Journal of Theoretical and Applied Information Technology
29th February 2024. Vol.102. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TECHNICAL ANALYSIS OF INTERNET SHUTDOWNS: ECONOMIC AND CYBERSECURITY DIMENSIONS IN INDIA AND INTERNATIONAL CONTEXT

HARISH CHOWDHARY[1], DR NAVEEN KUMAR CHAUDHARY[2]

FARAJ ABDULLAH HAZZA HARAHSHEH[3], MOHAMMED AHMED MUSTAFA[4]

DR MANINDRA RAJAK[5], RAJ KUMAR TOMAR[6]

[1]School of Doctoral Studies & Research, National Forensic Sciences University, Gandhinagar, Gujarat, India.
[2]School of Cyber Security and Digital Forensics, National Forensic Sciences University, Gandhinagar, Gujarat, India.
[3]Faculty of Business, Department of Business Administration, Isra University, Jordan
[4]Department of Medical Laboratory Technology, University of Imam Jaafar AL-Sadiq
[5]GITAM (Deemed to be University), India
[6]GNIOT- MBA Institute, Greater Noida, India
E-mail: [1]intern3tgovernance@gmail.com, [2]naveen.chaudhary@nfsu.ac.in, [3]faraj1harahsheh@iu.edu.jo, [4]mohammed.ahmed.mustafa1@sadiq.edu.iq, [5]mrajak@gitam.edu, [6]rktomar.mba@gmail.com

ABSTRACT

This article delves into the multifaceted repercussions of internet shutdowns, with a specific lens on their economic and cybersecurity implications in India and globally. The concept of internet shutdowns is explored as intentional disruptions of internet and mobile services by authorities, marked by varying degrees of scope and severity. The research underscores the profound impact of these shutdowns, particularly in regions where mobile-based internet access predominates, and broadband is less accessible. The paper includes an exhaustive literature review, encompassing the themes of digital authoritarianism, control over information flow, and the relationship between state authority, cyber power, and public dissent. It extends the discourse to the realm of cybersecurity, highlighting its critical role in sectors such as healthcare, education, and public policy. The paper also emphasizes the importance of incorporating cybersecurity policy and the development of organizational cybersecurity capabilities. Methodologically, the paper outlines a rigorous approach to standardizing diverse datasets on internet shutdowns from 2016 to 2022, utilizing data from the KeepItOn Shutdown Tracker Optimization Project. This process entails data acquisition, harmonization, and cleaning, resulting in a comprehensive, analyzable dataset. The empirical core of the study quantifies the economic impacts of internet shutdowns through an analysis of shutdown durations and their correlated economic consequences. A novel economic impact per hour calculation is presented, alongside annual economic impact estimations for India from 2016 to 2022. The paper also contemplates employing regression analysis for more nuanced economic impact projections. Concluding with cybersecurity considerations, the paper examines how internet shutdowns foster environments conducive to cyber threats and vulnerabilities. The study calls for robust strategies to mitigate these impacts, underscoring the criticality of understanding and addressing the broad spectrum of effects engendered by internet shutdowns.

Keywords: *Internet Shutdowns, Cybersecurity, Economic Impact, Internet Governance, Data, Standardization, Digital Safety, Policy Analysis, India.*

1. INTRODUCTION

An internet shut down, refers to measures taken by governments or other authorities that disrupt internet access or mobile applications. These measures are aimed at controlling what people can access, see, or share online. Internet shutdowns can vary in their scope and intensity. Internet shutdowns can impact an entire country or a specific region, usually targeting particular types

of internet access, such as mobile networks. Sometimes, these shutdowns also involve restricting access to virtual private networks (VPNs), making it harder to bypass these restrictions. In extreme cases, the measures might escalate to disabling entire telephone networks, effectively cutting off all forms of direct electronic communication. The impact of such shutdowns is more pronounced in countries where internet access is primarily through mobile devices and broadband internet is only affordable for the affluent, potentially leading to a complete internet blackout for the majority of the population [1].

Internet Shutdowns have become a prevalent and concerning issue in various regions of the world, with significant implications for economic stability and cybersecurity. The deliberate disruption of internet services, whether partial or complete, has far-reaching consequences that extend beyond the digital realm, impacting various facets of society. This article seeks to delve into the multifaceted implications of internet shutdowns, particularly focusing on the economic and cybersecurity dimensions in India and beyond. The phenomenon of internet shutdowns presents unanticipated and unintended consequences, as actions by governments and mobile network operators (MNOs) to curtail internet access can have profound effects on various sectors. The economic implications of internet shutdowns are particularly noteworthy, as they disrupt the normal functioning of businesses, financial transactions, and digital services.

Furthermore, the cybersecurity vulnerabilities that arise during internet shutdowns create an environment where cybercriminals and malicious actors thrive, posing significant risks to personal data, financial systems, and national security. This article aims to provide a comprehensive analysis of the economic and cybersecurity implications of internet shutdowns, drawing on empirical evidence and case studies from India and other regions. By quantifying the economic costs and assessing the cybersecurity risks associated with internet shutdowns, this research seeks to shed light on the far-reaching impact of these disruptions. Additionally, the article will explore the broader implications of internet shutdowns, considering the perspectives of various stakeholders, including educators, healthcare professionals, and policymakers. The findings of this research are expected to contribute to a deeper understanding of the consequences of internet shutdowns, providing valuable insights for policymakers, businesses, and individuals. By quantifying the economic and cybersecurity implications, this article aims to underscore the urgency of addressing internet shutdowns and implementing measures to mitigate their impact on economies and cybersecurity infrastructure. As the digital landscape continues to evolve, understanding the true cost imposed by internet shutdowns is crucial for safeguarding economic stability and cybersecurity in India.

2. LITERATURE REVIEW

Internet shutdowns have become a growing phenomenon globally, with contemporary literature revealing the consequences and impact of such shutdowns on various aspects of society [2]. The sustained internet shutdowns in recent years have been described as forms of 'digital siege,' where authorities seek to 'wear down public dissent under the guise of pacifying volatile situations' [3]. The existing literature on internet shutdowns examines the consequences of implementing a shutdown and why authorities issue such orders [4]. An internet shutdown is considered the ultimate form of control over the flow of information via the internet [5]. Furthermore, the interaction between people, state, and cyber power in the internet shutdown policy paints a dynamic picture involving repression, delegations of cyber power, and the future where countries are heading into a paradox where they exist as democratic countries under digital authoritarianism regimes [6].

In the context of cybersecurity, the relationship between risky cybersecurity behaviors, attitudes towards cybersecurity, and internet addiction has been explored [7]. Additionally, the significance of introducing cybersecurity measures in orientation and training events for new employees has been emphasized to develop their self-awareness in cybersecurity topics such as handling personal health information, using email systems securely, and surfing the internet safely [8]. Moreover, the incorporation of gender considerations throughout international cybersecurity policy and practice has been proposed to ensure that cybersecurity improves the security of people of all gender identities and expressions, as well as international peace and security [9].

In the healthcare sector, there is a need to analyze the literature on cyber risk to understand the real knowledge on this topic and propose frameworks for cybersecurity awareness to prevent exploitation in cybercrime, especially among the elderly [10, 11]. The increasing reliance on

technology in healthcare has created new risks, and healthcare has not been immune to the cybersecurity considerations plaguing other industries [12] .Furthermore, there is a need to address cybersecurity and privacy risks in different threat scenarios to support decision-making and compliance considerations in healthcare [13].

In the field of education, there is a need to develop a systematic and organizational perspective for studying the dynamics of cybersecurity capability development and the mechanisms by which organizations build cybersecurity capabilities, especially in complex organizations such as hospitals [14]. Additionally, the significance of cybersecurity knowledge among internet users has been highlighted to ensure they can react to cyber threats to limit their implications on people's lives [15].In the context of public policy, there is a need for research to understand internet shutdowns as a public policy and to track internet shutdown practices in democracies and hybrid regimes [16, 17]. Moreover, the political power of internet businesses and the impact of internet shutdowns on online media pioneers have been subjects of study, highlighting the need to understand the implications of internet shutdowns on various stakeholders [18] [19].

