)* are protocols that allow users to access many blocked sites by providing internet service based outside of a censored country using a proxy server. Users can download popular free VPNs from app stores, directly from product websites, or through Android application packages (APK files) sent by email or messaging apps. These services are most useful during targeted internet shutdowns, when a government blocks specific websites or platforms but preserves overall network connectivity.

  — An effective alternative to VPNs are *private servers*. Because VPNs are publicly accessible, governments can block them. Private servers (such as Outline, an open-source project from Google's Jigsaw unit, which works on internet safety) permit users to establish protected servers located anywhere in the world and to share them with other individuals. This method is particularly helpful during partial internet shutdowns or when states are blocking VPNs; its decentralized model means that there is no single domain or internet protocol (IP) address for governments to impede.

  — *Mesh networks* are another useful option during internet blackouts when all outside connectivity is blocked and users cannot use VPNs. Mesh networks allow users to maintain communication with one another without relying on the internet or short message service (SMS) services. Instead, they use Bluetooth or Wi-Fi technology to create a chain of devices that can send messages to one another when they are in close proximity. Activists in Hong Kong, for example, relied heavily on mesh networks like Bridgefy to facilitate peer-to-peer communications during protests in 2019–2020. While mesh networks do not facilitate internet access, they are among the only digital communication options available during a total shutdown.

  — *Serverless circumvention tools* also demonstrate promise and can be used to either facilitate internet access during short-term disruptions or to circumvent longer-term restrictions. Programs such as Intra, GoodbyeDPI, Green Tunnel, and Geneva do not tunnel traffic or rely upon third-party servers (like VPNs), which means that governments have a much harder time blocking them.

- Democratic states, together with local and international civil society organizations, technology developers, and companies, should pursue a multifaceted strategy to counter shutdown trends. The strategy should emphasize, first, advance preparation, such as encouraging citizens to mass download censorship-resistant VPNs ahead of specific windows of risk; second, user accessibility to facilitate scaling up, recognizing that the more steps required to install VPNs or circumvention technology, the less likely it is that individuals will actually use the software; third, nontechnological strategies to complement digital solutions; and fourth, raising the costs for governments and private companies to continue implementing shutdowns.

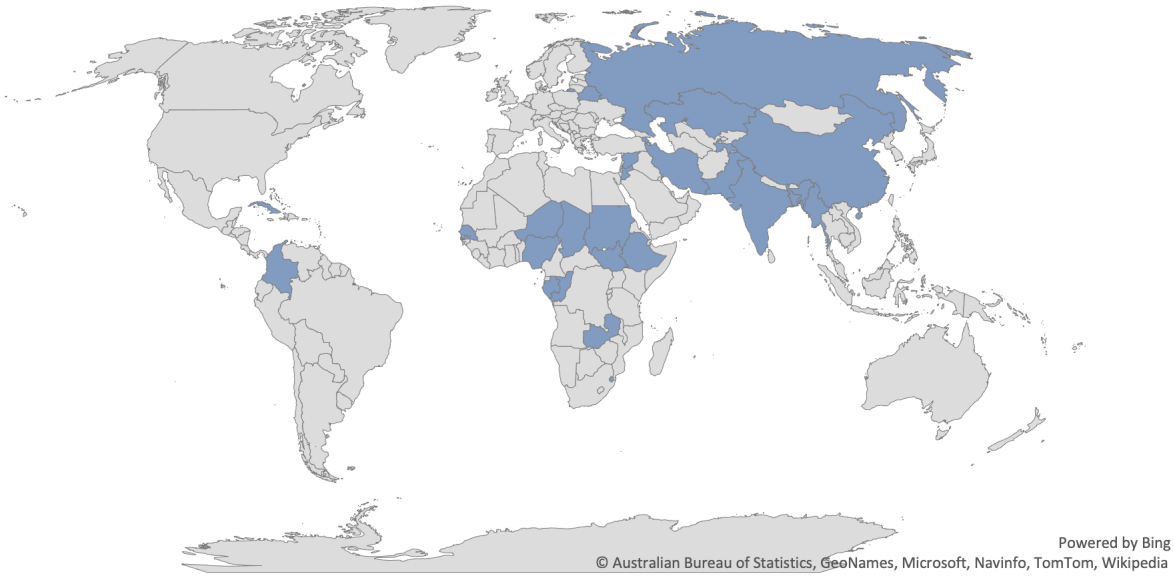
- Liberal democracies in particular should consider the best mix of carrots and sticks to contest internet shutdowns. Imposing reputational and legal costs for governments and companies that participate in shutdowns—whether by supporting strategic litigation, making internet blockages more economically costly, or flagging repressive behavior in international fora—can be successful deterrents. Conversely, providing financial inducements to states that maintain free and open internet access, and incentivizing countries to participate in the digital economy, can create structural incentives that mitigate against governments shutting down the internet. Finally, long-term investment and advocacy, rather than quick fixes, are the best paths to empowering citizens to navigate increasingly advanced online controls.

Introduction

The year 2021 was inauspicious for government-sponsored internet disruptions. In February, one of the first actions the Myanmar military undertook after seizing power in a coup and placing the elected civilian leader, Aung San Suu Kyi, under house arrest, was to cut internet access for the population. In the ensuing months, the military junta enacted a range of internet controls, implementing regular internet blackouts at night, blocking access to different platforms and services during the day, and periodically enacting full-scale national shutdowns.[6] By the end of 2021, the junta had imposed more than 12,000 hours of disruptions with some regions still unable to access social media.[7]

In July 2021, the Cuban government followed suit, shutting down internet access on the island for 176 hours in response to mass demonstrations protesting the government's handling of the coronavirus pandemic and a lack of food and medical supplies.[8] All told, the disruption led to $33 million in lost economic activity.[9] The year concluded with another gain for autocrats: in Sudan, the military detained former prime minister Abdalla Hamdok and killed dozens of protesters in October and November.[10] Like in Myanmar and Cuba, the Sudanese military shut down the internet in a bid to stifle citizen protests. Sudan is no stranger to online shutdowns—the country experienced monthslong outages in 2018 and 2019 when the government ordered private telecoms to cut internet access in response to pro-democracy demonstrators.[11] In the 2021 iteration, the military kept up the internet shutdown for nearly a month before slowly allowing communications to come back online (and then periodically shutting off access again).[12] While these three countries experienced crackdowns thousands of miles apart, each regime used common tactics to block internet access, disrupt communications, and maintain its monopoly on information.

Map 1. Global Prevalence of Internet Shutdowns in 2021



Source: Marianne Diaz Hernandez, Rafael Nunes, Felicia Anthonio, and Sage Cheng, "#KeepItOn Update: Who Is Shutting Down the Internet in 2021?," Access Now, June 7, 2021, https://www.accessnow.org/who-is-shutting-down-the-internet-in-2021; and Samuel Woodhams and Simon Migliano, "Cost of Internet Shutdowns 2021 Tracker Data," Top10VPN, January 30, 2022, https://docs.google.com/spreadsheets/d/1aed8Py4W3QYxhHpk0gEV-D2UCv1-3Ldfwhp9KVLUbwU/edit#gid=1286013195.

Internet shutdowns remain a favored tactic of governments to push back against mass demonstrations, entrench military coups, or cut off conflict areas from the rest of the world. In addition to Myanmar, Cuba, and Sudan, authorities in Chad, Ethiopia, India, and Iran, among others, throttled online access, blocked service providers, and carried out full network disruptions in 2021 (see map 1).[13]

Offending governments argue that shutting down the internet not only falls within their sovereign authority but also is needed to counter threats to public order and challenges to national security. Such a conception is badly out of step with democratic and human rights norms. A plurality of countries maintains that internet access is integrally linked to protecting freedom of expression and association and that cutting off access is "in violation of states' obligations under international human rights law."[14] As the United Nations Human Rights Committee affirms, "The right to access and use [the] 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."[15]

Despite the growing consensus that internet shutdowns run contrary to established international human rights principles, democracies are increasingly frustrated about their seeming inability to help citizens overcome internet controls. In the United States, this exasperation

came to a head in July 2021 following Cuba's shutdown. U.S. Senator Marco Rubio called on the White House "to facilitate open and free satellite internet access on the island of Cuba."[16] Florida Governor Ron DeSantis advocated for using, as reporters described it, "giant balloons as floating Wi-Fi hotspots" to restore online connectivity to Cuba's citizens.[17] In response, President Joe Biden asserted that the government was "considering whether [it had] the technological ability to reinstate that [internet] access."[18]

The issue boils down simply: What can citizens do to evade authoritarian controls and regain online access? How can democratic governments support these efforts and push back against governments that shut down and block the internet?

The short answer is that once a government imposes an internet blackout, there is little that liberal democracies can do to help citizens immediately restore connectivity. While floating Wi-Fi balloons or beaming the internet from satellites have captured the imagination of politicians, in truth these are costly and unworkable measures, both technically and politically. However, that doesn't mean that democracies cannot exert meaningful pressure against repressive governments to ease internet blocks—or that citizens cannot exercise creative options to circumvent internet controls.

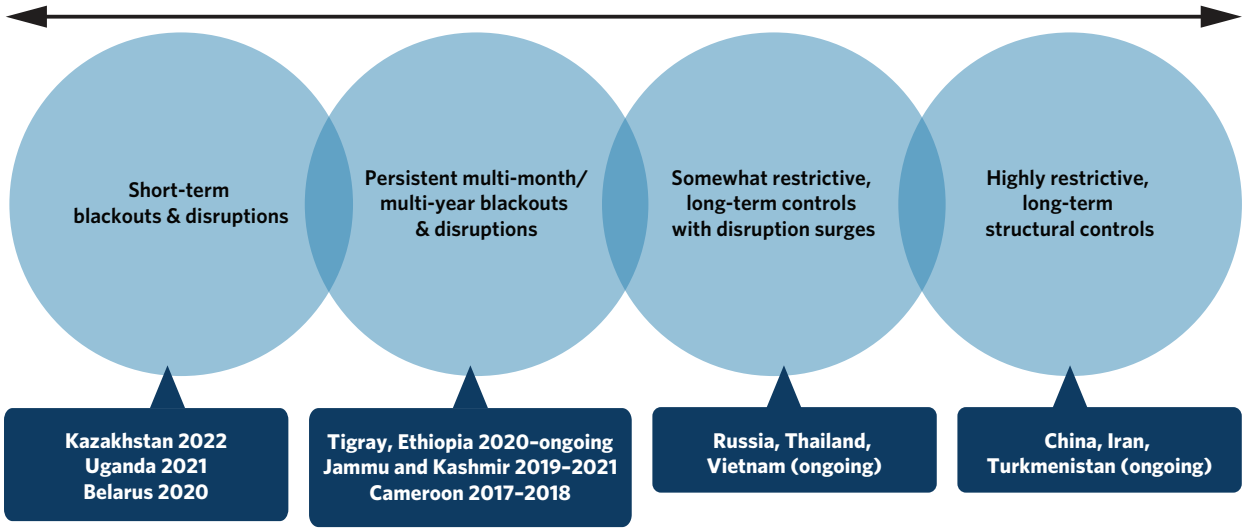
Confronting internet shutdowns should be an integral part of supporting democracy and human rights across borders. To that end, democratic states, together with local and international civil society organizations and technology developers and companies, should pursue a multifaceted strategy to counter shutdown trends. This strategy should focus on advance preparation, such as encouraging citizens to mass download censorship-resistant VPNs ahead of specific windows of risk; prioritize user accessibility to facilitate scaling up (recognizing that the more steps required to install VPNs or circumvention technology, the less likely it is that individuals will actually use the software); employ nontechnological strategies to complement digital solutions; and raise the costs for governments and private companies to continue implementing shutdowns.

What Are Internet Shutdowns and Where Are Trends Headed?

Internet shutdowns are "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.[19] Internet shutdowns exist on a spectrum and include everything from complete blackouts (where online connectivity is fully severed) or disruptions of mobile service to throttling or slowing down connections or selectively blocking certain platforms.

Internet blocking most often occurs either at the national level (where all traffic entering or exiting a country is subject to content blocking through a national gateway or firewall) or at the carrier and ISP level (where individual telecoms, both mobile and traditional, are instructed to block internet connectivity or restrict certain content or services). Some internet shutdowns last a few days or weeks, while others persist for months or even years. In certain countries, short-term disruptions have given way to longer-term internet controls, bringing definitional confusion as to whether these restrictions still qualify as shutdowns, per se, or whether they are more properly classified as permanent limitations on internet access. Figure 1 illustrates the continuum from shorter-term, timebound blackouts and disruptions to long-term structural internet controls.[20]

Figure 1. Internet Controls Continuum



Source: Compiled from various media, human rights, and other civil society organizations. See endnote 20 for the complete list.

Not all shutdowns or internet blocking techniques are the same. Countries take advantage of a multitude of tools and approaches. Table 1 illustrates the range of techniques deployed by governments globally.

