FRIEDRICH NAUMANN FOUNDATION For Freedom.
Global Innovation Hub

FORUM 2000

INTERNET SHUTDOWNS:

Assessing Their Impact and Effective Countermeasures

HERBERT MBA AKI
HERNÁN ALBERRO
EVAN FIROOZI
XIAO QIANG

POLICY BRIEF

IMPRINT

Editorial team

Forum 2000 Foundation
Pohořelec 6
118 00 Prague 1
Czech Republic

/forum2000.cz
/forum.2000
/Forum_2000

Friedrich Naumann Foundation for Freedom
Global Innovation Hub
15F.-6, No. 171, Songde Road, Xinyi District
Taipei City 110030
Taiwan

/freiheit.org/taiwan
/FNFGIHUB
/FNFGIHUB
/FNFGIHUB

Authors

Herbert Mba Aki, Hernán Alberro, Evan Firoozi, Xiao Qiang

Publisher

Friedrich Naumann Foundation for Freedom Global Innovation Hub

Contact

E-Mail: globalinnovation@freiheit.org

Date

September 2024

Notes on using this publication

This publication is an information offer of the Friedrich Naumann Foundation for Freedom.
It is available free of charge and not intended for sale.
It may not be used by parties or election workers for the purpose of election advertising during election campaigns (federal, state or local government elections, or European Parliament elections).

Disclaimer

The perspectives and opinions stated in this publication are those of the authors, and they do not necessarily reflect the view of Friedrich Naumann Foundation for Freedom.

TABLE OF CONTENTS

INTRODUCTION

Imagine waking up one morning to find that your access to the internet has been completely severed. No news, no messages, social media platforms go dark and no way to contact loved ones. For millions around the world, this scenario has become a reality. Internet shutdowns, employed as a tactic to quell protests, prevent the spread of information, or maintain political control, strip citizens of their fundamental rights to information, expression, and assembly. The use of internet blackouts has sparked global debates on their legality, effectiveness, and long-term repercussions.

This policy brief presents a brief history of how internet shutdowns have evolved and are spreading around the world. Understanding the evolution of internet shutdowns is crucial as they increasingly serve as tools for authoritarian governments and other entities to suppress dissent, control information, and violate human rights. As these tactics become more sophisticated and widespread, particularly during political unrest and elections, knowledge of circumvention methods is vital for ensuring access to essential information, protecting freedom of expression, and enabling communication among communities and activists. This awareness helps safeguard democratic processes, human rights, and the free flow of information.

THE DISCOVERY OF A NEW TOOL OF REPRESSION

Access Now broadly defines an internet shutdown as "an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information." The first widely known blackout happened in 2007 when Guinean President Lansana Conté mandated the shutting down of the fledgling internet industry in a nation where less than 1 percent of the population had access at all. This was his response to protests demanding his resignation. While this first exercise of shutting down the internet had a limited impact on a population with little or no access to it, it undoubtedly introduced other autocrats to a readily available tool for control.

Only two years later, amidst widespread mass protests during the Green Movement, the Iranian government throttled the internet to curb the spread of information and control the crowd during their monthlong protests. Learning from the Islamic Republic, the governments of Bahrain, Egypt, Libya, and Syria later instructed telecommunication companies to shutdown internet access.

In December 2010, the Tunisian Internet Agency directly interfered with web traffic, an escalation of the already common practice of blocking many news websites. A month later, almost at the same time, 3,500 individual Border Gateway Protocol routes – the paths systems use to communicate across the global internet – were withdrawn on orders from the Egyptian government, cutting the country off from the rest of the world and bringing internal communication to a halt.

When the government controls the country's internet service providers, it can order them to deny access by blocking routes to servers. This leads to a total internet shutdown, as all internet access is lost and no one, even those abroad, can reach the servers in that country. Since 2010, internet shutdowns have not only become more common across the world, but have also become more sophisticated.

EFFECTIVE INTERNET SHUTDOWNS
THE LEARNING CURVE (OF AUTHORITARIAN STATES)

The following three cases where the internet has been disrupted illustrate how this strategy of control has evolved and become geographically widespread. The practice of shutting down the internet emerged – as mentioned above – in Africa, and while it has since spread globally, it remains a persistent issue within the region.

In recent years, for instance, in **Gabon**, internet disruptions have been observed twice, both linked to electoral processes. After Ali Bongo, the third president of Gabon from 2009 to 2023, won the contentious 2016 presidential election, there was a surge in the number of demonstrations. These protests led to numerous arrests and involved allegations of extrajudicial killings. The government answered these protests with intermittent disruptions of internet connectivity and a complete shutdown of social media platforms between August 27 and September 14, 2016. Governmental authorities refrained from issuing any formal commentary on this internet disruption.