Analyzing trends and topics in internet governance and cybersecurity debates has provided insights into the evolving landscape of cybersecurity policies and practices, reflecting the dynamic nature of cybersecurity challenges [20]. Market concentration has been identified as a factor influencing cybersecurity risk, underscoring the need for diverse systems and deliberate choices to mitigate cyber risk [21]. Additionally, paper on "Is cybersecurity eating internet governance? Causes and consequences of alternative framings" explores the relationship between cybersecurity governance and internet governance, emphasizing the dynamic nature of cybersecurity-related discourse and its impact on established problems of internet governance [21]. This supports the notion that analyzing trends and topics in internet governance and cybersecurity debates provides insights into the evolving landscape of cybersecurity policies and practices. Furthermore, and Badiei's work highlights the dominance of research on the narrower Internet governance domain of cybersecurity, emphasizing the evolving nature of cybersecurity challenges within the broader study of Internet governance [22].

The literature on internet shutdowns and cybersecurity considerations encompasses a wide range of topics, including the consequences of shutdowns, the impact on different sectors such as healthcare and education, the need for gender considerations, and the implications for public policy and online media pioneers. Understanding the dynamics of cybersecurity capability development and the mechanisms by which organizations build cybersecurity capabilities is crucial, especially in complex organizations such as hospitals. Moreover, the integration of cybersecurity protocols in training sessions for newly hired employees has been highlighted. This is to enhance their understanding and vigilance in areas like managing personal health information, secure email system usage, and safe internet browsing practices.

3. METHODOLOGY

This study outlines a methodical approach for standardizing data on internet shutdowns from 2016 to 2022. It addresses the challenge of harmonizing disparate datasets into a cohesive, analyzable format, thereby facilitating comprehensive global analysis of internet shutdown trends.

This research details a methodology for consolidating diverse yearly datasets into a singular, standardized format. The aim is to enable robust analysis and provide insights into global patterns of internet access disruptions. We have utilized dataset obtained from the KeepItOn Shutdown Tracker Optimization Project [23].

3.1 Data Acquisition and Preliminary Inspection

Initial assessment of the Excel-based dataset revealed distinct sheets per year, each with unique structures and column names, necessitating a tailored approach for standardization.

3.2 Identification of Common Columns

A critical comparison across sheets identified shared columns, establishing a foundation for the unified dataset.

3.3 Creation of a Comprehensive Column List:

We compiled all unique columns across the sheets. This exhaustive list was vital for aligning similar data points that were inconsistently named across years.

3.4 Data Standardization and Cleaning:

Column Standardization: Columns with similar data were renamed for uniformity, such as converting 'Date' and 'Start_Date' to 'start_date' present in the dataset obtained from access now study.

3.5 Handling Missing Data:

We dropped columns with over 80% missing data to maintain analytical robustness, a

threshold determined based on data completeness and relevance.

3.6 Date Standardization:

Date columns were uniformly formatted to ensure temporal data consistency. Data Concatenation and Year Column Addition:

We merged data from all years into one DataFrame. A 'Year' column, derived from the 'start_date' or was added to facilitate temporal analysis.

3.7 Final Data Verification and Cleaning:

The combined dataset underwent rigorous inspection for consistency, with actions such as removing redundant columns and standardizing categorical data formats.

1) Data set Implications

The standardized dataset offers a detailed perspective on global internet shutdowns, crucial for analyzing trends and guiding policy. This methodological approach enhances the reliability of analyses, aiding researchers and policymakers in understanding the multifaceted impacts of internet shutdowns.

2) Reason for Data Adaptation:

Adapting the data was essential due to the original dataset's varied formats and quality across years. Standardization was crucial for producing a reliable, comprehensive dataset that accurately reflects the global scenario of internet access disruptions, thereby supporting nuanced research and informed techno-policy development in digital governance.

3.8 Methodology for Calculating the Economic Impact of Internet Shutdowns in India (2016-2022)

Further our methodology aims to quantify the economic impact of internet shutdowns in India from 2016 to 2022, utilizing a data-driven approach that correlates the duration of shutdowns with their economic consequences.

Data Sources and Preparation

1. Shutdown Duration Data (2016-2022) where details are extracted from a dataset detailing internet shutdowns in India. The total duration was calculated in hours for each year:

- 2016: 15,851 hours
- 2017: 10,587 hours
- 2018: 16,533 hours
- 2019: 48,412 hours
- 2020: 4,973 hours
- 2021: 12,672 hours
- 2022: 4,170 hours

2. Economic Impact Data (2012-2017) derived from "The Anatomy of an Internet Blackout" report [24].

The economic impact of internet shutdowns was thoroughly analyzed in this study, with a focus on the period from 2012 to 2017. During this timeframe, internet shutdowns totaling 16,315 hours resulted in an estimated economic impact of approximately $3.04 billion. To quantify this impact, the study employed a methodical approach for calculating the economic impact per hour, using data from 2012 to 2017. This calculation was based on the formula: Impact Per Hour = Total Economic Impact / Total Shutdown Hours. With the per-hour economic impact established, the study then applied this rate to the total shutdown hours for each year from 2016 to 2022. This application enabled the estimation of the annual economic impacts of internet shutdowns during this six-year period, providing a detailed understanding of the financial consequences associated with these disruptions.

Methodological Approach

a) Data Analysis and Processing: Ensured accuracy in calculating shutdown durations and applied the impact per hour rate consistently across the years and handled missing or incomplete data diligently.
b) Regression Analysis (Optional): Employed linear and polynomial regression models to estimate the economic impact for the years 2018 to 2022, based on shutdown durations.

3.9 Limitations

a) Data Limitations: The economic impact data was only available up to 2017, leading to the extrapolation of impact per hour for subsequent years.
b) Methodological Simplifications: The methodology assumes a direct correlation between shutdown duration and economic impact, potentially simplifying complex economic dynamics.
c) Temporal and Geographical Variations: The study did not account for variations in the economic impact of shutdowns based on specific regions or times within India.

This methodology offers a structured framework for estimating the economic impact of internet

shutdowns in India. While it provides valuable insights, it also acknowledges the need for more detailed data and advanced analytical techniques for a comprehensive understanding. The study highlights the importance of data-driven analysis in assessing the economic implications of internet shutdowns and serves as a basis for future research in this area.

4. DATA ANALYSIS

This section provides the data analysis of the Internet Shutdowns (worldwide) based the KeepItOn [23] dataset ,Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights Report of the Office of the United Nations High Commissioner for Human Rights [1] and report on Understanding India's Troubling Rise in Internet Shutdowns: A Qualitative and Quantitative Analysis [25].

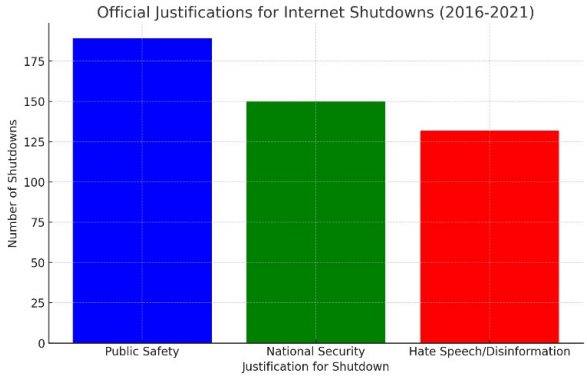

Figure 1: Justification for Internet Shutdowns

Figure 1 visualizes the official justifications for internet shutdowns between 2016 and 2021, as compiled by civil society groups:

- **Public Safety**: This category had the highest number of shutdowns, with 189 instances where shutdowns were justified by public safety concerns.
- **National Security**: There were 150 shutdowns justified on national security grounds.
- **Hate Speech/Disinformation**: There were 132 occurrences where shutdowns were rationalized as measures to curb the proliferation of hate speech, misinformation, or other types of unlawful or detrimental content.