Table 1. Network Disruption and Internet Blocking Techniques Deployed Globally

Network Disruption or Blocking Technique	Description	Censorship Effectiveness	Examples
Full or partial blackout	This type of blackout entails full loss of connectivity and can be national or regional, involving broadband or mobile network shutoffs.	Effective means of blocking communication during the duration of the blackout but doesn't remove actual content; comes with significant collateral costs.	Tigray, Ethiopia; Kazakhstan[21]
Throttling	Connectivity is substantially slowed for specific sites, apps, or segments of traffic; this method can also throttle all internet traffic.	Effective at encouraging users to turn to alternative services without revealing that blocking is occurring; discourages users from accessing certain services by making them believe they are unreliable.	Jordan, Myanmar, Venezuela[22]
IP and protocol-based blocking	IP-based blocking inserts barriers in the network, such as firewalls, that block all traffic to certain IP addresses. Protocol-based blocking uses other low-level network identifiers, such as TCP/ IP port numbers "that can identify a particular application on a server or a type of application protocol."[23] This type of blocking can also be used for lawful purposes by democratic governments to block harmful content.	Works poorly because IP addresses can easily change; simple blocking approach that doesn't directly block content but blocks traffic.	Egypt, Myanmar, Pakistan[24]
Deep packet inspection (DPI)	A device is inserted in the network between the end user and the rest of the internet that scrutinizes and filters internet packet payloads based on content, patterns, or application types. DPI can be used for domain blocking as well as keyword blocking and is a key component of advanced systems of internet control, such as China's Great Firewall or Russia's internet restrictions. DPI can also be used for lawful purposes by democratic governments to block harmful content. Note: many companies selling DPI technology are headquartered in democracies like the United States and Israel.	Diminished effectiveness because DPI is computationally intensive and therefore costly, requiring all content to be evaluated against blocking rules. Very effective where blocked information is easily characterized. Less effective for general blocking (such as a filter to "block political content").	Belarus, China, Egypt, Russia[25]

Table 1. Network Disruption and Internet Blocking Techniques Deployed Globally (continued)

Network Disruption or Blocking Technique	Description	Censorship Effectiveness	Examples
Domain name system (DNS) interference	At the network or ISP level, DNS traffic is funneled to a modified DNS server that can be configured to block lookups of certain domain names. Even if the ISP's resolver is working correctly, a DNS injector can be inserted to respond more quickly, "resulting in users receiving forged answers in an attack known as 'cache poisoning.'"[26]	Easily evaded by both content publishers and end users; only effective when the organization carrying out the blocking completely controls the network connection of the end user: "If the user can select a different connection, or use a different set of DNS servers, the technique does not affect them."[27]	Turkey, Iran[28]
URL-based blocking	A blocking device contains a list of web URLs in which to restrict access. Users trying to view any of the URLs on the list will encounter an interruption.	Common technique effective in blocking access to entire categories of information; much less effective in blocking new pages or smaller sites, as well as encrypted web servers (such as when a publisher is trying to avoid the filter, simply changing the name of the file or server can frequently avoid the block).	Thailand[29]
Platform-based blocking	Authorities work with ISPs to block information within their geographic region without blocking the entire platform. This includes platform filtering of major search engine providers or social media sites.	Works poorly; users can jump to alternate platforms or search engines.	Nigeria, Turkey, Vietnam[30]
Nontechnical Strategies	Authorities impose economic costs to deter online access (such as social media taxes, data usage fees, or onerous SIM card registration requirements), use online pressure to intimidate users, pressure companies to take down content, and institute legal restrictions to access.	Depends on implementation context and prospect for public backlash.	Myanmar, Thailand, Turkey, Uganda[31]

Autocratic and illiberal leaders continue to deploy shutdowns in large numbers. Data from Access Now, a prominent digital rights organization, show that global shutdown incidents have stayed relatively steady: 196 incidents were documented in 2018, 213 in 2019, and 155 in 2020. The first five months of 2021 recorded fifty shutdown incidents.[32] While the 2021 figure is slightly smaller than those from prior years, the average length of these disruptions has increased due to siege-like shutdowns in Myanmar, Ethiopia, and Jammu and Kashmir—incidents that extended into the new year. Government shutdowns in 2021 largely occurred in response to or in association with four types of events: mass demonstrations, conflict and military coups, elections, and school exams (purportedly to prevent cheating). A fifth category includes ongoing repression and state responses to communal violence or religious holidays (see table 2).

Table 2. Precipitating Events Leading to Internet Shutdowns in 2021

Internet Shutdown Event	Countries
Protests	Bangladesh, Burkina Faso, Chad, Colombia, Cuba, Eswatini, Gabon, India, Iran, Jordan, Kazakhstan, Pakistan, Russia, Senegal, South Sudan, Sudan
Conflict/military coups	Armenia, Ethiopia, India, Myanmar, Palestinian territories, Sudan
Elections	Niger, Republic of the Congo, Uganda, Zambia
School exams	Ethiopia, India, Sudan, Syria
Other (ongoing repression, communal violence, religious holidays, unknown)	Bangladesh, Belarus, Chad, China, Ethiopia, Iran, Nigeria, Russia, Tajikistan

Source: Marianne Diaz Hernandez, Rafael Nunes, Felicia Anthonio, and Sage Cheng, "#KeepItOn Update: Who Is Shutting Down the Internet in 2021?," Access Now, June 7, 2021, https://www.accessnow.org/who-is-shutting-down-the-internet-in-2021; and Samuel Woodhams and Simon Migliano, "Cost of Internet Shutdowns 2021 Tracker Data," Top10VPN, January 30, 2022, https://docs.google.com/spreadsheets/d/1aed8Py4W3QYxhHpk0gEV-D2UCv1-3Ldfwhp9KVLUbwU/edit#gid=1286013195.

It is noteworthy that just a handful of factors were primarily responsible for triggering shutdown measures. As will be discussed later, this can help activists anticipate the occurrence of future shutdowns and prepare accordingly. When certain windows of risk emerge, whether in the form of contested elections, religious holidays historically associated with violence, or mass protests, civic groups can institute preparatory strategies to help individuals stay connected in case there are network outages.[33]

Further, the composition of internet shutdowns is changing. While some countries continue to rely upon full internet blackouts in response to protests or political instability, many governments are adopting more finely honed internet controls to block communication. Regardless, the collateral damage and economic costs of these measures can be significant. Researchers Samuel Woodhams and Simon Migliano have used data from the Netblocks Cost of Shutdown Tool (COST) to estimate the economic impact of network

disruptions.[34] In 2021, they estimate that fifty internet shutdowns resulted in 30,179 hours of interrupted access and $5.45 billion in financial losses.[35] Myanmar showed the greatest financial impact, registering $2.8 billion in lost revenue. In 2020, ninety-three shutdowns led to $4.01 billion in lost revenue, with India as the most economically impacted country ($2.8 billion in forgone revenue). Such losses are not sustainable for long periods of time. Some leaders will continue to rely upon internet blackouts either due to desperation (such as former president Omar al-Bashir's attempts to shut down social media in Sudan in 2018–2019 and President Kassym-Jomart Tokayev's internet shutdown in Kazakhstan in 2022), insulation from short-term economic shocks (such as the Tatmadaw's coup in Myanmar), or to accompany armed operations in confined areas (for example, India's multiyear shutdown in Jammu and Kashmir and Ethiopia's shutdown in the Tigray region). But most countries will implement more advanced controls to filter out unwanted content while leaving their digital economies intact.[36]

Temporary or Permanent?

Inherent in the definition of internet shutdowns is that they are timebound and have fixed start and end dates. But more and more countries are establishing sophisticated, ongoing internet controls in lieu of blackouts or temporary restrictions. Russia's internet control strategy is a good case in point. Rather than rely on periodic connectivity disruptions to keep dissenters in check, authorities have created new systems of control to permanently limit internet users and platforms. Following street protests in 2011–2012 that roiled the regime, users of certain services and social media networks were "forced to register using their real names" and have been prosecuted for what they post online.[37] Russian authorities have deepened their use of deep packet inspection (DPI) and internet traffic routing to block user access to prohibited apps, such as Telegram.[38] New reports indicate that Russia's internet regulator, Roskomnadzor, has mandated that all of the country's ISPs install so-called black boxes designed to prevent users from accessing blacklisted websites and communications platforms.[39] Finally, President Vladimir Putin's regime has made a deliberate push to "technically isolate" Russia's internet (known as RuNet) from the rest of the world by creating a substitute set of Russian-made services and applications and by running technical tests to physically separate RuNet from the global internet (it is yet unclear whether these tests have been successful or not).[40] Unsurprisingly, Russian officials displayed little hesitation in blocking Facebook, Twitter, and subsequently Instagram following the Kremlin's invasion of Ukraine as well as restricting website access to the BBC, Deutsche Welle, Radio Free Europe/Radio Liberty, and Voice of America, among other news sites. Roskomnadzor claimed its actions were in response to recent restrictions imposed on Russian propaganda outlets, accusing Facebook of "discrimination."[41] Russia's actions served two purposes: banning platforms curtails the public's options when it comes to communicating about the war or their dissatisfaction with Putin. The restrictions also impart a warning to other platforms about the consequences of going too far in removing Russian media outlets from their networks.

Russia is far from the only country turning to advanced tools—such as DPI, IP blocking, and domain name system (DNS) interference—for its internet control strategies. Iran, Belarus, Egypt, Saudi Arabia, Turkmenistan, Thailand, and an array of other authoritarian countries have invested heavily in technologies that permit the state to filter unwanted content without sacrificing too much economic productivity.

State use of these technologies is not limited to authoritarian governments. Weak democracies (like India and Nigeria) and strong democracies (like New Zealand) also use DPI technology to block unwanted content.[42] The difference between how governments deploy censorship technology in Egypt or India versus New Zealand comes down to the rule of law. In New Zealand, DPI is narrowly used to protect against the dissemination of child pornography; most other content, especially political content, is left untouched.[43] By contrast, Egypt censors a range of topics and organizations, from media outlets and journalist blogging sites to civil society organizations.[44]

For certain countries like China, which possess a high capacity to manage their information infrastructure, citizens have few options to circumvent online restrictions. In many other countries, however, authorities are much less adept at filtering objectionable websites or services. Keith McManamen, an analyst with the internet censorship circumvention firm Psiphon, observes, "you have to manage that infrastructure, fine tune it. You need people to run it. And I think a lot of countries are just at the level that they could afford these kinds of solutions, but they're not quite there with how it's being implemented."[45] For now, this presents a dilemma for repressive regimes (and a corresponding opportunity for civic activists): states want to avoid accruing collateral damage from full internet shutdowns, but they lack sufficient capacity to efficiently implement blocking and filtering strategies. In these situations, citizens may actually have more options for circumventing internet controls than when they are contesting full internet shutdowns. As ever with technology, the cost is decreasing even for advanced network blocking tools, meaning that the prevalence of internet blocking will likely only grow.

Of note, governments do not always need to rely on sophisticated technical measures to curtail internet access. Some of the most insidious—and effective—tactics use basic economic levers to discourage online use. For example, in countries ranging from Uganda to Myanmar, governments have imposed excessive, so-called social media taxes, price hikes for data usage, or onerous SIM card registration requirements, all used to dampen citizen communication.[46] Governments continue to rely on old-fashioned pressure tactics to force internet platforms to remove unwanted content (or conversely to coerce platforms to preserve inflammatory state-sponsored messages that platforms have banned). In Twitter's January 2022 transparency report, for example, the company noted that it had received 43,387 legal demands from governments between January and June 2021 to remove content, representing "the largest number of accounts ever subject to removal requests in a reporting period since releasing [its] first transparency report in 2012."[47] This trend line, alongside the growth of technical shutdown measures and censorship strategies, will likely only increase.

Can Balloons or Satellite Internet Offset Internet Shutdowns?

There is growing interest in using satellite technology to get around ISP-based shutdowns.[48] Amazon and SpaceX are both developing low-orbiting satellites to deliver internet access for commercial purposes. SpaceX's satellite system, Starlink, has launched 1,000 satellites and has approval from the U.S. Federal Communications Commission to launch nearly 12,000 more.[49] Starlink satellites have even found their way to Ukraine, to help the country maintain internet access in the wake of Russia's invasion (see figure 2).[50] Starlink satellites

Figure 2. Delivery of Starlink Internet Satellite Stations to the Ukrainian Government

Source: Mykhailo Fedorov (@FedorovMykhailo), Twitter, March 9, 2022, https://twitter.com/FedorovMykhailo/status/1501648932824301570.

orbit the earth at a low altitude, which allows signals to travel quickly back and forth. This contrasts with traditional telecom satellites, which hover farther away from Earth, allowing them to cover more of the planet at once but increasing the round-trip signal time. Some advocates are pushing to repurpose these technologies as internet censorship circumvention tools and have proposed smuggling receivers into countries experiencing shutdowns to allow citizens to access satellite internet. But there are several obstacles to pursuing a satellite-based internet connectivity strategy.

Regimes such as Myanmar's Tatmadaw have banned civilian possession of all satellite dishes.[51] Satellite installations are difficult to obscure; satellites like Starlink or very-small-aperture terminal (VSAT) systems each require a router and an antenna that must be placed in a clear area to receive a proper signal.[52] The smallest of these kits weighs approximately 30 pounds—so even if citizens were able to obtain these kits from out of country, the likelihood that they would be able to conceal their use is low. As Michael Caster notes regarding Myanmar:

> "police are going house to house and tearing down satellite dishes for receiving pirate signals and things. They can exist in areas where there's maybe a weaker state control or it's easier to maybe to hide that type of thing, but still you need to get it, you need to receive the physical objects to receive the signal."[53]

Moreover, if Starlink or another satellite internet company wishes to broadcast into a country, they must apply for spectrum approval from the International Telecommunication Union (ITU). But as Caster writes, "radioelectric spectrum is regulated as a natural resource and countries have sovereignty claims over spectrum allocation related to broadcast in their territory."[54] In other words, it is highly unlikely that the ITU would authorize satellite transmissions into a territory without the sovereign government's express permission. If the company were to proceed anyway, not only would these transmissions face interference and jamming, but the company would open itself to corporate sanctioning (for example, consider the actions China might take against Tesla, also owned by Elon Musk, if Starlink carried out unauthorized transmissions in China).