In 2023, the government took repressions during an election one step further. A mandated internet shutdown occurred on August 26 at 6 p.m., coinciding with the scheduled closure of all polling stations. Unlike the partial disruptions observed in 2016, this shutdown was comprehensive in scope, rendering public television and radio as the sole sources of information. The shutdown lasted four days, during which a military coup ousted the incumbent regime. Throughout this period, the government, via a televised address by its spokesperson, posited it as necessary to prevent the spread of misinformation and false claims about the electoral outcomes. It appears clear that the Gabonese government learned from its experiences of the previous electoral cycle, where opposition supporters utilized social media platforms to disseminate purported voting results, thereby undermining public confidence in the officially announced outcomes and leading to violent unrest. In 2023, it not only imposed a more comprehensive shutdown, but also started it early enough to impede any protests from forming.

Shutting down the internet to repress protest is also popular in **Iran**, which is one of the most repressive regimes in the world. It implemented internet shutdowns at an early stage, exemplifying the learning curve utilizing this tactic. As the government maintains full control of the internet and communication infrastructure, it has been able to jam all digital communications since 2010. Unlike in Gabon, which escalated its shutdown in scale, Iran has refined its shutdowns, evolving from blunt, large-scale disruptions to more targeted and sophisticated measures. During the 2019 protests in Iran, the government ordered a total internet shutdown from November 15 to November 24. This action, imposed by the Ministry of Information and Communication Technology (ICT) under the directive of the Supreme National Security Council, aimed to suppress the widespread "aban-e-khoonin"[1] movement, which originated in Mashhad and spread nationwide. This internet shutdown is described by experts as the most severe disconnection tracked by NetBlocks in terms of technical complexity and scale. It took 24 hours to fully implement.

By contrast, the 2023 Women, Life, Freedom protests in Iran saw a partial internet shutdown. Despite the stoppage, the Iranian National Information Network (NIN) helped maintain essential services within the country. This partial shutdown highlights the government's capability to enact selective control over internet access, showcasing its newfound ability to implement a precise "kill switch" to quell dissent and limit the flow of information. This development underscores the evolving tactics employed by authorities to manage and suppress protests.

A partial shutdown operates similarly to a total blackout but targets specific online services. For instance, one method countries use to implement a partial shutdown is by restricting access to a specific IP address. In some cases, general internet access (that is access to the IP addresses of service providers) remains available, but when attempting to reach a banned IP address (for example, WhatsApp), an error message appears, as if the IP address does not exist. This occurs because the server has blocked that specific address and all associated IPs. In addition, access may be blocked in a specific geographical area, or different groups of people may experience varying levels of internet access. Another type of partial shutdown is when providers or the government throttle the internet speed, making communication nearly impossible.

The last example takes this brief to the other side of the Atlantic: **Cuba**.

On July 11, 2021, a massive wave of demonstrators took to the streets across almost the entire country. These were the largest demonstrations in Cuba since the 1959 revolution, driven by long-standing restrictions on rights, food, and medicine scarcity, as well as the government's response to the COVID-19 pandemic. During the protest, activists trying to share videos and pictures of the demonstrations or the repression on social media found it almost impossible. The government had implemented a partial disruption of social media and messaging platforms, making it difficult for Cubans to inform the outside world about what was happening.

Although this was not the first incident of shutting down the internet in Cuba, it marked the beginning of a trend where partial shutdowns became a common practice. Whenever there is a demonstration or a risk of unrest, the Cuban government shuts down internet access in certain parts of the island or specific internet services such as social media. In addition to these deliberate shutdowns, internet outages in Cuba are also linked to energy blackouts. This phenomenon is not unique to Cuba and was similarly observed in Egypt in 2011. While initially these blackouts are not a deliberate or precise curtailing of access, they often produce the same effect. As energy blackouts become more common, people protest against them, but since internet access is also affected, they cannot effectively organize their demonstrations to confront the government and push for policy or regime change.

The cases of Iran, Gabon, and Cuba illustrate the extent to which authoritarian regimes fear public demonstrations. Data from a Surfshark report reveals that, in 2023, protests were the primary trigger for internet shutdowns.

The presented cases show that internet shutdowns have evolved significantly over time, becoming more targeted, sophisticated, and widespread as governments have refined their control methods.