Figure 2 shows the severity of impacts on a scale from 0 to 1 across five different sectors: Reporting, Healthcare, Public Services, Businesses, and Employment. The bars indicate that Reporting is the most affected sector, followed by Healthcare and Businesses, with Public Services and Employment being less affected, though still significant.

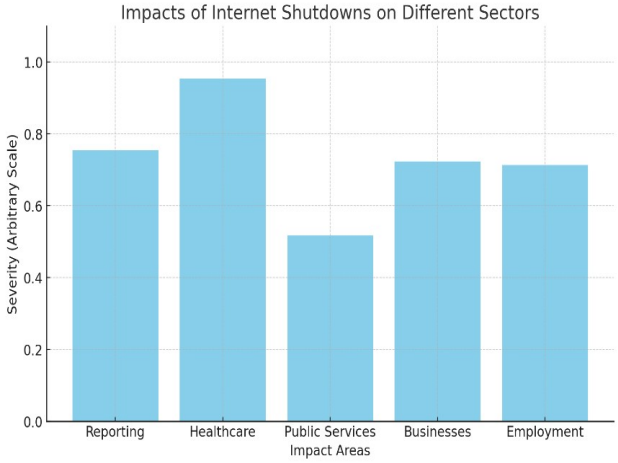

Figure 2: Impacts of Internet Shutdowns on different sectors

Journal of Theoretical and Applied Information Technology
29th February 2024. Vol.102. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

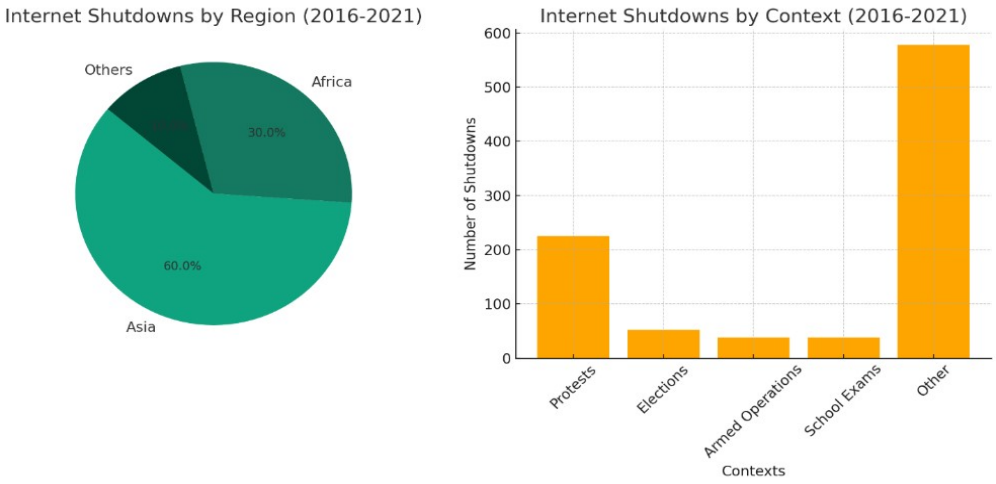

Figure 3: Internet Shutdown by Region and Context

Figure 3 displays two charts. On the left, a pie chart labeled "Internet Shutdowns by Region (2016-2021)" shows three segments: Asia (60%), Africa (30%), and Others (10%). On the right, a bar chart titled "Internet Shutdowns by Context (2016-2021)" illustrates the frequency of shutdowns across five contexts: Protests, Elections, Armed Operations, School Exams, and Other, with the 'Other' category having the highest frequency.

4.1 Data Analysis of Internet Shutdown in India

The bar chart in Figure 4 provides a quantitative analysis of the predominant causes for internet shutdowns within India and its neighboring regions. The x-axis categorizes the shutdowns into distinct causes, while the y-axis quantifies the number of instances associated with each category. The data elucidates that political instability is the leading cause, with approximately 200 instances, signifying a considerable reliance on internet shutdowns as a response to political unrest. This is followed by a category labeled 'Other', indicating shutdown causes that do not fit into the predefined classifications, and then by 'Protest', both indicating over 100 instances. Subsequent causes such as communal violence, general violence, and unknown reasons show a moderate number of instances, ranging from approximately 50 to 75. Categories like information control, exam cheating, and elections reveal a relatively lower prevalence, each accounting for under 50 instances. Notably, the least frequent cause for shutdowns is related to religious holidays or anniversaries, suggesting these events are less commonly associated with internet restrictions in the region.

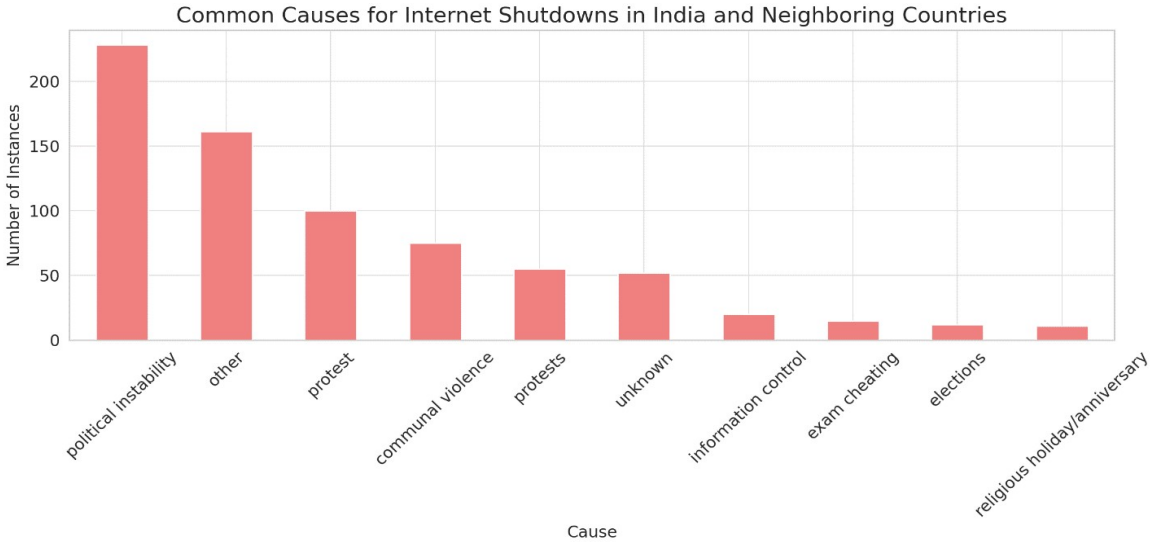

Figure 4: Common Cause for Internet Shutdown in India and Neighboring Countries

Journal of Theoretical and Applied Information Technology
29th February 2024. Vol.102. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 5, Internet Shutdowns in India: Authorities Orders and Network Impacts", shows the frequency of shutdowns ordered by various authorities, represented on the y-axis, with the entities responsible for the orders listed on the x-axis. The state government appears to be the most frequent authority to impose internet shutdowns, with the bar reaching close to 300 instances. It is followed by district authorities, local government, union government, and others, which show significantly fewer instances, all below 50.

Additionally, it illustrates the types of networks impacted by the shutdowns, with the y-axis indicating the number of shutdowns and the x-axis listing the network types. Mobile networks are predominantly affected, with the bar exceeding 300 shutdowns. This is a stark contrast to the other types of networks, such as mobile & broadband, broadband, and satellite, each depicted with bars considerably lower in height, reflecting fewer shutdowns affecting these networks.