Another idea seized upon by internet freedom advocates is using balloons to beam the internet into moderately sized areas. One test carried out by former Alphabet subsidiary Loon claimed that seven balloons could cover an area of 1,000 kilometers with internet access (which Loon said represented an area twenty to thirty times larger than an equivalent ground-based internet system).[55] In the case of Cuba's internet shutdown, theoretically, Loon could have launched a fleet of balloons over Florida and extended signal range to the island. Such balloons have previously delivered internet access to rural areas and natural disaster–affected zones in Kenya, Puerto Rico, and Peru.[56]

However, there are numerous problems associated with balloon-enabled internet. Loon, the main internet balloon manufacturer, closed production in early 2021 because it could not

reduce costs enough to make the experiment sustainable.[57] Loon balloons had a history of crashing (apparently the balloons developed steering problems if they were airborne for too long).[58] The balloons' transmission capabilities are not large and could only reach a limited segment of a country's population. Finally, there are considerable constraints when it comes to beaming internet access against a national government's wishes. For instance, the balloons require network integration with a local telecom to provide service and equipment on the ground in the targeted country, and they must access a free block of radio spectrum in order to broadcast, something typically controlled by national governments.[59] Even if balloon operators found solutions to these problems, they would still face a more basic challenge—radio signal jamming by a government to prevent access (or security officials simply shooting down balloons).

Better Alternatives: VPNs, Private Servers, and Mesh Networks

While satellite internet and Wi-Fi balloons face high constraints, other tools are available to citizens on the ground without necessitating external intervention. VPNs are protocols that allow users to access many blocked sites by providing internet service based outside of a censored country using a proxy server.[60] Proxies allow users to disguise their IP address so they can prevent eavesdropping and interference with communications. Users can download popular free VPNs, such as programs developed by TunnelBear and Psiphon, from app stores, directly from product websites, or through Android application packages (APK files) sent by email or messaging apps like Telegram and Signal.[61] These services are most useful during targeted internet shutdowns, when a government blocks specific websites but maintains overall network connectivity. Some countries have attempted to ban VPNs, however, either by outlawing them on paper (as in Russia) or by technically blocking them from being used or downloaded from app stores (as experienced in Iran and China).[62] VPN companies have responded by finding new methods to circumvent these tactics.

There are, however, several drawbacks to VPNs. For one, it can be difficult for users to discern trustworthy VPNs from insecure options. Many free VPNs have secretive ownership structures and possible links to repressive governments like China.[63] Other VPNs harvest user data and offer minimal privacy protections. They can obtain users' browsing histories and even personal identifiable information (PII) and sell this information to data brokers.[64] It is also worth noting that VPNs use slightly more data than regular browsing because they are routed through additional servers, adding to their cost. And if a VPN does not have servers close to the country where the user is based, then connection speeds are likely to be slower too. These limitations aren't insurmountable, but they represent areas for improvement. As a start, policymakers could push Apple and Google, for example, to only allow VPNs in their app stores that are verifiably secure and privacy-preserving.

One alternative to VPNs are private servers. Because VPNs are publicly accessible, governments can enumerate and block them by IP. An example of how access to private servers can be facilitated is through Outline, an open-source project from Google's Jigsaw that allows

users to create private servers located anywhere in the world and to share them with other individuals. This is particularly helpful during a partial internet shutdown or when other VPNs are blocked; its decentralized model means that there is no single domain or IP for governments to block. Once a host establishes the remote server, they can share unique keys with others, allowing civilians located in censored areas to receive unfettered internet access from users outside their country if necessary.[65] Another advantage is that users get access out of band, meaning that the network and associated devices have a secure connection. A government censor cannot simply download the app, connect, observe what IPs the app connects to, and block them accordingly. The tricky part with Outline, though, is that it assumes a requisite level of knowledge to set up, configure, and then successfully operate a private server over an extended period of time, skills that many individuals may lack.[66] Sudanese activists used Outline successfully during the country's internet shutdown in 2019 to coordinate demonstrations and share information with the outside world.[67]

Mesh networks are increasingly popular alternatives during complete internet shutdown when all outside connectivity is blocked and users are unable to use VPNs. Mesh networks allow users to maintain communications with one another without relying on the internet or SMS services; instead, they leverage Bluetooth or Wi-Fi technology to create a chain of devices that can send messages to one another when they are in the same vicinity.[68] Mesh networks like Bridgefy or Briar have a range of about 100 meters between devices, but the power of the model lies with the scale of users.[69] With Bridgefy's app, once third, fourth, and fifth devices are added to the network, the effective range increases accordingly. As Caster writes, "add five Bridgefy users into a network with each device around 100 meters from the next and you've potentially created an encrypted network with a range four times larger."[70] In other words, when sufficient density of users exists—such as at a soccer game or mass demonstration—then the network can hit a "percolation threshold" resulting in the sudden emergence of a cluster of connected nodes allowing for seamless communication in a geographic area.[71]

While mesh networks do not facilitate internet access, they are among the only digital communication options available during a total shutdown. Says Bridgefy founder Jorge Rios: "Bridgefy is the most valuable when nothing else is available . . . when people know that they're going to find themselves in a delicate situation, such as a natural disaster [or] a protest."[72] Accordingly, mesh networks have witnessed a surge in use, such as during the 2019 Hong Kong protests, when thousands used the app to coordinate demonstrations despite not having stable and secure internet connections.[73] Despite Bridgefy's advantages, some researchers raise concerns about its privacy controls. Researchers from the University of London found that moderately skilled hackers were able to breach the app's protections, leading to harmful outcomes, such as deanonymizing users, decrypting and reading direct messages, performing man-in-the-middle attacks to tamper with communications, and even completely shutting down the mesh network.[74]

Other creative technological options have sprung up as well in response to shutdowns.[75] The founders of SMSWithoutBorders created their app during Cameroon's 240-day-long

shutdown of its anglophone region in 2017–2018.[76] (During that shutdown, authorities severed internet connectivity, but SMS services remained functional.) SMSWithoutBorders allows citizens to register their Twitter and Gmail credentials with the service and then to use their mobile phones' SMS functions during an internet shutdown to post on Twitter or to send/receive emails.[77]

One tool designed for circumventing long-term internet controls in Iran is Nahoft (created by United for Iran, an Iranian human rights and civil liberties group). Nahoft is not an actual messaging app but instead bypasses Iranian censors' keyword-based blocking on unencrypted channels by making encrypted text look unencrypted to a naive classification system. Nahoft is designed to work in very narrow scenarios as a communications option of last resort in the event that the Iranian government decides to fully disconnect the country and force its citizens to exclusively use national substitutes (which the state can control and monitor).[78]

Serverless circumvention tools also demonstrate promise and can be used to either open internet access during short-term disruptions or to get around longer-term restrictions. Unlike VPNs, programs such as Intra, GoodbyeDPI, Green Tunnel, and Geneva do not tunnel traffic or rely upon third-party servers, which means that ISPs cannot easily block them. Instead, they rely upon "autonomous censorship circumvention software" to regain access to country-wide blocked websites.[79] Geneva, for example, uses automatic processes to learn how to circumvent censorship. When data packets are sent through the internet, governments using DPI blocking apply keyword recognition programs to determine whether to prevent a specific transmission. But Geneva "modifies how data is broken up and sent, so that the censor does not recognize forbidden content or is unable to censor the connection."[80] One drawback is that these tools are more limited in power and cannot, for example, bypass IP-based blocking.

A final option is the use of secure browsers, such as Tor Browser, although Tor is an anonymity tool meant to preserve user privacy and not a circumvention tool for getting around network censorship. Tor makes it difficult for authorities to trace the communications and web traffic of users by distributing online searches and activities between a network of servers around the world.[81] Tor servers, called entry relays, encrypt the online data and scramble the destination's IP address multiple times, preventing governments from intercepting or blocking the ultimate proxy server.[82] While Tor and other proxy servers can anonymize web traffic and bypass censorship, committed repressive governments, such as China and Russia, can IP block the Tor browser by shutting down all entry relays. In fact, as of December 2021, the Russian authorities had officially blocked access to Tor's main website in Russia, although users could circumvent this block by visiting a website mirror.[83]

Table 3 provides a breakdown of internet censorship circumvention and mitigation tools and their corresponding advantages and disadvantages.

Table 3. Internet Censorship Circumvention and Mitigation Tools

Tool	Advantages	Disadvantages
VPNs (such as Psiphon, TunnelBear, and Proton)	Allow users to bypass censorship by accessing outside proxy servers Are available for activists to download directly—no need for outside intervention	Outlawed or blocked from app store download by some governments Require an internet connection; do not work in the case of a full internet shutdown[84] Can make it difficult for users to discern whether options are untrustworthy; offer minimal privacy protections and security
Mesh networks (such as Bridgefy and Briar)	Are available for activists to download directly—no need for outside intervention Allow communication during total internet shutdowns with no internet connection required Can feature end-to-end encryption[85]	Have ranges limited by wireless transmission distance and numbers of users. (An initial range is up to 330 feet between two users.[86] However, as user density expands, the aggregate network effect correspondingly increases.)[87] Require downloading before a shutdown Are limited to domestic communications Cannot be used to access internet sites/social media; limited to messaging Can be infiltrated by law enforcement; risks of metadata collection to identify users[88] Can be blocked from app stores at governments' requests
Private servers (such as Outline)	Allow for lawful, peer-to-peer, uncensored internet sharing across borders Avoid detection and DNS or IP blocking through decentralized design	Require downloading before internet connections are restricted Requires some technical expertise by the host to set up the server
Serverless circumventions (such as Intra, GoodbyeDPI, Green Tunnel, and Geneva)	Do not rely upon third-party servers; instead use autonomous censorship circumvention software to regain access to blocked websites	Limited power; for example, cannot bypass IP-based blocking
Tor Browser	Enables anonymous browsing Is a useful anti-surveillance tool	Is not difficult for governments to block Is not appropriate as a circumvention tool

Strategies to Counter Internet Shutdowns

While there is not a one-size-fits-all solution to combating government internet shutdowns, a combination of approaches can make a big difference in helping both citizens within countries affected by internet shutdowns or blockages and outside actors, like concerned democratic governments and technology companies, push back against restrictions. This section will discuss the following concepts: preparing in advance for internet shutdowns, prioritizing user accessibility to facilitate scaling up, employing nontechnological strategies to complement digital solutions, and raising the costs for governments and companies to carry out shutdowns.

Preparing in Advance for Internet Shutdowns

Civil society organizations should consider what steps they can take in advance to prepare for internet shutdowns before they occur. By the time a government implements a shutdown, it is often too late to adapt by downloading VPNs, mesh networking apps, or other circumvention measures. Citizens should proactively acquire digital tools ahead of certain windows of risk, such as elections, religious holidays, and planned demonstrations, while it is still possible to connect to the internet. [89]

Citizens should also consider downloading multiple tools ahead of potential windows of risk, enabling users to prepare for different shutdown methods that the state might implement. For instance, residents in an affected area would ideally download VPNs, mesh networks, and peer-to-peer server-sharing options prior to a shutdown. The utility of each app would vary depending on the type of shutdown or censorship instrument implemented by the authorities, but such redundancy would give users options if any one tool became unavailable.

Digital rights organizations, supported by democratic governments, can anticipate shutdown-triggering events and coordinate widespread downloads of circumvention tools. McManamen explains that "when [Psiphon] expects that there will be disruptions, we will usually run a campaign telling our existing users to tell other non-users to download this so that they have it" on their devices if the internet becomes inaccessible.[90] Proactive messaging on social media or communications apps can alert citizens to potential shutdowns and disseminate instructions about how to download circumvention programs (although the risk of this approach is that it could raise security concerns where downloading such apps is prohibited). Organizations can also store their preferred circumvention apps in the form of APK files (only possible for Android users), which can be shared device-to-device by text, Bluetooth, or email, even without internet access.[91] Activists can even set up Telegram bots to distribute links to download apps in case an app store is blocked.[92] It is also a good idea for civil society organizations to improve their own resistance to blocking or state cyber intrusions by switching over to encrypted websites or using a content delivery network (CDN), which is a geographically dispersed group of servers that can protect against unusual spikes

in internet traffic such as distributed denial of service attacks. Certain firms offer enhanced protection for civil society groups; Project Galileo, operated by CloudFlare, for example, is specifically designed to help at-risk public interest organizations stay online.[93]

Prioritizing User Accessibility

To facilitate proliferating circumvention methods, technology companies need to prioritize user accessibility. The harder it is for users to install anticensorship tools, the less likely that individuals will actually use the software. An app's accessibility depends on four factors: cost, design, trust, and local ties.