[1] Bloody Aban aka Bloody November

ACCESS DENIED 24/7

Probably the most sophisticated system of curtailing internet access was developed by the **People's Republic of China**. The arrival of the internet seemed to bring with itself an era of free access to information. So too, many hoped, in China. In 2000, then-US President Bill Clinton compared China's efforts at online censorship to "trying to nail Jello to the wall". The Great Firewall (GFW) has done exactly this. With it, the government has implemented tools to limit the flow of information into and out of the country, blocking transmissions that do not meet government criteria and shielding users from information deemed counter to the Chinese Communist Party's (CCP) interests. The GFW, officially known as the "State Data Cross-Border Security Gateway", refers to the collection of institutions and technology (hardware and software) employed by the Chinese government to monitor and filter content on international gateways. It is the primary national censorship apparatus of the People's Republic of China (PRC) and is directly overseen by the Cyberspace Administration of China (CAC). This tool restricts Chinese internet users' access to foreign information sources and services like Google Search, Facebook, X, Netflix, Instagram, the BBC, and Wikipedia. It also actively blocks tools that attempt to circumvent its censorship.

The GFW is deployed at various international internet gateways across mainland China, including supercomputers, ordinary servers, routers, and related applications. Its content filtering and analysis are bidirectional, not only interfering with domestic users accessing foreign websites but also disrupting foreign users accessing websites in mainland China. The main blocking techniques include, but are not limited to, Transmission Control Protocol (TCP) connection resets, IP blocking, DNS poisoning, specific port blocking, SSL connection interruptions, Man-In-The-Middle (MITM) attacks, and traffic pattern recognition. Since the operation of the GFW depends on the backbone network's international gateways, this also causes frequent congestion at China's international gateway nodes. While the GFW might not appear to be a classic example of an internet shutdown and there is a debate on whether it classifies as such, it fulfills the broad criteria set by Access Now. In essence, the GFW acts as a national-level system that manipulates root nodes and conducts partial internet shutdowns for internet users within China. The sophistication of the Great Firewall is key to understanding potential escalations to temporary partial shutdowns and showcases the long term harm that such control over the internet and its rules has over the free flow of information.

MITIGATING INTERNET SHUTDOWNS

LESSONS FROM IRAN

That governments routinely resort to shutting off the internet shows the threat that the free flow of information and the possibility to connect online pose to authoritarian regimes. To navigate internet shutdowns and ensure that the flow of information remains intact, empowering activists worldwide and making sure that access can be regained requires innovative strategies. Various approaches, from technological solutions to proactive training initiatives, are vital to supporting democratic movements and upholding freedom of expression. This policy brief highlights three approaches that can be observed in Iran.

One way to circumvent internet shutdowns in Iran has been the use of Starlink satellites. These, however, require the use of terminals in-country which had to be smuggled into the country. The aim was to provide a tool for demonstrators in Iran to maintain access to the internet to send information abroad and also to be connected to each other and be able to organize themselves. This circumvention of the government's shutdown, however, did not sit well with the Iranian government. Arguing its case in front of the International Telecommunication Union (ITU)[2] in Geneva, Iran successfully claimed that "the network violates the UN agency's rules prohibiting use of telecommunications services not authorized by national governments". Iran's use of the ITU to curb Starlink exemplifies the geopolitical challenges of internet regulation. The ITU's rulings favoring Iran show the global impact of such disputes, posing risks to the international community's access to satellite internet services. This case highlights the need for robust regulatory frameworks and diplomatic engagement to address conflicts arising from emerging technologies.

[2] The United Nations' specialized agency for information and communication technologies. See: https://council.itu.int/2023/en/about-itu/

Another way of maintaining access to information during shutdowns is satellite broadcasting. Projects like Toosheh (Knapsack for Hope), which operates in Iran and Afghanistan, are examples of highly effective and accessible solutions during internet shutdowns. Toosheh and similar initiatives leverage satellite networks to deliver free data to end users, bypassing traditional internet infrastructure and government-imposed restrictions. This approach ensures widespread access to crucial information, as users only need a simple dish antenna and a satellite receiver to receive broadcasts without internet connectivity. Additionally, satellite broadcasting provides complete privacy and anonymity for users, making it virtually impossible to determine who has received the transmitted data. By repurposing older technologies like satellite broadcasting in innovative ways, projects like Toosheh demonstrate the potential to connect communities worldwide, even in regions facing significant challenges to internet access. Proof of how good these technologies are: the number of Instagram users in Iran is estimated to be more than 47 million, 55% penetration, one of the biggest shares in the Middle East even though Instagram is restricted in the country.

Another approach to circumventing internet restrictions involves peer-to-peer (P2P) services, which offer decentralized communication channels that enable individuals to share information despite government-imposed restrictions. This service empowers activists and civil society organizations to exchange messages and coordinate actions independently of centralized platforms. Training programs focused on digital literacy, cybersecurity awareness, and circumvention techniques – such as those promoted by projects such as Toosheh, play a critical role and ensure that communities are prepared to utilize technologies like satellite broadcasting and P2P services, even in the absence of traditional internet access.

