International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

Volume 10, Issue 7, May-June-2024 | Published Online : 20th June 2024

The Digital Darkness : Exploring Global Internet Shutdowns

K Kalaiarasan

Assistant Professor, Department of Information Technology, M. Kumarasamy College of Engineering, India

ABSTRACT

Global internet shutdowns have raised critical concerns about digital rights, governance, and information suppression. This research examines the causes, consequences, and societal implications of these events, shedding light on government methods to control online communication. It explores the interplay between policies, regulations, and human rights, unraveling legal frameworks facilitating shutdowns. The study scrutinizes social and political contexts, revealing connections to unrest, protests, elections, and dissent suppression. Consequences on civic participation, activism, and political movements are analyzed. Economic ramifications are investigated, highlighting costs on businesses, trade, employment, and digital economies, affecting innovation and investment. Technical aspects unravel methods used for control and monitoring, assessing circumvention feasibility. International responses and advocacy efforts are evaluated, offering insights and strategies for safeguarding internet freedom and promoting universal access. This research aims to deepen understanding, inspire dialogue, inform policies, and advocate for internet access as a fundamental right. The advent of the internet and the World Wide Web (www) has played a pivotal role in reshaping development across various sectors. The internet has found extensive use in education, business, healthcare, banking, media, and more, surpassing traditional modes of mass communication. Media, in particular, serves as a rapid medium to reach a wide audience. Modern communication methods have undergone a transformation, facilitated by the internet, enabling us to connect and engage with a vast audience. The internet has facilitated innovative modes of interaction between governments and citizens, empowering individuals to engage with the state and express.

I. INTRODUCTION

Global internet shutdowns have raised critical concerns about digital rights, governance, and information suppression. This research examines the causes, consequences, and societal implications of these events, shedding light on government methods to control online communication. It explores the interplay between policies, regulations, and human rights, unraveling legal frameworks facilitating shutdowns. The study scrutinizes social and political contexts, revealing connections to unrest, protests, elections, and dissent suppression. Consequences on civic participation, activism, and political movements are analyzed. Economic ramifications are investigated, highlighting costs on businesses, trade, employment, and digital economies, affecting innovation and investment. Technical aspects unravel methods used for control and monitoring, assessing circumvention feasibility. International responses and advocacy efforts are evaluated, offering insights and strategies for safeguarding internet freedom and promoting

universal access. This research aims to deepen understanding, inspire dialogue, inform policies, and advocate for internet access as a fundamental right. The advent of the internet and the World Wide Web (www) has played a pivotal role in reshaping development across various sectors. The internet has found extensive use in education, business, healthcare, banking, media, and more, surpassing traditional modes of mass communication. Media, in particular, serves as a rapid medium to reach a wide audience. Modern communication methods have undergone a transformation, facilitated by the internet, enabling us to connect and engage with a vast audience. The internet has facilitated innovative modes of interaction between their views. Many people now find it easier to communicate with the government and express their views thanks to the advent of the internet and digital media channels [1]. An internet closure is a complete limitation on the use of internet services imposed by a governing body's decision. This restriction can be limited to a specific geographical area and have a set duration, such as a time period or number of days. In other situations, the closure may be indefinite. An internet shutdown can affect only mobile internet services on cell phones, wired broadband connections generally used by desktops, or both [2]. When the infrastructure for communication, such as cellular or online networks, is purposely destroyed or degraded, network disconnections occur. These disturbances cause services such as phone calls, text messaging, and internet-enabled applications, including social media platforms, to be disrupted. Network outages can be caused by both technical faults and legal actions taken by authorities [3]. Whenever an internet shutdown occurs, authorities in that particular region often cite various reasons, including the spread of fake news. Internet shutdowns are also implemented to control the flow of news and current affairs, particularly in sensitive areas, with the aim of preventing information dissemination among the general public. The justifications provided for restricting internet access vary, with differing degrees of validity and justification [4]. Internet shutdowns can be seen as a form of online censorship that has evolved through different generations of control, involving filtering systems, legal and technical capabilities, counter-information tactics, and contested access [5]. Restricting access and discrediting specific content or citizen journalists aims to reshape and control the public sphere [6]. There is a range of opinions that have been published on the effects of the internet on society as a whole, therefore it cannot be easily divided into cyber optimists and cyber pessimists. While some gravitate towards optimistic or pessimistic views, there is a growing body of literature that explores the complexities and nuances of the internet's proliferation. Cyber-realists take a more balanced approach, transcending the binary positions of optimists and pessimists. The internet has both empowering and disempowering possibilities, with debates focusing on its transformative impact, alternative media platforms, and negative aspects such as hate speech and fake news. The internet, like media in general, possesses power and potential risks that individuals must navigate [7-11]. Internet shutdowns have become a favored tool for authoritarian governments, particularly since the global protests sparked by the Arab Spring and the Spanish Indignados movements. The concept of a "kill switch," exemplified by its implementation in Egypt during the protests in 2011, backfired and instead mobilized a larger mass of people to take to the streets. This trend extends beyond Africa, with governments in Asia, Europe, and South America also resorting to internet shutdowns to demobilize protesters and citizens. These shutdowns are frequently used to stifle dissent and restrict freedom of assembly during crucial events such as voting, protests, terror attacks, or national catastrophes. Excessive interruptions infringe human rights, including the freedom of communication, access to data, and engagement with politics. Downtime is justified for a variety of reasons, including defending state institutions and leaders, monitoring propaganda, and ensuring national security [12-14].