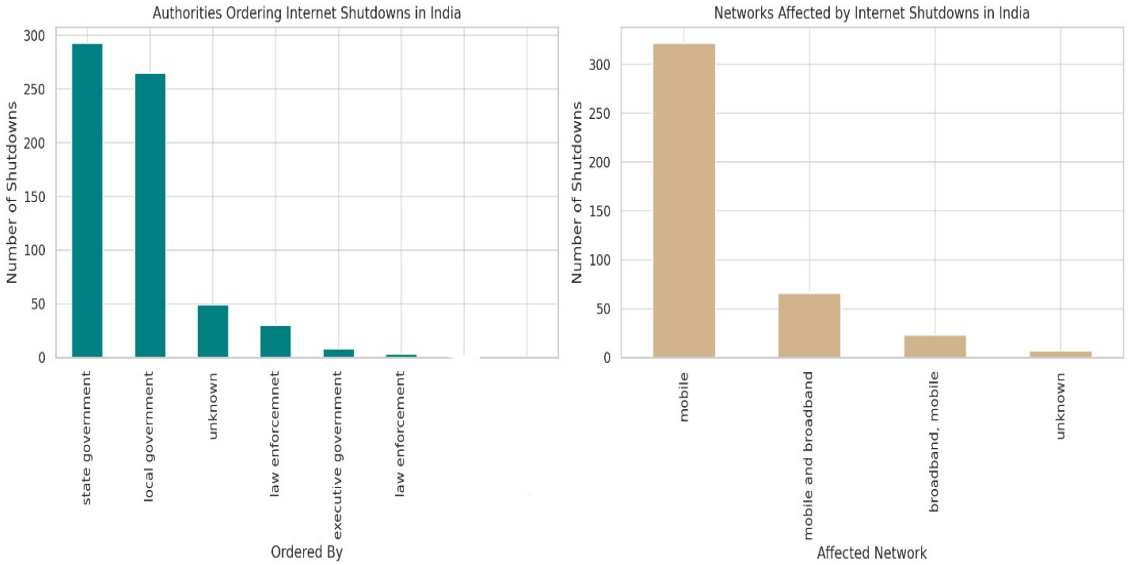

Figure 5: Internet Shutdowns in India: Authorities Orders and Network Impacts

Further, Figure 6 titled "Yearly Internet Shutdowns, India vs Top 10 Countries". The chart provides a comparative visualization of the frequency of internet shutdowns across India and nine other countries, presumably those with the highest number of shutdowns, over an unspecified time period. India appears to have the highest number of shutdowns each year, with bar heights significantly surpassing those of other countries.

Journal of Theoretical and Applied Information Technology
29th February 2024. Vol.102. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

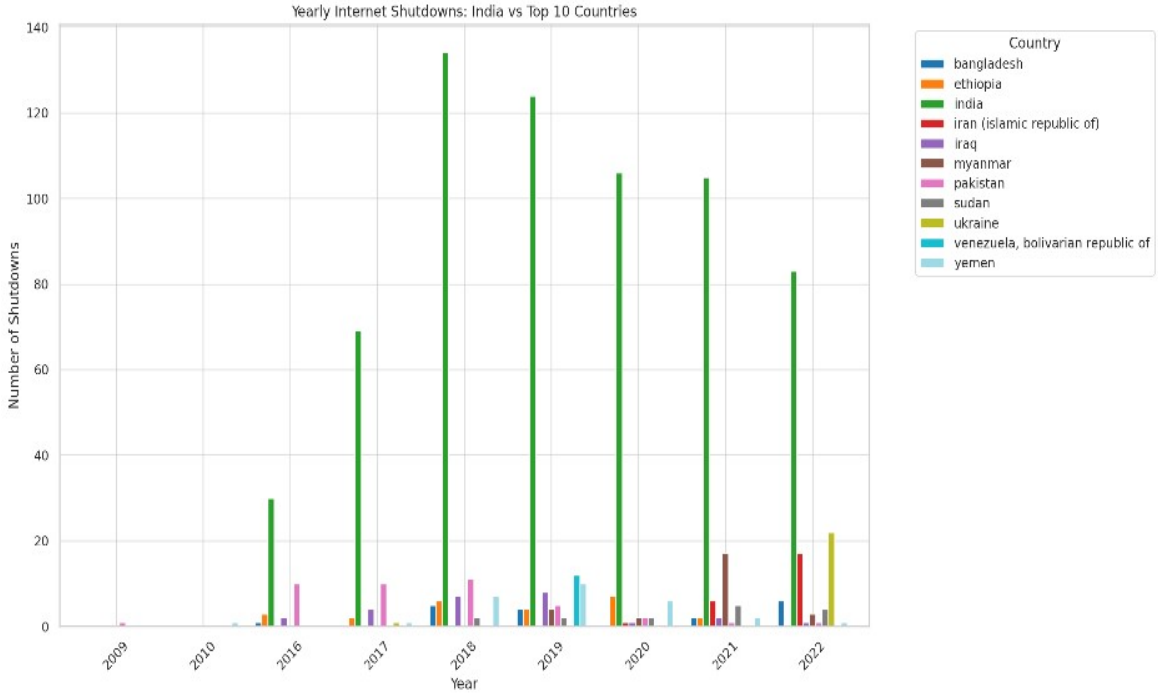

Figure 6: Yearly Internet Shutdowns: India Vs Top 10 Countries

The Figure 7, line graph titled "Yearly Trends of Internet Shutdowns in India" depicts a significant peak in internet shutdowns in 2019, followed by a notable decline. The trend shows an initial increase from 2016 to 2019, then a decrease through 2022, indicating variability in the frequency of shutdowns over the years. The highest frequency of shutdowns was recorded in 2019, marking it as a critical year for internet access disruptions in India.