Circumvention technologies can best serve communities around the world if they are *free or cost a minimal amount.* Many VPNs charge a subscription fee for access, which can be prohibitive for lower-income citizens. Similarly, distributed server-sharing tools, such as Outline, can require the host to pay a monthly fee to provide for cloud hosting of the network (although at least in the case of Outline, because one of its servers can be used by dozens of individuals, the overall cost is slight). The problem with no-cost services is that the programs still require resources in order to run—programmers don't work for free and acquiring necessary technology can be costly. A so-called freemium model, which offers basic services to users at no cost but charges a premium for supplemental or advanced features, is one alternative. Another option is for democratic governments to provide significantly scaled up subsidies in order to keep certain circumvention programs viable.

The design of the product must also be *accessible*. Users with low digital literacy need to be able to learn how to use these services quickly and effectively. Products that require technical knowledge to complete numerous steps before accessing the internet may narrow the potential user pool and prevent mass adoption. In contrast, thoughtful design features, such as simply pressing a button to activate the circumvention protocols, can help all users navigate blockages regardless of their prior experience with technology. Tool developers can lower barriers to entry by paying attention to local context and citizen capacity. Says McManamen: "At the end of the day, users are going to use whatever is working, easiest, and freest."[94]

By the same token, it is exceptionally hard for developers to create new circumvention tools: working across different platforms and dealing with dissimilar networking and VPN application programming interfaces (APIs) is challenging. While there is a lot of focus on developing new protocols to circumvent internet controls, there has not been the same level of emphasis on developing new apps. But new protocols mean very little if they never reach users. Investing in the infrastructure to facilitate the development of circumvention tools—to make their development more accessible to a wider array of programmers—can bring a virtuous effect. If, for example, small teams of two or three people could independently build new circumvention tools, then this would enhance technological diversity and make the online ecosystem much more resilient.

Citizens are most likely to adopt technologies to circumvent shutdowns if the organizations advocating for them have *local ties* to and knowledge of the community. Maria Xynou of the Open Observatory of Network Interference attributes the organization's success to its relationships with digital rights organizations already operating on the ground, organizations that spread information about how to respond to shutdowns. Community-based networks can provide instructions in local languages for how to download tools during a shutdown. And they can carry out this work in person, directly in the community, to build trust.[95] For instance, during the 2019 shutdown in Iran, experienced Psiphon users posted paper flyers in apartment buildings to provide residents with a location to visit to learn how to download a copy in person.[96] These efforts facilitated trust in an unknown technology by directly pairing users with advocates in their communities.

Local relationships also enable tech companies to design solutions with an understanding of domestic network characteristics. For instance, engineers designed United for Iran's Nahoft tool with Iran's National Information Network intranet in mind. Iran's authorities have shown a growing interest in forcing Iranians away from international services like Google, Instagram, and WhatsApp and onto domestic platforms controlled and monitored by the state. In response, Nahoft allows citizens to communicate covertly on communications platforms by scrambling their messages (the text resembles a string of garbled Farsi) and then having the app decrypt the text once delivered to the intended person.[97] When organizations are familiar with the nuances and specific features of a censorship system, they can build agile responses tailored to local contexts.

Finally, *building user trust* is critical as well. As mentioned earlier, one big challenge for users attempting to download a circumvention VPN is which one to choose. How can they be sure that a particular VPN will not degrade their operating system, sell their PII to third parties, or operate as a surveillance plant for government authorities? There are nascent efforts to list "trusted" programs to safeguard users from harm, but unearthing these resources requires some sleuthing.[98] A simpler solution would be for Google or Apple to restrict their app stores to only listing VPNs that are privacy-protecting and secure.[99] In this area, democratic governments can play a bigger role in pushing companies to set minimum standards for trustworthy VPNs.

Employing Nontechnological Strategies to Complement Digital Solutions

It is important for activists not to rely too heavily on technological solutions to counter government shutdown strategies. Instead, civil society should complement technological methods with adaptive approaches. Ethiopia's network shutdowns offer an illustrative example. During protests led by the Oromo ethnic group in 2015–2016, the government tried to subdue the movement on several occasions by shutting down the internet for weeks at a time in the Oromia region. But protesters soon found ways around the restrictions. Resistance leader Jawar Mohammed explains in *The Rise of Digital Repression* that government authorities had left internet access intact in the capital, Addis Ababa. "So every district

would finance one person to come here [to Addis]. I post whatever we hear from them, back there. They send information through SMS or sometimes they send it through papers. I put it back online."[100] Until the government was willing to cut internet access throughout the country and risk long-term damage to the economy, Jawar had devised an innovative way to get around government restrictions.[101]

Jawar's methods exemplify a growing body of scholarship examining how emergent strategies can counteract more centralized government repression efforts. Researcher Ionut C. Popescu describes emergent strategies as a process of "navigating through an unpredictable world by improvisation and continuous learning."[102] Emergent strategies take different forms and shapes, depending on the circumstances. In Sudan, for example, sympathetic engineers working for the country's telecommunications companies reportedly formed committees to coordinate smuggling out internet-enabled SIM cards for activists to use during 2019 antigovernment protests.[103] During Sudan's latest internet shutdown in 2021, citizens used international SIM cards sent by overseas organizations and the Sudanese diaspora to broadcast information to the outside world (a method used in Iraq and the Democratic Republic of the Congo to varying degrees of success).[104] Sudanese protesters have also relied on more conventional methods to coordinate demonstrations, such as both motorbike messengers who make contact with other neighborhoods and neighborhood committees that hand out flyers and offer safety advice by walking door-to-door.[105] Demonstrators in other countries have used comparable techniques to circumvent digital controls. In Turkey, during the 2014 blockage of Twitter, activists painted instructions for circumventing the ban on the sides of buildings (see figure 3).[106]

Even in periods when the internet is completely shut down and there are few avenues through which to transmit footage, digital documentation for later use is important. Video footage helps activists and human rights investigators monitor, report, and address violations, but only if the received information is properly authenticated and verified. To that end, citizens can download specialized documentation apps, such as ProofMode, Tella, or Eyewitness to Atrocities, that supplement footage with metadata or technical information pulled from a user's phone for verification purposes.[107] Users should also consider how they can best protect their hard drive or the files stored on it from the authorities, such as using encryption software like VeraCrypt.

A growing movement to combat internet shutdowns involves using strategic litigation to get courts to overturn unlawful shutdowns. In 2019, for instance, litigants brought nineteen internet shutdown–related legal cases before courts in twelve countries, many leading to positive outcomes for the litigants.[108] In January 2020, an Indian court found that shutdowns interfered with fundamental rights to freedom of expression, that shutdown orders should be made publicly available, and that shutdowns with indefinite timelines are unconstitutional.[109] In Sudan, a litigant sued Zain, a major Sudanese telecom provider, for violating its terms of service by shutting down the internet in 2019. (Initially, the judge ordered Zain to only restore the individual's internet access, but following a successful class action lawsuit, internet access throughout Sudan was eventually restored.)[110] Similarly, in 2021, a Sudanese

Figure 3. Turkish Activists Spray-Painted Instructions on Buildings for How to Evade the Government's Internet Controls

Source: Utku Can (@utku), Twitter, March 21, 2014, https://twitter.com/utku/status/446956710502993920.

court ordered the country's telecoms companies to restore internet access, paving the way for an eventual return of service.[111] In an analysis of legal challenges to internet shutdowns, researchers from the Internet Freedom Foundation found that lawsuits fell into one of three categories: whether the government used the right procedures when ordering the shutdown; whether the government violated fundamental rights to expression, equality, and trade; or whether shutdowns hurt the country economically.[112] Strategic lawsuits represent an area of promise, but potential litigants are hampered by a lack of resources. Thus, such lawsuits are an area where democratic donors could consider scaling up funding.

Raising the Costs for Governments and Companies to Continue Implementing Shutdowns

A final strategy involves imposing costs on governments that restrict internet access. Many autocratic regimes confront a dictator's digital dilemma, in which they must balance their desire to tightly control their digital ecosystems with the necessity of maintaining an open digital environment to sustain innovation and growth.[113] In Thailand, for example,

authorities reconsidered implementing a "single internet gateway" (which is designed to consolidate the country's twelve internet gateways into a single portal managed by the state telecom) after widespread public concern that these restrictions would undermine investor confidence in Thailand's economy.[114]

As research shows, internet shutdowns can bring significant financial and reputational damage to a country. To date, researchers estimate that Myanmar's 2021 shutdown and over 10,000 hours of disrupted connectivity have led to revenue loss exceeding $2.9 billion.[115] The more that countries' publics—not to mention large domestic businesses—become aware of these costs and generate backlash against these policies, the greater the likelihood that governments will reverse course on maintaining shutdowns.

Liberal democracies have started to develop complementary norms against internet shutdowns to reinforce negative consequences. The G7 condemned "politically motivated internet shutdowns" in its June 2021 open societies statement (despite reportedly succumbing to pressure from India to soften language that originally was broader).[116] The United States has begun to explicitly condemn shutdowns in its diplomatic statements.[117] The Freedom Online Coalition launched a task force during its 2021 annual conference focused on preventing internet shutdowns.[118] These developments will help increase the costs to governments of shutting down the internet while decreasing repressive dividends.

But democracies could do more. One troubling issue is the fact that much of the censorship technology used to impose website blocks and network disruptions comes from companies based in democracies, such as Canada, Israel, the United States, and EU member states. News reporting shows that governments that commit egregious human rights violations—such as Algeria, Belarus, Egypt, Pakistan, and Uzbekistan, for example—have acquired sophisticated DPI technology from Canadian and U.S. firms, despite very clear use of this technology to support repressive policies.[119] This raises a pressing question—why have democracies failed to crack down on these sales? If the United States and other democracies take internet shutdowns and online censorship as seriously as their G7 statements purport to, then they should pursue real steps to limit the export of harm-inducing technology.

At the same time, overly broad sanctions can backfire and incentivize governments to disconnect further from the global internet. Iran's case is instructive. Researchers at Article 19, a global organization focused on preserving freedom of expression and information, contend that international sanctions have brought about three negative outcomes: First, sanctions have limited the range of services that ordinary Iranians can access to circumvent internet controls. (Because of sanctions, Iranians cannot access tools hosted on services such as GitHub, Amazon Cloud, and Google Cloud.) Second, sanctions have provided Iranian authorities with a powerful excuse to centralize state control over the internet and create a tightly controlled local alternative, for fear that the United States will eventually cut Iran off from the global internet. Third, economic isolation due to sanctions has reduced the cost of imposing new internet shutdowns, thereby increasing the frequency of state-sponsored disruptions.[120] More recently in Russia, digital rights groups have raised a similar outcry regarding the unintended effect of U.S. sanctions causing internet infrastructure providers,

like Cogent, to pull out of the country. In a joint letter to Biden, they warn that cutting off Russian access to the internet will play into the Kremlin's hands by enhancing online censorship and undermining opposition to Putin.[121] It behooves democratic governments to pursue narrowly tailored export controls rather than wider prohibitions and to consider carefully the unintended consequences of well-meaning policies that could end up strengthening the hand of the autocratic regime.

While democracies dither, authoritarians are coming up with new strategies to control the internet. Few governments have explicitly defended their right to shut down the internet, but a raft of them have passed legislation authorizing heightened internet controls. Countries such as India, Indonesia, Russia, Thailand, Turkey, Vietnam, and Uganda have enacted new laws to regulate platform content, require local data storage, and enable centralized state control over internet infrastructure.[122] As a result, private companies are faced with losing options: accede to government demands in violation of international human rights norms, fight back against government dictates and risk getting kicked out of the country, or summarily depart and lose business. Many firms are choosing the first or third option. In Myanmar, following the military coup, Norwegian telecom operator Telenor Group has put its Burmese franchise on the sales block. The company has not minced words about why it is exiting the market: "We did however arrive at the sad conclusion that it is no longer possible to adhere to these [business and human rights] principles, keep our employees safe and at the same time remain as an operator in Myanmar. This makes our continued presence in Myanmar untenable."[123] Of note, Telenor's abrupt decision to sell off its operations to the M1 Group—an outfit notorious for ignoring even basic human rights commitments—has brought condemnation from advocacy groups.[124]

Companies that stay put are often forced into unsavory compromises. For example, an investigation by Unwanted Witness, a Ugandan civil society organization, found that several pan-African firms—such as Airtel, MTN, and Stanbic Bank—have been implementing different data privacy policies based on their country of operation. Researchers found that user data protections were much higher in South Africa and Nigeria (which are democracies with more robust rule of law protections) than in Uganda (a hybrid regime in the midst of a major political regression).[125] While it is unrealistic to expect telecoms to become human rights champions, they can take modest steps to make a difference. For one, telecoms could normalize disclosure and reporting on shutdowns, placing a greater onus on governments to explain why they have authorized a particular network disruption and for what cause.[126] A Swiss telecom, Telia Company, for example, uses a standardized form anytime it is requested by a government to block or restrict service leading to a serious impact on freedom of expression or individual privacy rights.[127] Telecoms should also clarify their legal obligations when governments order them to sever connectivity; shutdown orders are frequently not supported in countries' laws. The more telecoms can work collaboratively with a "coalition of allies" to push back against shutdown restrictions, the greater their prospects for minimizing harmful effects.[128]