Lastly, many activists in Iran keep multiple circumvention tools on their devices. The reasoning behind this is that different internet service providers (ISPs) may block certain tools while others remain operational, making it essential to have a range of options at hand. This approach allows activists to quickly switch between tools depending on which one is currently effective, maximizing their chances of bypassing government restrictions. By diversifying their circumvention methods, citizens are able to stay connected, even under the most stringent censorship conditions, ensuring that they can continue their work in advocating for change and disseminating critical information. This flexibility not only enhances their digital resilience but also demonstrates the constant innovation required to navigate an ever-evolving landscape of digital repression.

POLICY RECOMMENDATIONS

To address and mitigate the impact of internet restrictions and shutdowns, a diversified approach is essential. This section outlines key policy recommendations to mitigate the risk stemming from internet shutdowns.

Research and development of new tools

Democratic governments and tech companies should foster the research and development of new tools that can facilitate access to technology to enable communication and internet access in various sectors. These tools should not only empower individuals but also ensure equal opportunities. By developing tools that function even with limited internet access, civic activists will be better equipped to counteract or circumvent internet shutdowns.

Study the authoritarian information control toolbox

Further research is warranted to understand how the GFW and other apparatuses adopted by authoritarian governments control the flow of information. Research in this area should focus on how these technologies facilitate partial shutdowns and limit citizens' access to certain online information sources. Initiatives such as the Open Observatory of Network Interference (Ooni) and NetBlocks, which track and document internet interruptions, have been crucial to combating internet shutdowns and learning their models.

Technological exchange and training

Education and preparedness initiatives are essential for equipping communities to navigate internet shutdowns effectively. Both democratic governments and civil society organizations should provide technology and training to individuals and organizations in countries affected by internet shutdowns, enabling them to safely access and share information. Activists should be trained to prepare for both total internet shutdowns and focused shutdowns of specific apps. Having multiple messaging apps to rely on in case one is not working should be essential to any democracy activist, along with having a trustworthy contact abroad who can post on social media in case they are blocked inside their country. For instance, in Iran, most activists have several circumvention tools on their devices because each tool might work on a specific internet service provider. This has proved to be an effective method of combating severe censorship.

Education and awareness programs

Civil society actors should launch campaigns that educate the public about the importance of internet freedom. As democracy activists, in particular, and civil society, in general, access more courses on different digital tools to circumvent internet shutdowns, it will become more difficult for authoritarian governments to control the free flow of information. Many years of technology development and public work through satellite TV channels, social media, online courses, and the thirst for free information has allowed Iranians to access their favorite services online, even at the cost of a colossal speed reduction.

Strengthen international standards

International organizations such as the ITU are responsible for "facilitating international connectivity in communication networks and allocating global radio spectrum and satellite orbits, developing the technical standards that ensure networks and technologies connect seamlessly, and working to improve access to digital technologies in underserved communities worldwide". The decision the ITU makes and who leads it, is therefore paramount in safeguarding access to the internet worldwide. While it is at the moment headed by Doreen Bogdan-Martin from the US, democratic governments and civil society must be vigilant in the leadership election process. If the ITU were to be headed by representatives of authoritarian governments it could jeopardize the standards that guarantee the free flow of information. Democratic governments should use international organizations such as the ITU to advocate for sanctions against countries that engage in severe internet shutdowns and include internet freedom as a core topic in diplomatic dialogues, promoting global standards for an open and free internet.

AUTHORS

Herbert Mba Aki

Herbert Mba Aki is Assistant Professor of Political Science at the Université Omar Bongo in Gabon and Vice President of Biangg Consulting. He served as Coordinator of the Young Scholars Initiative Africa Working Group (2020-2023). Herbert is a member of Democratic Solidarity Africa with Forum 2000 Foundation.

Hernán Alberro

Hernán Alberro is Associate Fellow at Forum 2000 Foundation. He holds a BA in Journalism and graduated from a Masters in Public Policy. He is member of the International Coalition for Democratic Renewal (ICDR) and Democratic Solidarity Latin America with Forum 2000 Foundation.

Evan Firoozi

Evan Firoozi is Executive Director of NetFreedom Pioneers, leading the organization’s mission to empower individuals to exercise their digital rights and liberties. In Iran he served as a journalist and human rights activist. He was arrested several times by the Iranian government and was imprisoned in the notorious Evin prison.

Xiao Qiang

Xiao Qiang is a Research Scientist at the UC Berkeley School of Information and the Founder and Editor-in-Chief of China Digital Times, a bi-lingual China news website. He is member of the International Coalition for Democratic Renewal (ICDR) with Forum 2000 Foundation.

FORUM
2000

freiheit.org