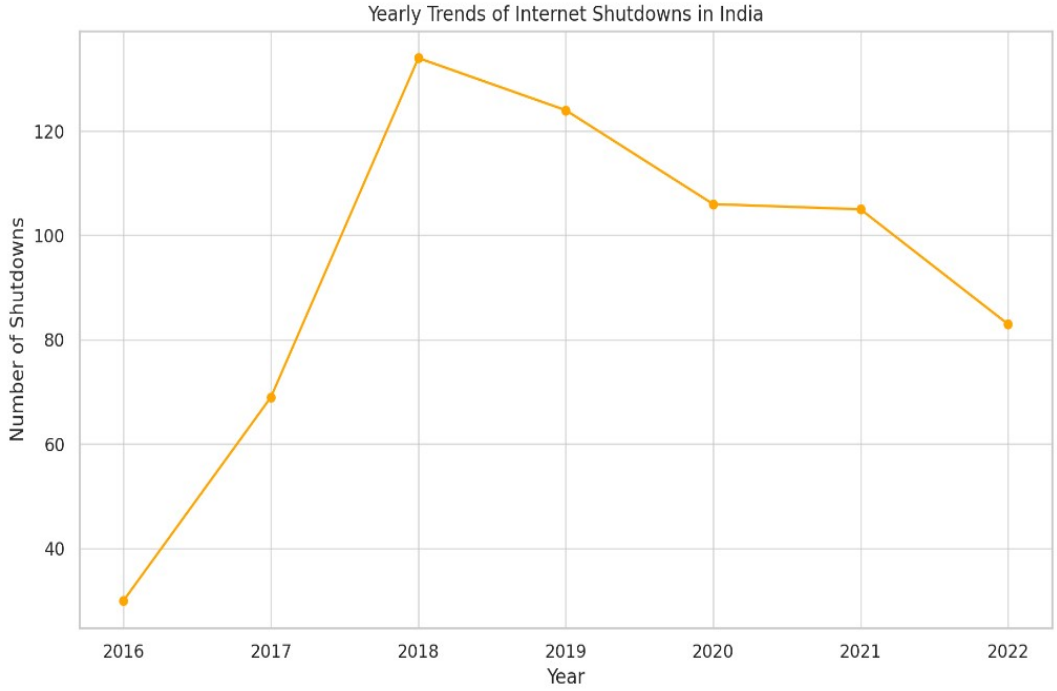

Figure 7: Yearly Trends of Internet Shutdowns in India

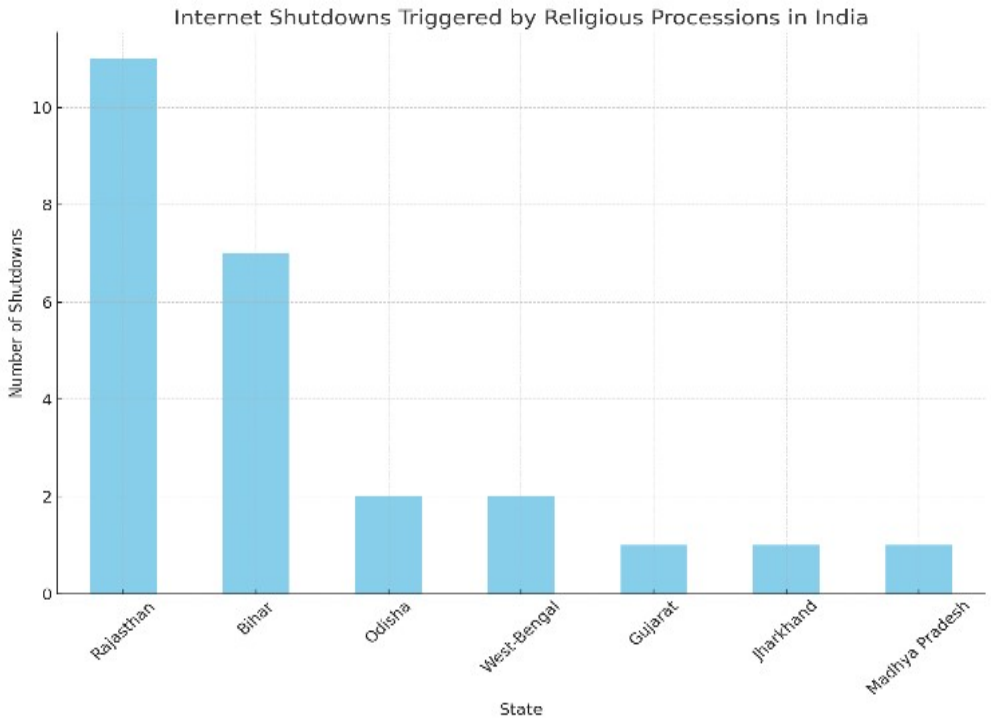

Figure 8: Internet Shutdowns Triggered by Religious Processions in India

The figure 8 visualizes the number of internet shutdowns triggered by religious processions in various Indian states [25]. This visualization highlights the frequency of shutdowns in different states, providing a clear perspective on the geographical distribution of these shutdowns in relation to religious events. Rajasthan appears to have the highest number of shutdowns, followed by Bihar and other states.

5. RESULTS AND DISCUSSIONS

To estimate the economic loss due to internet shutdowns in India from 2018 to 2022, we first need to understand the method of calculation based on the given data. The approach is based on two key components: the total duration of internet shutdowns in hours for each year and the economic impact per hour of shutdown.

5.1 Economic Impact Per Hour Calculation (2012-2017 Data):

- The data provided indicates that from 2012 to 2017, a total economic impact of $3.04 billion was associated with 16,315 hours of internet shutdowns.
- To find the economic impact per hour, we divide the total economic impact by the total shutdown hours: Economic Impact Per Hour=Total Economic ImpactTotal Shutdown HoursEconomic Impact Per Hour=Total Shutdown HoursTotal Economic Impact
- Using the figures given, the calculation becomes: Economic Impact Per Hour=$3.04 billion16,315 hoursEconomic Impact Per Hour=16,315 hours$3.04 billion

5.2 Annual Economic Impact Estimation (2016-2022):

- With the economic impact per hour determined, this rate is applied to the total shutdown hours of each year to estimate the annual economic impacts.
- The given shutdown duration data (in hours) for each year from 2016 to 2022 is used for this purpose.

5.3 Estimating the Loss for 2018-2022:

- To estimate the loss for the years 2018 to 2022, we apply the calculated economic impact per hour to the total shutdown hours for each of these years.

- The sum of these values gives us the estimated total economic loss for the period 2018-2022.
- Specifically, for each year from 2018 to 2022, the total shutdown hours are multiplied by the economic impact per hour, and these figures are then added together.

The calculation we performed based on the above methodology resulted in an estimated economic loss of approximately $16.17 billion from 2018 to 2022. This estimate is crucial for understanding the financial impact of internet shutdowns over these years in India and highlights the significant economic consequences of such disruptions. To further elucidate this point, Table 1 presents a comprehensive overview of the multifaceted aspects of internet shutdowns. It details their impacts and delineates the responsibilities of different stakeholders, offering a broader perspective on the ramifications of these events beyond just the economic losses."

Table 1: Multifaceted aspects of internet shutdowns, their impacts, and the responsibilities of different stakeholders

Category	Insights and Details
Trends in Internet Shutdowns	931 shutdowns reported across 74 countries between 2016-2021. Majority in Asia and Africa. Shift from blanket interventions to targeted approaches using technologies like 5G. Variations in scope and duration, ranging from hours to years. However Internet Shutdown data is not available for Americas and European region in the KeepitOn dataset
Economic Impacts	Disruption in financial transactions, commerce, industry, and labor markets. Creates investment uncertainties, affecting companies and startups. Exacerbates social and economic inequalities.
Impacts on Essential Services	Affects education, healthcare, and social assistance. Inhibits education planning, health information access.
Humanitarian Assistance	Shutdowns impede data collection and assistance delivery. In Myanmar, they endangered local aid organizations.
Companies' Responsibilities	Face pressure to implement shutdowns. Should prevent/mitigate human rights impacts, maintain transparency, and challenge shutdown requests.
Community Resilience	Improved coordination among communities, civil society, and companies. Promotes use of circumvention tools like VPNs. Initiatives for digital media literacy.
Judicial Redress	Various courts found shutdowns illegal. Courts demand reinstatement of connectivity, grant compensation.
General Observations	Often occur without justification, affecting millions. Rarely necessary or proportionate, with extended impacts.
State Responsibilities	Should avoid shutdowns, maximize internet access. Ensure compliance with human rights standards.
Visibility and Collaboration	Calls for collaborative information collection on shutdowns. Proposes a database of shutdown orders and impacts.
Shutdown Guidelines for States	Shutdowns must adhere to legal, necessary, and proportional standards. Require authorization, communication, and redress mechanisms.
Recommendations for Companies	Prevent shutdowns, conduct human rights due diligence. Include shutdown mitigation in policies.
Role of Development Agencies	Integrate human rights in digital connectivity projects. Monitor shutdown impacts on sustainable development goals.
Civil Society's Role	Collaborate in preventing, detecting, responding to shutdowns. Promote digital literacy and access to tools.

The Judicial Redress section in the UN Report on Internet Shutdowns[1] offers an in-depth analysis of the legal responses to internet shutdowns. For a concise overview, Table 2 summarizes these insights, presenting key legal actions and outcomes associated with these shutdowns

Table 2: Key Findings on Internet Shutdowns: Trends, Impacts, and Stakeholder Responsibilities (2016-2021)

Aspect	Details
Role of Judiciary	It is vital for victims and civil society to pursue accountability for human rights violations caused by

	shutdowns.
Legal Actions Against Shutdowns	Many national and regional judicial systems have adjudicated cases involving government entities, officials, and corporations responsible for implementing internet shutdowns
Court Rulings	Courts have deemed previous shutdowns unlawful, mandated the restoration of internet services in active shutdown instances, prohibited authorities from executing future shutdowns, and awarded damages to those impacted.
Specific Examples	India's Supreme Court: Required the disclosure of all internet shutdown orders and set up systems for their review, as seen in the case of Anuradha Bhasin v. Union of India (2020). Economic Community of West African States (ECOWAS) Community Court of Justice: Delivered judgments opposing internet shutdowns in Togo and Nigeria. European Court of Human Rights: Determined a violation of the right to freedom of expression in a case concerning internet censorship
Challenges in Judicial Review	Delays and slow pace of court proceedings. Cases sometimes deemed moot once a shutdown ends. Limited digital expertise among judiciary members. Broad discretion in matters of national security can obstruct judicial challenges.