Paradoxically, encrypted protocols, such as hypertext transfer protocol secure (HTTPS), which makes it harder for states to unilaterally block specific content, can encourage governments to adopt coercive tactics against private platforms. HTTPS forces states to

block entire websites, like in the case of Turkey's now-lifted ban on Wikipedia, rather than blocking specific entries.[129] Such broad-based bans increase citizen ire and bring high potential economic costs. Governments that are reluctant to fully ban a website or internet service are instead pressuring platforms to remove unwanted content by threatening fines or even criminal prosecution of local staff. Such was the case recently in Russia, where authorities threatened to prosecute local staff from Google and Apple if they did not comply with state orders to remove opposition leader Alexei Navalny's voting app ahead of 2021 elections, and in India, where the Delhi High Court ruled that Twitter was noncompliant with the country's controversial new information technology laws and risked losing legal immunity.[130] Without countervailing pressure from democratic governments and publics, the path of least resistance for large tech firms is to quietly accede to authoritarian censorship demands.[131]

Shifting the cost-benefit calculus for governments that impose shutdowns remains challenging. In situations where a country's leader cares little about collateral damage, options are few. Such is the case in Turkmenistan, where the government tightly controls the internet—completely banning Facebook, YouTube, and Wikipedia, for example—and blocks access to most circumvention tools.[132] The regime simply does not seem to value the country's digital economy or technological advancement enough to broaden citizens' internet access or succumb to outside pressure to ease controls. Instead, its leadership opts for isolation over growth. One of the few developments that could change the regime's shutdown stance would be the shutdown's ineffectiveness in quelling dissent. As researchers Navid Hassanpour and Jan Rydzak show, state shutdowns often bring unintended effects. In the case of Egypt, described by Hassanpour, authorities shut down the internet during the Arab Spring demonstrations. Rather than dampen protests, the shutdown led to the opposite outcome—protest escalation to unprecedented levels.[133] Likewise, in India, Rydzak found that shutdowns were strongly associated with increases in violent collective action: shutdowns "can turn a predictable situation into one that is highly volatile, violent, and chaotic. . . . Network shutdowns in India are clearly not uniformly effective, but remain prohibitively costly when maintained."[134]

In general, complete internet shutdowns will become less and less common in the future. Instead, governments will use more precise blocking methods to deny access to specific websites while avoiding general service disruptions. Myanmar's selective blocking is a good illustration. The military junta has created a system where websites are either blocked (blacklisted) or explicitly permitted (white-listed), thus maintaining the overall functionality of the internet while censoring unfavorable content.[135] More technically advanced countries, such as Russia and Iran, are starting to adopt their own versions of China's intranet, where authorities embed censorship capabilities directly into their network infrastructure and have developed capabilities to sever citizen access to international platforms and services.[136]

That still leaves a large group of countries in the middle—countries with either lower capabilities to implement digital censorship or a reluctance to fully curtail internet access due to digital economy concerns and the potential public backlash. These countries—think Turkey, Kenya, Bangladesh, or Thailand—have a greater susceptibility to outside pressure from democratic governments and international advocates.

Table 4 summarizes recommendations that democratic governments, civil society organizations, and technology companies, developers, and telecoms can pursue to push back against internet shutdown restrictions and content limitations.

Table 4. Recommended Actions to Counter Internet Shutdowns and Disruptions

Stakeholder	Recommendations
Democratic governments	• Establish clear norms regarding prohibitions against internet shutdowns and long-term internet controls; issue consistent public condemnations against internet shutdowns; and create a multilateral entity responsible for codifying and enforcing this norm • Scale up rapid response funding for digital rights groups in countries at risk for internet shutdowns and disruptions • Use economic leverage to impose costs on governments that enact shutdowns and unlawfully censor content, through targeted sanctions, export restrictions, and pressure on investors • Enact meaningful restrictions on the export of dual-use technologies, such as DPI, that enable serious human rights harms; rethink far-reaching sanctions that cut off citizens from international digital platforms yet insulate regimes from harmful effects (such as in Iran and now Russia) • Fund strategic litigation efforts intended to overturn unlawful shutdowns • Offer more consistent public support for tech companies that push back against government censorship policies like platform content takedown requests or directed telecom shutdowns; encourage tech companies to withstand pressure to disrupt or censor content • Pressure companies to uphold international human rights and business standards, based on the United Nations Guiding Principles, in countries with concerning digital repression trends; encourage companies to implement enhanced data security and privacy safeguards to protect at-risk citizens • Push tech companies to set minimum privacy and security standards for VPNs listed in app stores • Invest in the infrastructure to facilitate the development of circumvention tools; for example, make it easier for small teams to independently build tools to enhance technological diversity and make the online ecosystem more resilient • Provide scaled-up subsidies to keep circumvention programs viable
Civil society	• Anticipate shutdown-triggering events and coordinate widespread downloads in advance, including multiple circumvention tools (VPNs, mesh networks, private servers, and serverless circumvention tools) • Raise public awareness about the high economic cost to ongoing restrictions; coordinate opposition to internet restrictions across business, civic, social, and political networks • Ensure that organizations distributing circumvention tools have local ties and are responsive to community needs, including members who reside in affected communities and speak local languages • Leverage nontechnological strategies to circumvent internet controls, such as smuggling internet-enabled/international SIM cards, using motorbike messengers to maintain contact with different communities, and distributing flyers to provide instructions for circumventing bans • Use specialized documentation apps, such as ProofMode, Tella, or Eyewitness to Atrocities, to digitally document regime violations during shutdowns • Pursue strategic litigation against governments that enact unlawful shutdowns and internet controls

Table 4. Recommended Actions to Counter Internet Shutdowns and Disruptions (continued)

Stakeholder	Recommendations
Technology developers, tech companies, and telecoms	• Enlist a coalition of allies to push back against shutdown orders and blocking restrictions; enlist democratic governments to more vocally support these efforts • Commit to conducting due diligence and carrying out more transparent and robust public consultation when creating or modifying policies that affect data privacy and content moderation standards in countries of concern • Implement heightened privacy and user data protections to counter government attempts to extend surveillance or censorship measures, particularly in authoritarian contexts • Implement enhanced transparency and documentation about shutdowns and state-authorized disruptions, such as standardized reporting on shutdown and blocking requests • Clarify legal obligations when governments order telecoms to sever connectivity; telecoms should interpret shutdown orders as narrowly as possible to minimize negative effects on citizens • Build user trust in VPNs by restricting app stores to only listing VPNs that are privacy-protecting and secure • Keep costs low for circumvention technologies, such as minimizing prohibitive subscription fees for VPNs • Design accessible circumvention tools that can be used by a wide array of users; incorporate simple design features so that all users can navigate blockages regardless of technological experience

Conclusion

The most promising strategies to help citizens circumvent internet shutdowns do not involve deploying satellite internet devices or floating balloons. Instead, simpler solutions, such as encouraging citizens to download anticensorship apps or software ahead of time, are much more useful. But they do not work well without advance organizational and logistical preparation. This requires engaging local civil society organizations and holding awareness campaigns to encourage mass adoption before a shutdown initiates. Such efforts are also more likely to succeed if technologies are free, easy to use, and redundant, so that citizens can communicate and access information regardless of context or network restrictions in place. Tech companies also have a role to play in ensuring that citizens can access circumvention solutions that are privacy-preserving and secure. Effective strategies will also incorporate nontechnical adaptations, such as tapping into a diaspora network to import unlocked SIM cards, connecting with sympathetic telecoms officials to circumvent connectivity restrictions, or even using human messengers to smuggle out footage. Finally, enhanced transparency and documentation about shutdowns can also be useful. Telecoms and internet platforms, for example, can institutionalize disclosure and reporting on shutdowns, placing a greater burden on states to justify specific network disruptions.

Liberal democracies should consider the optimal mix of carrots and sticks to combat internet shutdowns. Imposing reputational and legal costs for governments and companies that participate in shutdowns—whether by supporting strategic litigation, making internet blockages more economically costly, or calling out repressive behavior in international fora—can be effective deterrents. Conversely, offering economic inducements to countries that preserve free and open internet access, and broadly incentivizing countries to partake in the digital economy, can create structural incentives against state-sponsored shutdowns. Ultimately, sustained investment and advocacy, rather than quick fixes, are the best routes to helping citizens navigate increasingly sophisticated internet controls.

About the Author

Steven Feldstein is a senior fellow in Carnegie's Democracy, Conflict, and Governance Program, where he focuses on issues of democracy, technology, human rights, and U.S. foreign policy.

Acknowledgments

The author would like to acknowledge numerous individuals and organizations for making this study possible. Special thanks to Sarah Gordon, who served as a research assistant in Carnegie's Democracy, Conflict, and Governance Program and had a direct hand in early drafts of the paper.

The author is grateful to Scott Carpenter and Jigsaw's engineering team, as well as Jan Rydzak and Samuel Woodhams, for generously giving their time to read through prior drafts of this paper and offering valuable advice and feedback.

The author would also thank the Ford Foundation and the Open Society Foundations for support to Carnegie's Democracy, Conflict, and Governance Program, where this research work is based. The author alone is responsible for the views expressed.

Notes

1 Marianne Diaz Hernandez, Rafael Nunes, Felicia Anthonio, and Sage Cheng, "#KeepItOn Update: Who Is Shutting Down the Internet in 2021?," Access Now, June 7, 2021, https://www.accessnow.org/who-is-shutting-down-the-internet-in-2021.

2 Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, "Ending Internet Shutdowns: A Path Forward," United Nations Human Rights Council A/HRC/47/24/Add.2, June 15, 2021, https://undocs.org/A/HRC/47/24/Add.2.

3 Dan Milmo, "Russia Blocks Access to Facebook and Twitter," *Guardian*, March 4, 2022, https://www.theguardian.com/world/2022/mar/04/russia-completely-blocks-access-to-facebook-and-twitter; and Shannon Bond and Bobby Allyn, "Russia Is Restricting Social Media. Here's What We Know," NPR, March 7, 2022, https://www.npr.org/2022/03/07/1085025672/russia-social-media-ban.

4 James Vincent, "Russia Bans Instagram As Promised, Blocking Access for 80 Million Users," The Verge, March 14, 2022, https://www.theverge.com/2022/3/14/22976603/russia-bans-instagram-facebook-meta-call-to-violence.

5 Will Oremus, "The Real Reason Russia Is Blocking Facebook," *Washington Post*, March 5, 2022, https://www.washingtonpost.com/technology/2022/03/05/russia-facebook-block-putin-ban-roskomnadzor; and "Russia Blocks Access to BBC and Voice of America Websites," Reuters, March 4, 2022, https://www.reuters.com/business/media-telecom/russia-restricts-access-bbc-russian-service-radio-liberty-ria-2022-03-04.

6 Russell Goldman, "Myanmar's Coup, Explained," *The New York Times*, February 1, 2021, https://www.nytimes.com/article/myanmar-news-protests-coup.html; Lily Hay Newman, "Myanmar's Internet Shutdown Is an Act of 'Vast Self-Harm,'" *WIRED*, April 2, 2021, https://www.wired.com/story/myanmar-internet-shutdown.

7 Samuel Woodhams and Simon Migliano, "Government Internet Shutdowns Cost $5.5 Billion in 2021," Top10VPN, January 13, 2022, https://www.top10vpn.com/research/cost-of-internet-shutdowns.

8 Ernesto Londoño and Daniel Politi, "'Terror': Crackdown After Protests in Cuba Sends a Chilling Message," *New York Times,* July 28, 2021, https://www.nytimes.com/2021/07/28/world/americas/cuba-protests-crackdown-arrests.html; and Samuel Woodhams and Simon Migliano, "Government Internet Shutdowns Cost $5.5 Billion in 2021."

9 Samuel Woodhams and Simon Migliano, "Government Internet Shutdowns Cost $5.5 Billion in 2021."

10 Declan Walsh, "Sudanese Security Forces Fire on Protesters as Military Tightens Grip," *New York Times,* November 13, 2021, https://www.nytimes.com/2021/11/13/world/africa/sudan-protests.html.

11 Jina Moore, "Anatomy of an Internet Shutdown," Rest of World, May 12, 2020, https://restofworld.org/2020/sudan-revolution-internet-shutdown.

12 "Internet Shutdowns and Blockings Continue to Hide Atrocities of Military Coup in Sudan," Access Now, November 23, 2021, https://www.accessnow.org/update-internet-shutdown-sudan; and NetBlocks (@netblocks), "[Information emoji] Update: Mobile internet is being restored in #Sudan after a day-long telecommunication disruption targeting the first anti-coup protests of 2022 in #Khartoum; real-time metrics show incident duration of ~10 hours [Chart Increasing emoji] #Jan2March," Twitter, January 2, 2022, 1:44 PM, https://twitter.com/netblocks/status/1477712295023333376?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1477712295023333376%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fnetblocks.org%2Freports%2Finternet-disrupted-in-sudan-amid-reports-of-coup-attempt-Q8ov93yn.

13 Marianne Diaz Hernandez et al., "#KeepItOn Update: Who Is Shutting Down the Internet in 2021?"

14 "FOC Joint Statement on Freedom of Expression Online Presented at the 47th Session of the United Nations Human Rights Council," Freedom Online Coalition, July 2021, https://freedomonlinecoalition.com/wp-content/uploads/2021/07/FOC-Joint-Statement-on-Freedom-of-Expression-Online-Presented-at-the-47th-Session-of-the-United-Nations-Human-Rights-Council.pdf.