In recent years, the world has witnessed a concerning rise in the frequency and scale of internet shutdowns. These deliberate disruptions, often imposed by governments or other authorities, have significant implications for communication, access to information, human rights, and the global digital landscape. This news and views provide an in-depth overview of the latest news and views surrounding global internet shutdowns, shedding light on the impact, reasons, controversies, and potential solutions to this growing phenomenon. Despite widespread condemnation and the clear violation of human rights, governments worldwide persist in implementing internet shutdowns, even during critical national moments. These concerning trends have been extensively documented by Access Now and the global coalition, and they continue to be prevalent in 2023. Since the beginning of the year, a minimum of 80 shutdowns has been identified across 21 countries, with 18 of them ongoing since 2022. In May, notable shutdowns occurred, including a blanket shutdown in Manipur, India, the nationwide blocking of 14 messaging applications in India, and the blocking of social media platforms to suppress protesters in Guinea. As the on community diligently identifies and verifies additional shutdowns, it is expected that the figures will further rise, underscoring the alarming surge in global internet shutdowns. Figure 1 presents the most up-to-date data available at the time of this update, encompassing information from the 2022 report on internet shutdowns. The data for 2023 includes the initial identification of shutdowns between January 1 and May 19, 2023 [15]. In Figure 2, the focus is on illustrating the impact of internet shutdowns in Ukraine, specifically those imposed by Russian forces. The figure highlights the disruptive nature of these shutdowns and emphasizes their significance within the context of the ongoing conflict.

Persistent Offenders Escalate their Actions: As the unlawful full-scale invasion of Ukraine by Russia persists, the military continues to target both the internet and crucial civilian infrastructure as part of its offensive tactics. Purposeful airstrikes in various regions, such as Odessa, Kharkiv, Zhytomyr, and Luhansk, are deliberately disrupting internet access, exacerbating uncertainty and deepening the hardships faced by the Ukrainian people. Despite hopes for a counteroffensive to bring an end to the conflict and the remarkable resilience displayed by Ukrainians in rebuilding infrastructure and restoring connectivity, there is no indication that the Russian military will decrease the frequency of imposed shutdowns since February 2022. Despite a peace agreement in Tigray, Ethiopia, the government has failed to fully restore internet access, prolonging an over two-and-a-half-year-long shutdown in a region already devastated by civil war. Furthermore, the government has imposed additional shutdowns in various parts of the country. These include long-lasting nationwide social media blocks and a mobile shutdown in the Amhara region in early April. There have also been reports, yet to be verified, of sporadic shutdowns in the Oromia region. According to our documentation in the STOP database, the government of Ethiopia has enforced at least 24 shutdowns since 2016, the highest count in Africa. The arbitrary and frequent use of shutdowns in response to significant national crises is highly detrimental and unacceptable. We urge the authorities to restore access to communication platforms throughout Ethiopia and prioritize the full reestablishment of connectivity in Tigray and all other affected regions. Iran, identified as one of the major perpetrators of internet shutdowns in 2022, began the year by implementing a shutdown specifically for school exams on January 19. However, this approach has proven ineffective in curbing cheating, addressing corruption, or addressing exam leaks. Furthermore, Iranian authorities persist in cracking down on the protest movement present across the country, targeting various cities and regions. Internet shutdowns have become a common tool in this crackdown, aimed at silencing dissenting voices and concealing continues to enforce shutdowns in regions facing armed resistance, with new

disconnections observed in multiple townships in Chin State in January, in addition to existing long-term shutdowns across the country. To compound the situation, Cyclone Mocha struck western Myanmar in May, exacerbating the impact of the deadly storm due to the near-total lack of connectivity. People who were already deliberately disconnected were unable to receive proper storm warnings, participate in evacuation efforts, and access post-disaster relief assistance.