Further, table 3 summarizes key insights into the patterns of internet shutdowns in India, highlighting the increased frequency and duration of shutdowns, the geographic areas most affected, the political and social reasons behind these actions, the roles of responsible officers, and the broad impacts on multiple sectors of society.
Overview of Internet Shutdown Trends in India [25]

Table 3: Key insights into the patterns of internet shutdowns in India

Key Insight	Description
Increased frequency of shutdowns	India has experienced a significant increase in the number of internet shutdowns in recent years, particularly in the Northern and North-Eastern states
Responsible officers	The individuals authorized to order a shutdown.
Duration of shutdowns	Over time, the average length of internet shutdowns has grown, suggesting a trend towards more focused and strategic use of these shutdowns.
Impact on various sectors	Internet shutdowns have far-reaching consequences for internet users, affecting their socio-economic well-being, psychological health, and access to information and communication resources.

6. DISCUSSION

The analysis reveals a growing trend of increased internet shutdowns in India, and the shutdowns have profound consequences on various sectors, affecting socio-economic well-being, psychological health, and access to information and communication resources. Recent trends show some decline in the Shutdown incidents. The trends highlight the need for a nuanced approach to address the multifaceted impacts of internet shutdowns, considering both economic losses and broader societal implications. It is urgent for stakeholders, including the governments, to reevaluate policies and practices to minimize repercussions on citizens and the economy and to standardize the process of Internet Shutdowns balancing the National needs.

7. CYBERSECURITY CONSIDERATIONS

Correlation coefficients are statistical measures that can be used to determine the strength and direction of the relationship between two variables. In this case, we used Pearson's correlation coefficient, which is a measure of the linear correlation between two data sets. The two datasets used are KeepitOn dataset [23] for Internet Shutdown and cyber events database [26].

The coefficient has a value between -1 and 1, where:

- 1 indicates a perfect positive linear correlation,
- 0 indicates no linear correlation,

-1 indicates a perfect negative linear correlation

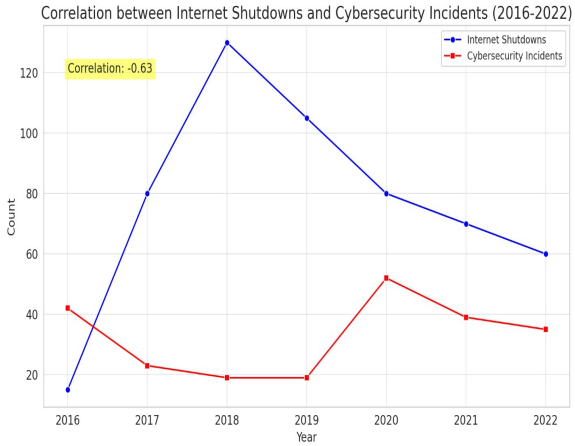

Figure 9: Correlation between Internet Shutdowns and Cybersecurity Incidents (2016-2022)

The formula for Pearson's correlation coefficient (r) is:

$$r = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2 \cdot \sum(y_i - \bar{y})^2}} \quad (1)$$

Where,

x_i and y_i are the individual sample points indexed with i,
$\bar{x}$ and $\bar{y}$ are the means of the X and Y datasets, respectively

The coefficient of approximately -0.63 in this context indicates a moderate negative linear relationship, meaning that generally, as one variable increases, the other tends to decrease, but this relationship is not strong enough to predict the exact behavior of one variable based solely on the other.

The relationship between internet shutdowns and cybersecurity vulnerabilities is a complex and multifaceted issue. Internet shutdowns, whether imposed by authorities or due to technical issues, can significantly impact a region's cybersecurity landscape. When authorities shut down the internet, it not only disrupts communication channels but also hampers the ability to implement timely cybersecurity measures, leaving individuals and organizations more susceptible to cyber threats [27]. One key aspect of this relationship is the loss of real-time monitoring and threat intelligence that occurs during an internet shutdown. Cybersecurity relies heavily on continuous monitoring of network activities to detect and respond to potential threats promptly. With the internet inaccessible, security teams lose their ability to monitor and analyze incoming and outgoing traffic, making it challenging to identify and mitigate cyber threats effectively [28]. Internet shutdowns can exacerbate existing vulnerabilities by impeding the application of security patches and updates. Without online access, individuals and organizations may struggle to download and install crucial security updates, leaving systems exposed to known exploits. This heightened vulnerability becomes particularly concerning as threat actors often target unpatched systems during periods of disruption or uncertainty [29].

The impact of internet shutdowns on cybersecurity infrastructure is a critically significant concern in the ever-evolving digital age. By deliberately interrupting access to the vast expanse of the internet, these disruptive shutdowns create insidious vulnerabilities within the intricate web of cybersecurity systems, thus creating ample opportunities for nefarious and malicious actors to exploit. Consequently, the loss of connectivity during such a shutdown effectively strips individuals and organizations of the indispensable defenses and invaluable resources necessary to effectively safeguard their sensitive data and intricate networks. Moreover, during this period of forced isolation from the digital realm, the looming specter of cyber threats has the potential to intensify exponentially due to the glaring absence of robust monitoring and responsive capabilities [30]. During internet shutdowns, cybersecurity risks are significantly amplified, posing a grave threat to individuals, enterprises, and institutions alike. The limited access to the internet not only hampers the flow of information but also creates fertile ground for exploiting vulnerabilities in the cyber infrastructure. This unfortunate state of affairs is particularly conducive to potential unauthorized access attempts, insidious data breaches, and crippling denial-of-service attacks. Cybercriminals, emboldened by the disrupted communication channels, seize the opportunity to infiltrate systems, exploit weaknesses, and carry out malevolent activities with impunity. The absence of real-time monitoring and updates during internet shutdowns exacerbates the vulnerability of networks and systems, leaving them susceptible to all manner of cyber threats.

The lack of immediate visibility into potential breaches and the inability to promptly respond to security incidents can plunge organizations into a perilous situation. The consequences of a weakened cybersecurity posture during these turbulent times can be catastrophic, leading to irreparable damage, financial losses, and degradation of public trust. Therefore, it is vital for individuals, organizations, and authorities to recognize and address the magnitude of

cybersecurity concerns during internet shutdowns. The implementation of robust mitigation strategies becomes an imperative necessity in order to minimize the potential risks and fortify the cyber defenses. Proactive measures such as strengthening firewalls, enhancing encryption protocols, conducting regular vulnerability assessments, and fostering a culture of cyber awareness amongst all stakeholders can provide much-needed resilience and protection during these tumultuous periods [11, 31].

The spread of misinformation and disinformation is a significant consequence of internet shutdowns, exacerbating cybersecurity vulnerabilities. During shutdowns, the lack of access to reliable sources of information creates an environment where false narratives can thrive. Misinformation, whether unintentional or deliberately disseminated, can have severe consequences on individuals, communities, and even national security [8]. Internet shutdowns facilitate the rapid dissemination of false information through social media platforms and other communication channels. This unrestricted flow of misinformation can incite fear, panic, and social unrest, leading to widespread confusion and distrust. In addition, malicious actors can take advantage of the chaos caused by shutdowns to manipulate public opinion and further their own agendas [32]. Verifying information during shutdowns becomes a daunting challenge as reliable sources are inaccessible or limited. This hampers individuals' ability to differentiate between accurate and false information, making them more susceptible to manipulation and propaganda. Consequently, authorities and stakeholders must implement strategies to address information distortion during internet shutdowns, ensuring access to reliable information sources and promoting media literacy among the public. Only by countering the spread of misinformation and disinformation can the potential cybersecurity vulnerabilities and societal implications be mitigated [32].