15 Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, "Ending Internet Shutdowns: A Path Forward"; and United Nations Human Rights Committee (129th Session, 2020, virtual), "General Comment No. 37 (2020) on the Right of Peaceful Assembly (Article 21): Human Rights Committee," CCPR/C/GC/37, September 17, 2020, paragraph 6, https://digitallibrary.un.org/record/3884725?ln=en.

16 Marco Rubio, "Rubio Outlines Steps POTUS Must Take Following Historic Protests in Cuba," Marco Rubio: US Senator for Florida, July 12, 2021, https://www.rubio.senate.gov/public/index.cfm/press-releases?id=8F7A6638-A9AB-46C2-953B-7396957220F8.

17 Bobby Caina Calvan and Freida Frisaro, "DeSantis Presses Biden to Help Keep Internet Flowing in Cuba," Associated Press, July 15, 2021, https://apnews.com/article/cuba-florida-riots-08875572486e356aaf01105016626a1c.

18 David Shepardson, "U.S. Reviewing Whether It Can Help Restore Internet Access in Cuba –Biden," Reuters, July 15, 2021, https://www.reuters.com/world/americas/us-reviewing-whether-it-can-help-restore-internet-access-cuba-2021-07-15.

19 Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance* (Washington, DC: Carnegie Endowment for International Peace, 2021), 34.

20 Margaret Hu, "Kazakhstan's Internet Shutdown Is the Latest Episode in an Ominous Trend: Digital Authoritarianism," The Conversation, January 24, 2022, https://theconversation.com/kazakhstans-internet-shutdown-is-the-latest-episode-in-an-ominous-trend-digital-authoritarianism-174651; Nita Bhalla and Alice McCool, "100 Hours in the Dark: How an Election Internet Blackout Hit Poor Ugandans," Reuters, January 20, 2021, https://www.reuters.com/article/us-uganda-internet-rights-trfn/100-hours-in-the-dark-how-an-election-internet-blackout-hit-poor-ugandans-idUSKBN29P1V8; "Belarus: Internet Disruptions, Online

Censorship," Human Rights Watch, August 28, 2020, https://www.hrw.org/news/2020/08/28/belarus-internet-disruptions-online-censorship; Patrick Kingsley, "Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards," New York Times, September 2, 2019, https://www.nytimes.com/2019/09/02/world/africa/internet-shutdown-economy.html; "India," *Freedom on the Net 2021,* Freedom House, 2021, https://freedomhouse.org/country/india/freedom-net/2021; Felicia Anthonio, Alexia Skok, and Marianne Diaz Hernandez, "Voices From Tigray: Ongoing Internet Shutdown Tearing Families, Communities, and Businsses Apart," Access Now, September 13, 2021, https://www.accessnow.org/voices-from-tigray-ongoing-internet-shutdown-tearing-families-communities-businesses-apart/#:~:text=Since%20the%20start%20of%20the,and%20mobile%20internet%20shut%20off; Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance* (Washington, DC: Carnegie Endowment for International Peace, 2021), 96–133; "Vietnam," Freedom on the Net 2021, Freedom House, 2021, https://freedomhouse.org/country/vietnam/freedom-net/2021; "Russia: Growing Internet Isolation, Control, Censorship," Human Rights Watch, June 18, 2020, https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship; Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton, New Jersey: Princeton University Press, 2018); Mahsa Alimardani, "Iran: Tightening the Net 2020 After Blood and Shutdowns," Article 19, September 2020, https://www.article19.org/wp-content/uploads/2020/09/TTN-report-2020.pdf; and RFE/RL's Turkmen Service, "Internet In Turkmenistan, Already The World's Slowest, Faces Further Restrictions," Radio Free Europe/Radio Liberty, January 13, 2022, https://www.rferl.org/a/turkmenistan-internet-slowest-restrictions/31652467.html.

21 "What's Happening in Tigray? Internet Shutdowns Avert Accountability," Access Now, July 29, 2021, https://www.accessnow.org/tigray-internet-shutdowns; Natalia Krapiva, Anastasiya Zhyrmont, and Alexia Skok, "Timeline: Kazakhstan Internet Shutdowns Aim to Crush Protests, Hide State Violence," January 12, 2022, https://www.accessnow.org/kazakhstan-internet-shutdowns-protests-almaty-timeline-whats-happening.

22 "Jordan's Internet Throttling to Censor Protesters Must End," Access Now, March 19, 2021, https://www.accessnow.org/jordan-protest-throttling; "Update: Internet Access, Censorship, and the Myanmar Coup," Access Now, updated January 31, 2022, https://www.accessnow.org/update-internet-access-censorship-myanmar; and Samuel Woodhams, "The Rise of Internet Throttling: A Hidden Threat to Media Development," Center for International Media Assistance, May 20, 2020, https://www.cima.ned.org/publication/the-rise-of-bandwidth-throttling-a-hidden-threat-to-media-development.

23 "Internet Society Perspectives on Internet Content Blocking: An Overview," Internet Society, March 2017, https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf.

24 Gian M. Volpicelli, "The Draconian Rise of Internet Shutdowns," *WIRED,* September 2, 2021, https://www.wired.co.uk/article/internet-shutdowns; and "Major IP Address Blocks for Pakistan," *Nirsoft,* https://www.nirsoft.net/countryip/pk.html.

25 Ryan Gallagher, "U.S. Company Faces Backlash After Belarus Uses Its Tech to Block Internet," *Bloomberg,* September 11, 2020, https://www.bloomberg.com/news/articles/2020-09-11/sandvine-use-to-block-belarus-internet-rankles-staff-lawmakers?sref=QmOxnLFz; Kevin Bock et al., "Exposing and Circumventing China's Censorship of ESNI," Great Firewall Report, August 7, 2020, https://gfw.report/blog/gfw_esni_blocking/en; "Sandvine, Francisco Partners Facing Mounting Pressure for Accountability Around Censorship Tools," Access Now, September 23, 2020, https://www.accessnow.org/sandvine-francisco-partners-facing-mounting-pressure-for-accountability-around-censorship-tools; and "Russia: Growing Internet Isolation, Control, Censorship," Human Rights Watch, June 18, 2020, https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship.

26 "The Internet Shutdowns Issue," The Current 004, Jigsaw, 2021, https://jigsaw.google.com/the-current/shutdown.

27 "Internet Society Perspectives on Internet Content Blocking: An Overview," Internet Society.

28 Carrie Mihalcik, "Google: Turkey Is Blocking Our DNS Service," CNET, March 30, 2014, https://www.cnet.com/tech/services-and-software/google-confirms-turkey-is-blocking-its-dns-service; and Simone Basso, "DNS Over TLS Blocked in Iran," Open Observatory of Network Interference, June 24, 2020, https://ooni.org/post/2020-iran-dot.

29 Apornrath Phoonphongphiphat, "Thailand to Block 2,000 Websites Ahead of Pro-Democracy Protests," *Nikkei Asia*, September 18, 2020, https://asia.nikkei.com/Politics/Turbulent-Thailand/Thailand-to-block-2-000-websites-ahead-of-pro-democracy-protests#:~:text=Thailand%20to%20block%202%2C000%20websites%20ahead%20of%20pro%2Ddemocracy%20protests,-Clampdown%20targets%20Facebook&text=BANGKOK%20%2D%2D%20Thailand's%20government%20is,pro%2Ddemocracy%20movement%20this%20weekend.

30 Ebenezer Obadare, "Twitter Ban Shows Limits of State Power in Nigeria," Africa In Transition (blog), Council on Foreign Relations, January 18, 2022, https://www.cfr.org/blog/twitter-ban-shows-limits-state-power-nigeria; "Turkey," Freedom on the Net 2021, Freedom House, 2021, https://freedomhouse.org/country/turkey/freedom-net/2021; James Pearson, "Exclusive: Facebook Agreed to Censor Posts After Vietnam Slowed Traffic—Sources," Reuters, April 21, 2020, https://www.reuters.com/article/us-vietnam-facebook-exclusive/exclusive-facebook-agreed-to-censor-posts-after-vietnam-slowed-traffic-sources-idUSKCN2232JX.

31 Alyson Chadwick and Simon Billenness, "Opinion: Myanmar's Military Is Using TikTok Against Protesters. The App Must Take a Stand," *Washington Post*, March 16, 2021, https://www.washingtonpost.com/opinions/2021/03/16/myanmars-military-is-using-tiktok-against-protesters-app-must-take-stand/; "Resist Myanmar's Digital Coup: Stop the Military Consolidating Digital Control," Access Now, February 8, 2022, https://www.accessnow.org/myanmars-digital-coup-statement; Daniel Mwesigwa, "Uganda Abandons Social Media Tax But Slaps New Levy on Internet Data," Collaboration on International ICT Policy in East and Southern Africa, July 1, 2021, https://cipesa.org/2021/07/uganda-abandons-social-media-tax-but-slaps-new-levy-on-internet-data/#:~:text=Introduced%20on%20July%201%2C%202018,Facebook%2C%20Twitter%2C%20and%20WhatsApp.&text=In%20the%20second%20year%2C%20the,a%20paltry%20USD%2016.3%20million; Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*, 96–133; and "Turkey," Freedom on the Net 2021, Freedom House, 2021, https://freedomhouse.org/country/turkey/freedom-net/2021.

32 Marianne Diaz Hernandez et al., "#KeepItOn Update: Who Is Shutting Down the Internet in 2021?"

33 Keith Proctor, "Social Media and Conflict: Understanding Risks and Resilience; An Applied Framework for Analysis," Mercy Corps, July 2021, https://www.mercycorps.org/sites/default/files/2021-08/Assessing-Digital-Conflict-Risks-Resilience-073021.pdf.

34 Samuel Woodhams and Simon Migliano, "Government Internet Shutdowns Cost $5.5 Billion in 2021."

35 Woodhams and Migliano use a slightly different methodology than Access Now to document internet shutdowns. As a result, their 2021 numbers vary from Access Now's totals. Ibid.

36 Eleanor Marchant and Nicole Stremlau, "A Spectrum of Shutdowns: Reframing Internet Shutdowns From Africa," *International Journal of Communication* 14 (2020): 18; and Jan Rydzak, "A Tightrope Over the Shadows: Grim Prospects in the Fight Against Shutdowns," in *Issues on the Frontlines of Technology and Politics*, ed. Steven Feldstein, Carnegie Endowment for International Peace, 2021, 19–20.

37 Leonid Kovachich and Andrei Kolesnikov, "Digital Authoritarianism With Russian Characteristics?," Carnegie Endowment for International Peace, April 21, 2021, https://carnegiemoscow.org/2021/04/21/digital-authoritarianism-with-russian-characteristics-pub-84346.

38 "Russia Starts Rolling Out DPI Filtration Tech That Might Finally Block Telegram," *Meduza,* September 27, 2019, https://meduza.io/en/news/2019/09/27/russia-starts-rolling-out-dpi-filtration-tech-that-might-finally-block-telegram.

39 Adam Satariano and Paul Mozur, "Russia Is Censoring the Internet, With Coercion and Black Boxes," *New York Times,* October 22, 2021, https://www.nytimes.com/2021/10/22/technology/russia-internet-censorship-putin.html; Ksenia Ermoshina, Benjamin Loveluck, and Francesca Musiani, "A Market of Black Boxes: The Political Economy of Internet Surveillance and Censorship in Russia," *Journal of Information Technology & Politics,* April 1, 2021, https://www.tandfonline.com/doi/full/10.1080/19331681.2021.1905972?scroll=top&needAccess=true.

40 Justin Sherman, "Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior," Atlantic Council, July 12, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior; Andrei Soldatov and Irina Borogan, "Opinion: Vladimir Putin Is Finally Getting the Internet He Wants," *Washington Post,* September 22, 2021, https://www.washingtonpost.com/opinions/2021/09/22/kremlin-is-pushing-internet-users-to-rely-on-runet.

41 Will Oremus, "The Real Reason Russia Is Blocking Facebook"; "Russia Blocks Access to BBC and Voice of America Websites," Reuters; Dan Milmo, "Russia Blocks Access to Facebook and Twitter"; and James Vincent, "Russia Bans Instagram As Promised, Blocking Access for 80 Million Users."

42 See, for example, a report on Israeli telecommunications company Allot Ltd., which provides DPI technology to fourteen ISPs in twenty-one countries to restrict content. Samuel Woodhams and Christine O'Donnell, "The Tech Companies Behind Internet Shutdowns: Allot Ltd.," Top10VPN, June 29, 2021, https://www.top10vpn.com/research/internet-shutdown-tech-allot.

43 "New Zealand's DIA Selects Allot to Protect Its Citizens From Digital Child Exploitation Content," Allot Ltd., August 24, 2020, https://www.allot.com/corporate/media-center/press-releases/new-zeland-dia-protects-digital-child-exploitation-content-with-allot.

44 Elissa Miller, "Egypt Leads the Pack in Internet Censorship Across the Middle East," Atlantic Council, August 28, 2018, https://www.atlanticcouncil.org/blogs/menasource/egypt-leads-the-pack-in-internet-censorship-across-the-middle-east.