Restricting internet accessibility can be viewed as a limitation on the freedom of expression, as the internet is a platform for free speech. Internet shutdowns not only impact various sectors within a region but also hinder atrocities. In the province of Sistan and Baluchestan, particularly in the capital city of Zahedan, weekly protests during Friday prayers have been repeatedly met with deliberate and prolonged internet shutdowns, lasting for months. These shutdown measures replicate the pattern observed in the previous year when authorities imposed regular curfew-style shutdowns to suppress protests. According to the Software Freedom Law Center, India, as of May 19, a total of 33 shutdowns have been imposed in 13 states across India in 2023. While some of these shutdowns are enacted locally or even at the neighbourhood level in response to religious anniversaries, protests, and communal violence, authorities have also implemented wide-scale state-wide shutdowns and extended shutdowns throughout the entire country. Notably, during exams in Rajasthan, a state- wide police search in Punjab, and widespread protests in Manipur, the internet was completely suspended for periods ranging from days to weeks, resulting in the disconnection of tens of millions of people.
Disaster response efforts are impeded by internet shutdowns:

As a result of brutal crackdowns by the military junta, millions of people in Myanmar have been without internet access for over a year. Our partners have reported that all 330 townships in Myanmar experienced internet shutdowns at least once in 2022. The military

economic growth. They are detrimental to both inter and intra-societal communication. The media sector, which plays a crucial role in a developing country like India, is severely constrained by such shutdowns. It is essential to prioritize the right to information and communication for all individuals, avoiding blackout situations as much as possible. Media should be granted unrestricted access to fulfil their vital role in delivering information to the general public.

In the aftermath of the devastating M7.8 earthquake in Turkey in February, Turkish authorities deliberately restricted access to Twitter, ostensibly to suppress growing criticism of the country's response to the crisis. This throttling of internet access severely impeded humanitarian coordination efforts, impeding rescue operations and the delivery of aid. Following widespread condemnation, authorities eventually restored full-speed access to Twitter, which had been non-functional for a continuous period of 12 hours on February 8. The impact of the access throttling was particularly severe considering that the earthquake had occurred just two days earlier, with thousands still trapped in rubble and ongoing aftershocks causing additional building collapses. Unfortunately, this incident was not the first time Turkish authorities had imposed social media shutdowns following a disaster. Similar measures were implemented after a tragic and deadly explosion in Istanbul the previous year. This pattern of cutting off communication channels during times of danger is a deeply concerning trend, compounded by the passage of a disinformation bill in October 2022 that expanded the government's censorship powers, enabling consistent restrictions on the flow of information precisely when people need it most.

Internet shutdowns for fugitive capture or protest suppression result in a total information blackout for the population.

In 2023, law enforcement agencies and government leaders have increasingly resorted to imposing widespread and prolonged network disruptions during the apprehension and incarceration of high-profile suspects. For instance, in March, authorities in Mauritania enforced a six-day mobile internet shutdown following the escape of four prisoners from a prison. This response was widely criticized as disproportionate, ineffective, and excessively harsh. Similarly, in Punjab, India, authorities implemented a lengthy, multi-phase shutdown across the state in March during a police operation aimed at locating an alleged separatist leader. In response to the protests sparked by the arrest of former Prime Minister Imran Khan, Pakistani authorities implemented punitive shutdowns that had significant repercussions. The Pakistan Telecommunication Authority (PTA) issued an order to indefinitely suspend internet services, resulting in a complete three- day shutdown across four mobile providers starting from May 10. Access to popular social media networks such as Facebook, Instagram, Twitter, and YouTube were also restricted for a week. These disruptive measures reflect the growing trend worldwide of combining regionally targeted mobile shutdowns with layered social media blocks.

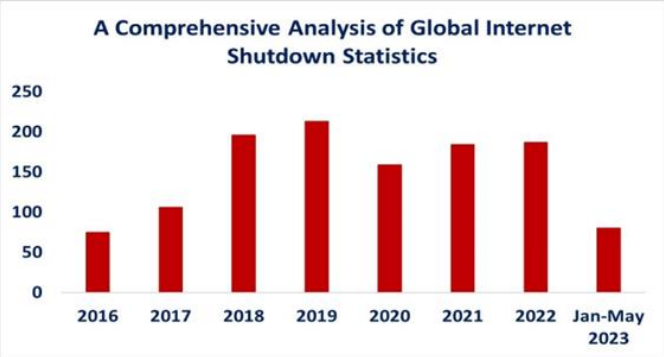

Fig. 1. Revealing the Data: A Thorough Examination of Statistics on Global Internet Shutdowns[15].