Promoting access to reliable information during internet shutdowns is paramount to sustaining democratic principles and informed decision-making. Policymakers should prioritize the development and implementation of measures that safeguard the public's right to access accurate information even in times of crisis. This includes establishing alternative communication channels and technologies that can operate independently of traditional internet infrastructure, such as mesh networks or satellite-based systems. Authorities must also refrain from imposing blanket internet shutdowns and instead focus on targeted interventions that address specific security concerns, balancing the need for public safety with the preservation of fundamental freedoms[33, 34].

Hence, the relationship between internet shutdowns and cybersecurity vulnerabilities is intricate and multifaceted. The impact of internet shutdowns on cybersecurity infrastructure is a critically significant concern in the ever-evolving digital age. It is vital for individuals, organizations, and authorities to recognize and address the magnitude of cybersecurity concerns during internet shutdowns. The spread of misinformation and disinformation during shutdowns exacerbates cybersecurity vulnerabilities, making it essential for policymakers to prioritize the development and implementation of measures that safeguard the public's right to access accurate information even in times of crisis.

8. RECOMMENDATIONS

8.1 Policy and Practice

Policy and practice in the realm of cybersecurity and internet shutdown challenges, a multi-faceted approach is essential. Policymakers should prioritize the development and enforcement of comprehensive regulations that safeguard digital rights, promote transparency, and hold those accountable for malicious cyber activities or misinformation dissemination. International collaboration and information-sharing agreements should be fostered to enhance collective resilience and response capabilities against global cyber threats. Authorities must invest in educational initiatives to elevate digital literacy, empowering individuals to discern credible information and contribute to a more informed online environment. Additionally, fostering public-private partnerships and incentivizing the adoption of resilient technologies can fortify cybersecurity measures, ensuring a cohesive defense against evolving threats while mitigating the impact of internet shutdowns on communication channels. This integrated strategy, combining regulatory frameworks, global cooperation, educational efforts, and technological advancements, is crucial to establishing a secure and resilient digital landscape.

Based on the analysis of the economic and cybersecurity impacts of internet shutdowns, the following policy recommendations are suggested:

a) Regulatory Framework for Shutdowns: Establish clear legal and regulatory frameworks governing when and how internet

shutdowns can be implemented, ensuring they are used only as a last resort and for the shortest time necessary.

b) Transparency and Accountability: Mandate transparency in the decision-making process for internet shutdowns, including public disclosure of the reasons and duration.
c) Protection of Essential Services: Ensure that access to critical online services like healthcare, banking, and emergency services is maintained even during shutdowns.
d) Compensation Mechanism: Develop a compensation mechanism for individuals and businesses adversely affected by shutdowns.
e) Cybersecurity Education: Implement widespread cybersecurity education initiatives to address issues that shutdowns aim to solve, such as the spread of misinformation.
f) International Collaboration: Encourage international collaboration to develop best practices and standards for managing internet access during crises.
g) Monitoring and Evaluation: Regularly monitor and evaluate the impact of shutdowns to inform future policy decisions.

Implementing these policies can mitigate the negative impacts of internet shutdowns while balancing the need for national security and public safety.

8.2 Developing International Norms and Standards

The development of international norms and standards is crucial in addressing cybersecurity vulnerabilities and information distortion caused by internet shutdowns. By establishing uniform guidelines, countries can work together to mitigate the risks associated with these shutdowns and ensure the security and integrity of online systems. These norms and standards can encompass various aspects, including protocols for responding to cyber threats, sharing information on vulnerabilities and attacks, and cooperation in investigating and prosecuting cybercriminals. Additionally, international norms and standards can help in promoting the free flow of accurate information during shutdowns, mitigating the spread of misinformation and disinformation. By fostering collaboration and coordination at a global level, the development and implementation of these norms and standards can significantly strengthen cybersecurity efforts and protect individuals and organizations from the detrimental effects of internet shutdowns. The progressive development of international cyber law is suggested to pacify the internet and internationally criminalize cyber violence [35]. This aligns with the need for uniform guidelines and international cooperation to address cybersecurity vulnerabilities and information distortion caused by internet shutdowns. Additionally, the lack of awareness of human vulnerabilities related to cybersecurity, such as phishing attacks and social engineering, needs to be addressed and reduced through proper awareness and training [36]. This emphasizes the importance of establishing protocols for responding to cyber threats and sharing information on vulnerabilities and attacks, as well as the need for cooperation in investigating and prosecuting cybercriminals. Furthermore, the development of state security issues related to cybercrime is being debated among international security studies [37]. This highlights the significance of establishing international norms and standards to address cybersecurity vulnerabilities and information distortion caused by internet shutdowns, as it requires global collaboration and coordination. Additionally, the development of the Internet has made cybersecurity more important and serious [38], emphasizing the need for uniform guidelines and standards to ensure the security and integrity of online systems. Moreover, the development of international cybersecurity norms through bilateral collaboration has made the United States an impactful actor in international cybersecurity [39].

This underscores the importance of developing international norms and standards to foster collaboration and coordination at a global level, as it can significantly strengthen cybersecurity efforts and protect individuals and organizations from the detrimental effects of internet shutdowns. In conclusion, the synthesis of these references supports the critical need for developing international norms and standards to address cybersecurity vulnerabilities and information distortion caused by internet shutdowns. By establishing uniform guidelines and fostering collaboration at a global level, countries can work together to mitigate the risks associated with these shutdowns and ensure the security and integrity of online systems.

9. CONCUSION AND FUTURE WORK

In conclusion, the impact of internet shutdowns on cybersecurity vulnerabilities and information distortion is significant and multifaceted. Internet shutdowns not only disrupt the functioning of critical cybersecurity infrastructure but also amplify

cybersecurity risks. Furthermore, during shutdowns, the spread of misinformation and disinformation becomes prevalent, challenging the verification of information and leading to the manipulation of public opinion with political consequences. To mitigate these challenges, preemptive measures to strengthen cybersecurity, ensure resilience of internet infrastructure during shutdowns, and promote access to reliable information are crucial. Additionally, it is important to consider the legal and ethical implications of internet shutdowns, striking a balance between national security and individual freedoms. The implications for future research and action in the context of internet shutdowns and cybersecurity vulnerabilities involve several key areas. Firstly, there is a need for further investigation into the long-term effects of internet shutdowns on cybersecurity infrastructure, as these disruptions can potentially weaken the overall security of networks and systems. Additionally, further research should focus on understanding how internet shutdowns amplify cybersecurity risks, such as the increased likelihood of cyberattacks and data breaches during these periods. Understanding these dynamics will provide deeper insights into the broader consequences of internet shutdowns.

REFERENCES

[1] Human Rights Council, U., Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights. 2022, Human Rights Council. p. 17.