45 Author interview with Keith McManamen, video call, September 29, 2021.

46 Daniel Mwesigwa, "Uganda Abandons Social Media Tax But Slaps New Levy on Internet Data"; and "Myanmar Junta Raises SIM and Internet Taxes to Silence Opposition," *Irrawaddy*, January 12, 2022, https://www.irrawaddy.com/news/burma/myanmar-junta-raises-sim-and-internet-taxes-to-silence-opposition.html.

47 "An update to the Twitter Transparency Center," Twitter Inc., January 25, 2022, https://blog.twitter.com/en_us/topics/company/2021/transparency-19.

48 Another idea gaining momentum is to build community-based networks to provide internet access to smaller, local populations. This model offers some promise in that it avoids having citizens rely on national-level ISPs for online access and can fly under the radar if/when a government decides to impose censorship controls. On the other hand, if government authorities are sufficiently committed to blocking online content, they can easily order community networks to comply with regulations, too. See Kim Harrisberg, "Bridging Africa's Digital Divide: The Rise of Community Internet," World Economic Forum, December 3, 2021, https://www.weforum.org/agenda/2021/12/bridging-africas-digital-divide-the-rise-of-community-internet.

49 Christopher Mims, "Elon Musk and Amazon Are Battling to Put Satellite Internet in Your Backyard," *Wall Street Journal,* March 20, 2021, https://www.wsj.com/articles/elon-musk-and-amazon-are-battling-to-put-satellite-internet-in-your-backyard-11616212827.

50 Graeme Massie, "Ukraine's Leaders Thank Elon Musk for Latest Delivery of Satellite-Internet Gear," Independent, March 10, 2022, https://www.independent.co.uk/news/world/europe/ukraine-russia-elon-musk-starlink-b2032413.html.

51 Rebecca Ratcliffe, "Myanmar Junta Bans Satellite Dishes in Media Crackdown," *Guardian,* May 5, 2021, https://www.theguardian.com/world/2021/may/05/myanmar-junta-bans-satellite-dishes-in-media-crackdown.

52 Michael Caster, "Why Elon Musk Won't Save Us From Internet Shutdowns," *Vice,* May 10, 2021, https://www.vice.com/en/article/5dbbe5/elon-musk-satellite-internet. See also "What Is Satellite Internet and How Does It Work?," Satoms (blog), May 1, 2018, https://satoms.com/satellite-internet.

53 Author interview with Michael Caster, in-person interview, Washington, DC, September 14, 2021.

54 Michael Caster, "Why Elon Musk Won't Save Us from Internet Shutdowns."

55 Salvatore Candido, "1 connection, 7 balloons, 1,000 kilometers," X, the Moonshot Factory, September 11, 2018, https://blog.x.company/1-connection-7-balloons-1-000-kilometers-74da60b9e283?gi=80c57c0021d6.

56 Abdi Latif Dahir, "A Bird? A Plane? No, It's a Google Balloon Beaming the Internet," *New York Times,* July 7, 2020, https://www.nytimes.com/2020/07/07/world/africa/google-loon-balloon-kenya.html; Alastair Westgarth, "Turning On Project Loon in Puerto Rico," X, the Moonshot Factory, October 20, 2017, https://blog.x.company/turning-on-project-loon-in-puerto-rico-f3aa41ad2d7f; and Neel V. Patel, "Google Is Going to Deploy Loon Balloons in Rural Peru," *MIT Technology Review,* November 21, 2019, https://www.technologyreview.com/2019/11/21/131863/google-is-going-to-deploy-loon-balloons-in-rural-peru.

57 Manish Singh, "Alphabet Shuts Down Loon Internet Balloon Company," TechCrunch, January 21, 2021, https://techcrunch.com/2021/01/21/google-alphabet-is-shutting-down-loon-internet/?guccounter=1.

58 Colin Neagle, "More of Google's Project Loon Internet Balloons Will Crash Into U.S. Backyards Soon," Network World, June 3, 2015, https://www.networkworld.com/article/2931094/more-of-googles-project-loon-internet-balloons-will-crash-into-u-s-backyards-soon.html.

59 Tali Arbel, "EXPLAINER: Could Balloons Power Uncensored Internet in Cuba?," Associated Press, July 17, 2021, https://apnews.com/article/technology-joe-biden-business-cuba-4fd3378eb76f6c750f6723a11b190ff1.

60 "Surveillance Self-Defense: Choosing the VPN That's Right for You," EFF, March 7, 2019, https://ssd.eff.org/en/module/choosing-vpn-thats-right-you.

61 "Digital Safety: Internet Shutdowns," Committee to Protect Journalists, April 13, 2021, https://cpj.org/2021/04/digital-safety-internet-shutdowns.

62 Jake Rudnitsky, "Russia Blocks NordVPN, Express VPN in Bid to Control Content," *Bloomberg*, September 3, 2021, https://www.bloomberg.com/news/articles/2021-09-03/russia-blocks-nord-vpn-express-vpn-in-bid-to-control-content?sref=QmOxnLFz; "TunnelBear Circumvents Iran VPN Block, Launches 10GB Monthly Offer in the Country," TunnelBear, September 1, 2020, https://www.tunnelbear.com/blog/tunnelbear-circumvents-iran-vpn-block; "China Tells Carriers to Block Access to Personal VPNs by February," *Bloomberg,* July 10, 2017, https://www.bloomberg.com/news/articles/2017-07-10/china-is-said-to-order-carriers-to-bar-personal-vpns-by-february?sref=QmOxnLFz.

63 Michael Kan, "DHS: Spying Risk From Foreign VPNs Is Real," *PC Mag*, May 29, 2019, https://www.pcmag.com/news/dhs-spying-risk-from-foreign-vpns-is-real.

64 Simon Migliano, "Internet Shutdowns & Free VPNs: Are The Most Popular Apps Safe?," Top10VPN, January 13, 2022, https://www.top10vpn.com/research/free-vpn-investigations/internet-shutdown-vpn-security.

65 Andy Greenberg, "Alphabet's 'Outline' Software Lets Anyone Run a Homebrew VPN," *WIRED,* March 28, 2018, https://www.wired.com/story/alphabet-outline-vpn-software.

66 Zohair A., "The Only Complete Alphabet Outline VPN Review," Security Gladiators, updated July 2, 2021, https://securitygladiators.com/alphabet-outline-vpn.

67 "How It Works," *Outline*, https://getoutline.org/how-it-works.

68 Kelsey Houston-Edwards, "The Mathematics of How Connections Become Global," *Scientific American,* April 1, 2021, https://www.scientificamerican.com/article/the-mathematics-of-how-connections-become-global.

69 Michael Caster, "How to Bypass 'Digital Dictatorship' During the Myanmar Coup," *Vice,* February 8, 2021, https://www.vice.com/en/article/dy8ekx/how-to-bypass-digital-dictatorship-during-the-myanmar-coup.

70 Michael Caster, "How to Bypass 'Digital Dictatorship' During the Myanmar Coup."

71 Kelsey Houston-Edwards, "The Mathematics of How Connections Become Global."

72 Author interview with Jorge Rios, video call, October 7, 2021.

73 John Koetsier, "Hong Kong Protesters Using Mesh Messaging App China Can't Block: Usage Up 3685%," *Forbes,* September 2, 2019, https://www.forbes.com/sites/johnkoetsier/2019/09/02/hong-kong-protestors-using-mesh-messaging-app-china-cant-block-usage-up-3685/?sh=7504b927135a.

74 Martin R. Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková, "Mesh Messaging in Large-Scale Protests: Breaking Bridgefy," in K.G. Paterson (ed.), Topics in Cryptology – CT-RSA 2021, Lecture Notes in Computer Science, vol 12704, Springer, Cham, May 11, 2021, 375–398, https://link.springer.com/chapter/10.1007%2F978-3-030-75539-3_16; and Dan Goodin, "Bridgefy, the Messenger Promoted for Mass Protests, Is a Privacy Disaster," Ars Technica, August 24, 2020, https://arstechnica.com/features/2020/08/bridgefy-the-app-promoted-for-mass-protests-is-a-privacy-disaster.

75 Other examples of creative shutdown work-arounds abound. Coda Story recently reported how computer programmers were able to circumvent the 2022 Kazakhstan shutdown by identifying five open network ports (out of a total of 65,000) that allowed them to establish an outside internet connection: "[the programmers] later learned that it was a bug in outdated Cisco equipment, used widely by Kazakh telecom operators, which had accidentally kept these ports open." See Katia Patin, "Kazakhstan Shut Down Its Internet. These Programmers Opened a Backdoor," Coda Story, January 27, 2022, https://www.codastory.com/authoritarian-tech/kazakhstan-shut-down-its-internet-these-programmers-opened-a-backdoor.

76 Patrick Kingsley, "Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards," *New York Times*, September 2, 2019, https://www.nytimes.com/2019/09/02/world/africa/internet-shutdown-economy.html.

77 Author interview with SMSWithoutBorders, email exchange, September 28, 2021. Note that a government could order telecoms to block the phone number that SMSWithoutBorders uses.

78 Author interview with United for Iran, email exchange, September 29, 2021; and Lily Hay Newman, "A New App Helps Iranians Hide Messages in Plain Sight," WIRED, September 17, 2021, https://www.wired.com/story/nahoft-iran-messaging-encryption-app. Another innovative Iranian circumvention tool is Toosheh, which uses common satellite equipment to deliver digital content without relying on internet access. It was created by a U.S. non-profit, NetFreedom Pioneers. See Andy Greenberg, "The Ingenious Way Iranians Are Using Satellite TV to Beam in Banned Internet," *WIRED*, April 22, 2016, https://www.wired.com/2016/04/ingenious-way-iranians-using-satellite-tv-beam-banned-data.

79 "GoodbyeDPI," Open Technology Fund, https://www.opentech.fund/results/supported-projects/goodbyedpi.

80 University of Maryland, "New Artificial Intelligence System Automatically Evolves to Evade Internet Censorship," ScienceDaily, November 13, 2019, https://www.sciencedaily.com/releases/2019/11/191113124822.htm.

81 "Ways to Circumvent the Internet Shutdown in the Democratic Republic of Congo," Access Now, December 19, 2016, https://www.accessnow.org/ways-circumvent-internet-shutdown-democratic-republic-congo.

82 "Countermeasures," in "The Internet Shutdowns Issue," The Current 004, Jigsaw, 2021, https://jigsaw.google.com/the-current/shutdown/#countermeasures.

83 mrphs, "Breaking Through Censorship Barriers, Even When Tor Is Blocked," Tor Blog, August 3, 2016, https://blog.torproject.org/breaking-through-censorship-barriers-even-when-tor-blocked; ggus, "Responding to Tor censorship in Russia," Tor Blog, December 7, 2021, https://blog.torproject.org/tor-censorship-in-russia.

84 Benmin Smith, "Does VPN Work Without WiFi? (Answered)," Internet Access Guide, May 12, 2020, https://internet-access-guide.com/does-vpn-work-without-wifi.

85 Mike Butcher, "Bridgefy Launches End-to-End Encrypted Messaging for the App Used During Protests and Disasters," TechCrunch, November 2, 2020, https://techcrunch.com/2020/11/02/bridgefy-launches-end-to-end-encrypted-messaging-for-the-app-used-during-protests-and-disasters.

86 "What Are Mesh Networks and How Do They Work?" Bridgefy, April 15, 2021, https://bridgefy.me/what-are-mesh-networks-and-how-do-they-work.

87 Kelsey Houston-Edwards, "The Mathematics of How Connections Become Global."

88 Thomas Brewster, "Hong Kong Protesters Are Using This 'Mesh' Messaging App—But Should They Trust It?," *Forbes,* September 4, 2019, https://www.forbes.com/sites/thomasbrewster/2019/09/04/hong-kong-protesters-are-using-this-mesh-messaging-app--but-should-they-trust-it/?sh=5ae2b72318b4.

89 Keith Proctor, "Social Media and Conflict: Understanding Risks and Resilience."

90 Author interview with Keith McManamen, video call, September 29, 2021.

91 "Digital Safety: Internet Shutdowns," Committee to Protect Journalists.

92 Author interview with Keith McManamen, video call, September 29, 2021.

93 "Project Galileo by Cloudfare," Cloudfare, accessed February 8, 2022, https://www.cloudflare.com/galileo.

94 Author interview with Keith McManamen, video call, September 29, 2021.

95 Author interview with Maria Xynou, video call, October 6, 2021.

96 Author interview with Keith McManamen, video call, September 29, 2021; and Mehr Nadeem, "How the Iranian Diaspora Is Using Old-School Tech to Fight Internet Shutdown at Home," Rest of World, September 24, 2020, https://restofworld.org/2020/cat-and-mouse-censorship.

97 Author interview with United for Iran, email exchange, September 28, 2021; and Lily Hay Newman, "A New App Helps Iranians Hide Messages in Plain Sight."

98 For an example of this type of effort to compile a list of trusted programs, see "About the Project," Bypass Censorship, accessed February 8, 2022, https://www.bypasscensorship.org#about.

99 Another design solution to facilitate user trust would be for VPN services like Psiphon to adopt consistent messaging and web presence. For example, psiphon3.com and psiphon.ca are both legitimate sites, but they have completely different logos and design features that could easily spark mistrust.

100 Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*, 201.