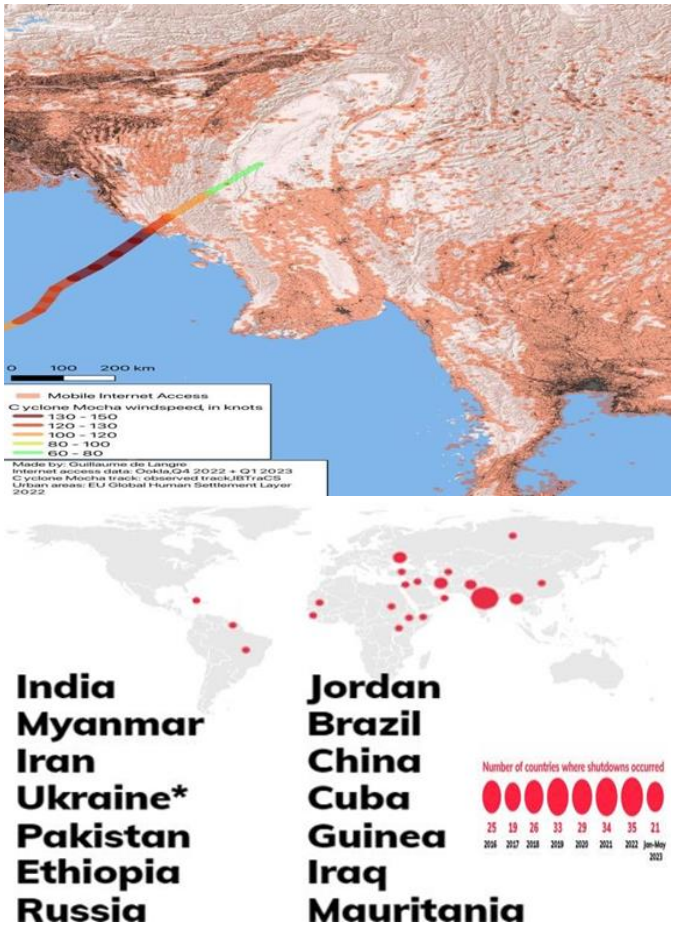

Fig. 2. Global Impact: Countries Affected by Internet Shutdowns, Including Ukraine under Russian Forces (Jan-May 2023) [15].

Democracies pursue expanded censorship authority.

In the early months of 2023, we continue to witness concerning trends where countries with well-established democratic institutions are increasingly resorting to censorship and shutdown measures. In Brazil, for instance, a court order resulted in the blocking of Telegram across multiple internet service providers (ISPs) from April 26 to April 30. The order was issued due to alleged non- compliance by the company in providing information about participants in hate group chat rooms to the police. Brazilian courts have frequently relied on contempt orders to shut down social media applications in the past. Similarly, in the United States, the state of Montana implemented

an outright ban on TikTok amid escalating geopolitical tensions between China and the U.S. concerning data protection, surveillance, and national security. However, such bans tend to overlook the larger issue at hand: the pressing need for robust data protection laws and surveillance reforms to safeguard privacy and security for everyone. Imposing platform blocks not only undermines the credibility of governments that otherwise denounce internet shutdowns but also fails to address the root problems effectively. Armenian authorities previously blocked TikTok in September 2022, and there are indications that they may be responsible for the blocking of Facebook, Instagram, and WhatsApp in the Nagorno-Karabakh region on May 18, 2023, during the context of the conflict with Azerbaijan. The alarming aspect is that the Armenian government is seeking legal authority to enforce shutdowns during periods of military conflict. Regardless of the ongoing peace talks and whether a ceasefire would halt the shutdowns, Armenia must take stronger measures to protect people's internet access and freedom of expression.

The Scope of the Problem: Highlighting the scale and severity of internet shutdowns worldwide, this section explores the regions and countries most affected by these disruptions. It delves into the economic, social, and political ramifications of such shutdowns, illustrating their detrimental effects on businesses, education, healthcare, civil liberties, and democratic processes.

Causes and Triggers: Examining the factors that lead to internet shutdowns, this section uncovers the motivations behind governments' decisions to restrict or cut off internet access. It discusses various triggers, including political unrest, social movements, national security concerns, misinformation, and even attempts at controlling public narratives. Case studies offer insights into specific incidents and shed light on the reasoning behind these actions.