[2] Tarisayi, K.S. and E. Munyaradzi(s), A Teacher Perspective on the Impact of Internet Shutdown on the Teaching and Learning in High Schools in Zimbabwe. Human Behavior and Emerging Technologies, 2020. https://doi.org/10.1002/hbe2.230

[3] Murrey, A.(s), A Decolonial Political Geography of Resistance and Digital Infrastructural Harm in Cameroon and Ethiopia. Globalizations, 2022. https://doi.org/10.1080/14747731.2022.2149162

[4] Bhatia, K.V., et al.(s), Protests, Internet Shutdowns, and Disinformation in a Transitioning State. Media Culture & Society, 2023. https://doi.org/10.1177/01634437231155568

[5] Momen, M.N., S. Harsha, and D. Das(s), Mediated Democracy and Internet Shutdown in India. Journal of Information Communication and Ethics in Society, 2020. https://doi.org/10.1108/jices-07-2020-0075

[6] Hadi, I.S., R.N. Arfani, and H. Ikhwan(s), Internet Shutdown Policy at Papua and West Papua Through the Public Policy Perspective. Indonesian Journal of Social Science Research, 2022. https://doi.org/10.11594/ijssr.03.01.01

[7] Hadlington, L.(s), Human Factors in Cybersecurity; Examining the Link Between Internet Addiction, Impulsivity, Attitudes Towards Cybersecurity, and Risky Cybersecurity Behaviours. Heliyon, 2017. https://doi.org/10.1016/j.heliyon.2017.e00346

[8] Alhuwail, D., et al.(s), Information Security Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities. Applied Clinical Informatics, 2021. https://doi.org/10.1055/s-0041-1735527

[9] Millar, K., J. Shires, and T. Tropina(s), Gender Approaches to Cybersecurity: Design, Defence and Response. 2021. https://doi.org/10.37559/gen/21/01

[10] Sardi, A., et al.(s), Cyber Risk in Health Facilities: A Systematic Literature Review. Sustainability, 2020. https://doi.org/10.3390/su12177002

[11] Zulkipli, N.H.N.(s), Synthesizing Cybersecurity Issues and Challenges for the Elderly. Turkish Journal of Computer and Mathematics Education (Turcomat), 2021. https://doi.org/10.17762/turcomat.v12i5.2180

[12] Gordon, W.J., et al.(s), Protecting Procedural Care—cybersecurity Considerations for Robotic Surgery. NPJ Digital Medicine, 2022. https://doi.org/10.1038/s41746-022-00693-8

[13] Jofre, M., et al.(s), Cybersecurity and Privacy Risk Assessment of Point-of-Care Systems in Healthcare—A Use Case Approach. Applied Sciences, 2021. https://doi.org/10.3390/app11156699

[14] Jalali, M.S. and J.P. Kaiser(s), Cybersecurity in Hospitals: A Systematic, Organizational Perspective. Journal of Medical Internet Research, 2018. https://doi.org/10.2196/10059

[15] Amankwa, E.(s), Relevance of Cybersecurity Education at Pedagogy Levels in Schools. Journal of Information Security, 2021. https://doi.org/10.4236/jis.2021.124013

[16] Hadi, I.S., R.N. Arfani, and H. Ikhwan(s), Dynamics of People, State, and Cyber Power in the Internet Shutdown Policy at Papua and West Papua in 2019. 2022. https://doi.org/10.2991/assehr.k.220705.025

[17] Vargas-Leon, P.(s), Tracking Internet Shutdown Practices: Democracies and Hybrid Regimes. 2016. https://doi.org/10.1057/9781137483591_9

[18] Freyburg, T., L. Garbe, and V. Wavre(s), The Political Power of Internet Business: A Comprehensive Dataset of Telecommunications Ownership and Control (TOSCO). The Review of International Organizations, 2022. https://doi.org/10.1007/s11558-022-09483-z
[19] Safitri, R. and U.F. Noviadhista(s), Where Did Indonesian Online Media Pioneer Stand on Internet Shutdown Issue? Komunikator, 2020. https://doi.org/10.18196/jkm.121030
[20] Cogburn, D.L.(s), Analyzing Trends and Topics in Internet Governance and Cybersecurity Debates Found in Twelve Years of IGF Transcripts. 2019. https://doi.org/10.24251/hicss.2019.110
[21] Mueller, M.(s), Is Cybersecurity Eating Internet Governance? Causes and Consequences of Alternative Framings. Digital Policy Regulation and Governance, 2017. https://doi.org/10.1108/dprg-05-2017-0025
[22] Cogburn, D.L.(s), Big Data Analytics and Text Mining in Internet Governance Research: Computational Analysis of Transcripts From 12 Years of the Internet Governance Forum. 2020. https://doi.org/10.7551/mitpress/12400.003.0010
[23] Felicia Anthoni, Z.R., *Shutdown Tracker Optimization Project (STOP)* 2023.
[24] Rajat Kathuria, M.K., Gangesh Varma,Kaushambi Bagchi,Richa Sekhani, *The Anatomy of an INTERNET BLACKOUT: Measuring the Economic Impact of Internet Shutdowns in India*. 2018, Indian Council for Research on International Economic Relations: India. p. 68.
[25] Ruijgrok, K., *Understanding India's Troubling Rise in Internet Shutdowns*. 2021: India. p. 39.
[26] Harry, C., and N. Gallagher.(s), Classifying Cyber Events: A Proposed Taxonomy. Journal of Information Warfare, 2018. vol. 17(pp. 17–31.
[27] Joseph, A.M., et al.(s), COVID-19 Misinformation on Social Media: A Scoping Review. Cureus, 2022. https://doi.org/10.7759/cureus.24601
[28] Treen, K.M.d.I., H.T.P. Williams, and S. O'Neill(s), Online Misinformation About Climate Change. Wiley Interdisciplinary Reviews Climate Change, 2020. https://doi.org/10.1002/wcc.665
[29] Schaaf, K.v.d., B. Tekinerdoğan, and Ç. Çatal(s), A Feature-based Approach for Guiding the Selection of Internet of Things Cybersecurity Standards Using Text Mining. Concurrency and Computation Practice and Experience, 2021. https://doi.org/10.1002/cpe.6385
[30] Taran, P.K., M. Bakkal, and N. Mammadlİ(s), Florür Ve Internet: Halkın Kullanımına Sunulan Çevrimiçi Bilgilerin Değerlendirmesi. Acta Odontologica Turcica, 2022. https://doi.org/10.17214/gaziaot.947860
[31] Fernández-Caramés, T.M. and P. Fraga-Lamas(s), Teaching and Learning IoT Cybersecurity and Vulnerability Assessment With Shodan Through Practical Use Cases. Sensors, 2020. https://doi.org/10.3390/s20113048
[32] Kuo, R. and A.E. Marwick(s), Critical Disinformation Studies: History, Power, and Politics. 2021. https://doi.org/10.37016/mr-2020-76
[33] Siatitsa, I.(s), Freedom of Assembly Under Attack: General and Indiscriminate Surveillance and Interference With Internet Communications. International Review of the Red Cross, 2020. https://doi.org/10.1017/s1816383121000047
[34] Royan, R., et al.(s), Use of Twitter Amplifiers by Medical Professionals to Combat Misinformation During the COVID-19 Pandemic. Journal of Medical Internet Research, 2022. https://doi.org/10.2196/38324
[35] Simović, M.N., Ž. Rašević, and V. Šimović(s), Cyber Warfare and International Cyber Law: Whither? Journal of Criminology and Criminal Law, 2020. https://doi.org/10.47152/rkkp.58.3.2
[36] Alsharif, M., S. Mishra, and M. Alshehri(s), Impact of Human Vulnerabilities on Cybersecurity. Computer Systems Science and Engineering, 2022. https://doi.org/10.32604/csse.2022.019938
[37] Darussalam, M.F. and A.A. Adhisty(s), State Action as an Individual Security Threat in Case of Cybercrime Securitization. Jurnal Pertahanan Media Informasi TTG Kajian & Strategi Pertahanan Yang Mengedepankan Identity Nasionalism & Integrity, 2019. https://doi.org/10.33172/jp.v5i3.589
[38] Shi, J., et al.(s), Research on Cro's Dilemma in Sapiens Chain: A Game Theory Method. 2018. https://doi.org/10.5121/csit.2018.81508
[39] Purwanti, D.(s), The United States Motivation in Having Cyber Security Cooperation With China. Journal of International Studies on Energy Affairs, 2021. https://doi.org/10.51413/jisea.vol2.iss1.2021.105-122