101 Jawar's tactics mirror similar strategies used in Cameroon during the shutdown of the Anglophone region in 2017. One noteworthy innovation was the creation of impromptu communications centers just across the border from Cameroon's shutdown zone. See Abdi Latif Dahir, "Reeling From an Internet Shutdown, Startups in Cameroon Have Created an 'Internet Refugee Camp,'"

Quartz Africa, March 28, 2017, https://qz.com/africa/942879/an-internet-shutdown-in-cameroon-has-forced-startups-to-create-an-internet-refugee-camp-in-bonako-village; and Patrick Kingsley, "Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards."

102 Core elements of emergent theory include adopting recursive approaches that prioritize experimentation, learning, and iteration; using flexible, horizontal structures to enhance innovation in line with changing circumstances; employing efficient actions against a well-equipped adversary that are not reliant on significant resources to implement; and taking advantage of peer-to-peer technologies (such as communications apps and social media) to facilitate new innovations. Ionut C. Popescu, "Grand Strategy vs. Emergent Strategy in the Conduct of Foreign Policy," *Journal of Strategic Studies* 41, no. 3 (2018): 446. Popescu's theory is also echoed by W. Lance Bennett and Alexandra Segerberg's concept of "organization as communication" and "connective action," in which organizations with looser ties forged digitally through social media networks have replaced more formal, structured organizations to enable collective action and large-scale engagement on a variety of political causes. W. Lance Bennett and Alexandra Segerberg, *The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics* (New York: Cambridge University Press, 2013).

103 Jina Moore, "Anatomy of an Internet Shutdown."

104 Nita Bhalla, "SIMs to Leaflets: Sudanese Find Ways to Skirt Net Outage," Thomson Reuters Foundation, November 5, 2021, https://news.trust.org/item/20211104180126-c7sd0. See also Katie Collins, "Inside the Dystopian Nightmare of an Internet Shutdown," CNET, October 31, 2019, https://www.cnet.com/features/inside-the-dystopian-nightmare-of-an-internet-shutdown; and Patrick Kingsley, "Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards."

105 For example, a new service named Awala is exploring setting up data couriers anytime a region experiences an internet shutdown as a nontechnological circumvention strategy. See "Awala Helps to Circumvent Internet Blackouts," Awala, accessed [February 11, 2022], 2021, https://awala.network.

106 Utku Can (@utku), "Twitter is blocked in Turkey. On the streets of Istanbul, the action against censorship is graffiti DNS addresses [photo of graffiti reading "DNS: 8.8.8.8 kuşun Ötsûn, Alternatif: 8.8.4.4"]," Twitter, March 21, 2014, 6:29 AM, https://twitter.com/utku/status/446956710502993920?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E446956710502993920%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fblog.witness.org%2F2020%2F02%2Ffile-sharing-communication-internet-shutdown%2F.

107 Yvonne Ng, "Documenting During Internet Shutdowns," WITNESS, January 31, 2020, https://blog.witness.org/2020/02/documenting-during-internet-shutdowns; Yvonne Ng, "Should I Use This Documentation App?," WITNESS, January 31, 2020, https://blog.witness.org/2020/02/use-documentation-app.

108 Aayush Rathi and Arindrajit Basu, "Dialing in the Law: A Comparative Assessment of Jurisprudence on Internet Shutdowns," Association for Progressive Communications, October 30, 2020, https://www.apc.org/sites/default/files/Internet_Shutdowns_20.11.10.pdf.

109 Berhan Taye, "Targeted, Cut Off, and Left in the Dark: The #KeepItOn Report on Internet Shutdowns in 2019," Access Now, 2020, https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf.

110 "Mobile Internet Access Slowly Restored in Sudan," *Al Jazeera,* July 9, 2019, https://www.aljazeera.com/news/2019/7/9/mobile-internet-access-slowly-restored-in-sudan; "Sudan Crisis: Internet Restored—But Only for Lawyer," BBC, June 24, 2019, https://www.bbc.com/news/world-africa-48744853.

111 "Sudan court orders end to internet shutdown," Al Jazeera, November 9, 2021, https://www.aljazeera.com/news/2021/11/9/calls-for-strike-and-civil-disobedience-in-sud.

112 In response, governments have argued that the targets of shutdowns intended to commit violent acts or disturb the peace, that landline internet was still accessible (thus not impinging upon the right to free expression), or that the state enacted the shutdown within an acceptable legal framework. See Aayush Rathi and Arindrajit Basu, "Dialing in the Law: A Comparative Assessment of Jurisprudence on Internet Shutdowns.".

113 Steven Feldstein, "How the Dictator's Digital Dilemma Constrains Leaders' Choices," Net Politics (blog), Council on Foreign Relations, May 11, 2021, https://www.cfr.org/blog/how-dictators-digital-dilemma-constrains-leaders-choices.

114 Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*, 113.

115 Samuel Woodhams and Simon Migliano, "Government Internet Shutdowns Cost $5.5 Billion in 2021."

116 "2021 Open Societies Statement," G7, 2021, https://www.consilium.europa.eu/media/50364/g7-2021-open-societies-statement-pdf-355kb-2-pages.pdf; "G7 Accommodates Indian Stand on Internet Curbs," *The Hindu,* June 14, 2021, https://www.thehindu.com/news/national/g7-accommodates-indian-stand-on-internet-curbs/article34816130.ece.

117 Antony J. Blinken, "World Press Freedom Day," U.S. Department of State press statement, May 2, 2021, https://www.state.gov/world-press-freedom-day.

118 "Openness, Accessibility and Inclusion - Human Rights Online in the 2020's: Freedom Online Coalition Chair's Summary," Freedom Online Coalition and the Ministry of Foreign Affairs of Finland, December 2021, https://freedomonlinecoalition.com/wp-content/uploads/2021/12/Freedom_Online_Conference_2021_Chairs_Summary.pdf.

119 Ryan Gallagher, "American Technology Is Used to Censor the Web From Algeria to Uzbekistan," *Bloomberg*, October 8, 2020, https://www.bloomberg.com/news/articles/2020-10-08/sandvine-s-tools-used-for-web-censoring-in-more-than-a-dozen-nations?sref=QmOxnLFz; Arslan Athar, "Unpacking DPI and Its Implications," The News on Sunday (TNS), December 1, 2019, https://www.thenews.com.pk/tns/detail/576187-unpacking-dpi-and-its-implications; Samuel Woodhams and Christine O'Donnell, "The Tech Companies Behind Internet Shutdowns: Allot Ltd."

120 Mahsa Alimardani, "Iran: Tightening the Net 2020 After Blood and Shutdowns," Article 19, September 2020, https://www.article19.org/wp-content/uploads/2020/09/TTN-report-2020.pdf.

121 "Civil Society Letter to Biden Admin Re Russia Sanctions and Internet Access," Access Now, March 10, 2022, https://www.accessnow.org/cms/assets/uploads/2022/03/Civil-society-letter-to-Biden-Admin-re-Russia-sanctions-and-internet-access_10-March-2022-1.pdf.

122 Justin Sherman, "Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior"; and Adrian Shahbaz and Allie Funk, "The Global Drive to Control Big Tech," Freedom on the Net 2021, Freedom House, 2021, https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech.

123 "Continued Presence in Myanmar Not Possible for Telenor," Telenor press release, September 15, 2021, https://www.telenor.com/media/announcement/continued-presence-in-myanmar-not-possible-for-telenor.

124 In a joint public letter, a coalition of advocacy groups described their dismay about Telenor's rapid decision to leave Myanmar and saw no evidence that Telenor had undertaken credible assessments of "potential adverse human rights impacts of disengagement" from Myanmar, required under the United Nations' Guiding Principles. They charged that Telenor's actions appeared to be a "hurried 'disposal' rather than a responsible exit." See Joint Letter to Telenor, Access Now et al., August 12, 2021, https://www.accessnow.org/cms/assets/uploads/2021/08/Letter-to-Telenor_12-August-2021.pdf; and Morgan Meaker, "Myanmar's Fight for Democracy Is Now a Scrap Over Phone Records," *WIRED*, February 8, 2022, https://www.wired.com/story/telenor-myanmar-phone-records.

125 "Privacy Scorecard Report," Unwanted Witness, November 2021, https://www.unwantedwitness.org/wp-content/uploads/2021/11/Privacy-Scorecard-Report-2021.pdf.

126 The organization Ranking Digital Rights provides a useful reporting and disclosure template for telecommunications companies to adopt when ordered to shut down internet access over their networks. See "F10: Network Shutdown (Telecommunications Companies)," in "2020 Ranking Digital Rights Corporate Accountability Index – Governance," Ranking Digital Rights, 2020, https://rankingdigitalrights.org/index2020/indicators/F10.

127 "Form for Assessments and Escalation – Freedom of Expression & Surveillance Privacy 'Unconventional Requests' (Major Events)," Telia Company, March 2020, https://www.teliacompany.com/globalassets/telia-company/documents/sustainability/template-foe-assessments-and-escalation_march2020_withcommentforpublicversion.pdf.

128 For a fuller discussion of options telecoms can pursue to mitigate harms from internet shutdowns, see David Sullivan, "Five Ways Telecommunications Companies Can Fight Internet Shutdowns," Lawfare (blog), August 23, 2020, https://www.lawfareblog.com/five-ways-telecommunications-companies-can-fight-internet-shutdowns.

129 Jeanette Si, "HTTP vs HTTPS: What it Means for Internet Censorship," Berkman Klein Center (blog), July 13, 2017, https://medium.com/berkman-klein-center/http-vs-https-what-it-means-for-internet-censorship-36a3ea4cfe80; and Wikimedia Foundation, "Access to Wikipedia Restored in Turkey After More Than Two and a Half Years," January 15, 2020. https://wikimediafoundation.org/news/2020/01/15/access-to-wikipedia-restored-in-turkey-after-more-than-two-and-a-half-years.

130 Anton Troianovski and Adam Satariano, "Google and Apple, Under Pressure From Russia, Remove Voting App," *New York Times,* September 17, 2021, https://www.nytimes.com/2021/09/17/world/europe/russia-navalny-app-election.html; Upmanyu Trivedi, "India Court Says Twitter in 'Total Non Compliance' of New Rules," Bloomberg, July 28, 2021, https://www.bloomberg.com/news/articles/2021-07-28/india-court-says-twitter-in-total-non-compliance-of-new-rules; and Saheli Roy Choudhury, "India Wants to Cut Big Tech Down to Size. Critics Say the New Rules May Give the State Too Much Power," CNBC, April 20, 2021, https://www.cnbc.com/2021/04/20/indias-social-media-law-puts-big-techs-power-into-states-hands-critics-say.html.

131 Manish Singh, "Twitter Now in Compliance With India's New IT Rules, Government Says," TechCrunch, August 10, 2021, https://techcrunch.com/2021/08/10/twitter-now-in-compliance-with-india-new-it-rules-government-says.

132 Bruce Pannier, "Turkmenistan Increases Crackdown on Internet Access as Living Standards Continue Downward Spiral," Radio Free Europe/Radio Liberty, September 19, 2020, https://www.rferl.org/a/turkmenistan-increases-crackdown-on-internet-access-as-living-standards-continue-downward-spiral/30846977.html; Anastasiya Zhyrmont, "What Turkmenistan Internet Shutdowns Tell Us About Digital Repression in Central Asia," Access Now, December 7, 2021, https://www.accessnow.org/turkmenistan-internet-shutdowns.

133 Navid Hassanpour, *Leading From the Periphery and Network Collective Action* (New York: Cambridge University Press, 2016).

134 Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India," working paper, February 7, 2019, available at https://ssrn.com/abstract=3330413. Of note, Sudan's blocking of social media in 2018–2019 did not eliminate peaceful protests in the country. Rather, as Rydzak, Karanja, and Opiyo observe, "they correlated with a near-disappearance of violence on the part of Sudanese citizens who had filled the streets. The prevalence of nonviolent resistance against a background of partially severed communication channels appears to run counter to the trends identified in India, where shutdowns tended to be followed by escalations in violence." Rydzak et al. conclude that these varying effects illustrate that information disruptions can foster divergent collective action responses. Jan Rydzak, Moses Karanja, and Nicholas Opiyo, "Dissent Does Not Die in Darkness: Network Shutdowns and Collective Action in African Countries," *International Journal of Communication* 14 (2020), https://ijoc.org/index.php/ijoc/article/view/12770.

135 However, Myanmar's strategy still has resulted in substantial economic losses for the country. See "Whitelisted Content Takes Myanmar Back to a 'Dark Age,'" *Frontier Myanmar,* June 30, 2021, https://www.frontiermyanmar.net/en/whitelisted-internet-takes-myanmar-back-to-a-dark-age.

136 "Russia Disconnects From Internet in Tests as It Bolsters Security," Reuters, July 22, 2021, https://www.reuters.com/technology/russia-disconnected-global-internet-tests-rbc-daily-2021-07-22; asl19, "Iran's National Information Network," Citizen Lab, November 9, 2012, https://citizenlab.ca/2012/11/irans-national-information-network.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decision-makers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Democracy, Conflict, and Governance

The Carnegie Democracy, Conflict, and Governance Program rigorously analyzes the global state of democracy, conflict, and governance, the interrelationship among them, and international efforts to strengthen democracy and governance, reduce violence, and stabilize conflict.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org