Human Rights Implications: Internet shutdowns frequently violate fundamental human rights, such as freedom of expression, access to information, and the right to assemble peacefully. This section explores the legal and ethical dimensions of these disruptions, examining how shutdowns affect journalists, activists, marginalized communities, and individuals dependent on the internet for their livelihoods.

Technological and Economic Consequences: Internet shutdowns pose significant challenges to technology companies, internet service providers, and digital infrastructure. This section analyses the economic repercussions, including financial losses, stifled innovation, and reduced investment, while also exploring technical aspects such as network manipulation and censorship techniques employed during shutdowns.

International Response and Advocacy: Focusing on the global response to internet shutdowns, this section explores the efforts of international organizations, civil society groups, and activists to address the issue. It highlights initiatives promoting internet freedom, policy advocacy, and the role of digital rights organizations in raising awareness, lobbying for change, and supporting affected communities.

Mitigation and Solutions: Concluding the overview, this section delves into potential solutions to combat and mitigate the impact of internet shutdowns. It explores technical tools, circumvention strategies, policy frameworks, and international collaborations aimed at preserving internet access as a fundamental human right and safeguarding against unwarranted disruptions.

The rise of internet shutdowns poses a serious threat to the free flow of information, civil liberties, and global digital progress. By examining the latest news, discussing viewpoints, and highlighting potential solutions, this article aims to raise awareness about this concerning trend and inspire action to protect internet access, human rights, and the future of the connected world.

Conflict of interest

The authors declare that they have no conflict of interest.

Acknowledgement

The authors are grateful to the anonymous reviewers for their constructive and valuable review comments and helped us to improve the research publication.

II. REFERENCES

[1]. Mare, A. (2016). —Facebook, Youth and Political Action: A Comparative Study of Zimbabwe and South Africa PhD diss., Rhodes University.

[2]. Srivastava, R. (Digital Empowerment Foundation) (2016), Anatomy of Virtual Curfews: Human Rights vs. National Security.

[3]. Dancey-Downs, K, We Need to Talk about Internet Shutdowns, Lush.

[4]. Kaye, D. (UN Special Rapporteur on Freedom of Expression) (2016), Freedom of Expression and the Private Sector in the Digital Age –Annual Report to the Human Rights Council.

[5]. Mare, A. (2018). Politics unusual? Facebook and Political Campaigning during the 2013 harmonised elections in Zimbabwe. African Journalism Studies. 38(2): 1–22.

[6]. Wagner, B. (2018). Understanding Internet Shutdowns: A Case Study from Pakistan. International Journal of Communication.12: 3917–3938.

[7]. Castells, M. (2010). The Rise of the Network Society, Second Edition (with a new preface). London: Wiley- Blackwell.

[8]. Morozov, E. (2011). The net delusion: The dark side of internet freedom. New York: Public Affairs.

[9]. Aouragh, M. (2013). Social Media as Damocles Sword: The Internet for Arab Activists. Unlike Us #3. Retrieved on the 4th of April 2019.

[10]. Lim, M. (2018). Roots, Routes, and Routers: Communications and Media of Contemporary Social Movements. Journalism and Communication monographs. 20(2): 92-136.

[11]. Mare, A. (2016). —Facebook, Youth and Political Action: A Comparative Study of Zimbabwe and South Africa. PhD diss., Rhodes University.

[12]. Curran, J. (2002). Mass media and democracy. In Curran, J. and Gurevitch, M. (2002). Mass media and society. New York: Edward Arnold. [20] Gerbaudo, P. (2013). The 'Kill Switch' as 'Suicide Switch': Mobilising Side Effects of

[13]. Mubarak's Communication Blackout. Westminster Papers in Communication and Culture, 9(2): 25-43.

[14]. AFEX. (2018). Constricting Freedom of Expression Online: Annual Report on the State of Internet Freedom in Africa 2017 report, Accra: AFEX.

[15]. https://www.accessnow.org/publication/internet-shutdowns-in-2023-mid-year-update/#disaster-response.

Author

K. Kalaiarasan, an exceptionally accomplished assistant professor in the Department Information Technology department at M Kumarasamy College of Engineering, exudes a remarkable depth of knowledge and expertise. Having obtained a postgraduate degree in Computer Science and Engineering from Sethu Institute of Technology, he brings a wealth of invaluable insights to his role. His unwavering dedication to groundbreaking research in website development, application development, robotics, blockchain, and data analysis has garnered widespread acclaim, positioning him as a visionary and inventive researcher at the forefront of his field.