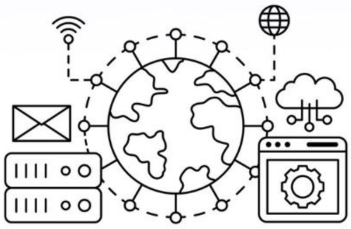
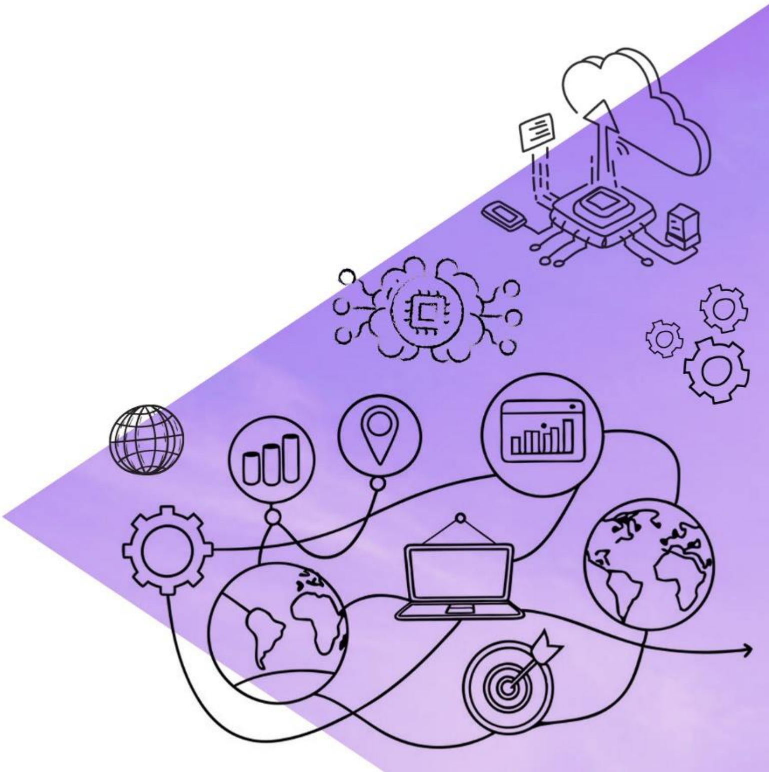
CASS
CENTRE for AEROSPACE & SECURITY STUDIES



Guarding Against Global IT Outages: A Blueprint for Digital Resilience

Shah Muhammad
Research Assistant



Working Paper

Opinions expressed are those of the author/s and do not necessarily reflect the views of the Centre. Complete responsibility for factual accuracy of the data presented and bibliographic citations lie entirely with the author/s. CASS has a strict zero tolerance plagiarism policy.

President
Air Marshal Javaid Ahmed (Retd)

Edited by:
Sarah Siddiq Aneel

Layout
Hira Mumtaz

All correspondence pertaining to this publication should be addressed to CASS, Islamabad, through post or email at the following address:

Centre for Aerospace & Security Studies

☎ +92 051 5405011
✉ cass.thinkers@casstt.com
f cass.thinkers
◎ cassthinkers
𝕏 @CassThinkers
in Centre for Aerospace & Security Studies

Old Airport Road, Islamabad, Pakistan
www.casstt.com

CENTRE for AEROSPACE & SECURITY STUDIES

Guarding Against Global IT Outages: A Blueprint for Digital Resilience

Working Paper

Shah Muhammad

Research Assistant

TABLE OF CONTENTS

Abstract

There is an accelerating trend of global disruptions becoming increasingly digital in nature. This trend of global IT outages is indicative of deep-seated vulnerabilities and technical lapses in the interconnected networks of Digital Public Infrastructure (DPI). Drawing on the theoretical stream of digital disconnection, this paper offers an empirical account of the causes and detailed cases of prominent global IT outages in the recent past. The cases offer insights into the intricacies of IT meltdowns as well as ensuing ramifications on different sectors globally. Subsequently, it lays down a set of viable policy measures that may be undertaken at global, national, organisational and individual levels to prevent the likelihood of IT blackouts in future and thereby maintain digital resilience in the DPI worldwide. The paper essentially contributes to the relatively scant literature on IT outages – a subject of paramount significance in an increasingly interconnected world of Industry 4.0.

Keywords: Global IT Outage, Digital Resilience, Digital Era, Globalisation, Blackouts

Introduction

Outages have long been a recurring feature of history, from telegraph disruptions to widespread electricity blackouts. However, IT outages are a defining characteristic of the digital era marked by their speed, scale, and cross-sector impact. In an increasingly globalised world, such disruptions often trigger cascading effects that transcend national and institutional boundaries. On July 19, 2024, the world woke up to the 'largest outage in history' that left organisations, sectors and individuals in a state of disarray.[1] A technical glitch in Microsoft's Windows operating system caused it to abruptly fail, setting off a chain reaction of disruptions worldwide. Prominent IT service providers and Big Tech companies are usually at the centre of such meltdowns because their systems are embedded in every nook and cranny of the digital realm. Evidently, they are responsible for around two-thirds of all reported outages globally.[2]

While there is no objective or universally accepted definition of a global IT outage, this paper adopts the Atlantic Council's approach, which links such outages to disruptions in Digital Public Infrastructure (DPI).[3] DPI is a 'combination of networked open technology standards built for public interest, enabling governance, and a community of innovative and competitive market players working to drive innovation, especially across public programmes.'[4] Therefore, digital services offered by Big Tech companies essentially fall under the purview of DPI. Its intangibility is analogous to the tangibility of public infrastructure given that DPI connects 'people, data and money in much the same way that roads and railways connect people and goods.'[5] Hence, it is crucial to theoretically and empirically analyse the complex facets of IT meltdowns worldwide given the accelerating convergence of 'sociality' (social structures) and 'digitality' (digital systems).

The past instances of infrastructural breakdowns have been evaluated to argue that these disruptions have widespread and, at times, under-researched implications for the financial as well as sociocultural condition of the population. Along with raising the need for theoretical developments in this domain, the paper offers an empirical

[1] Dan Milmo et al., "Slow Recovery from IT Outage Begins as Experts Warn of Future Risks," *Guardian*, July 20, 2024, https://www.theguardian.com/australia-news/article/2024/jul/19/microsoft-windows-pcs-outage-blue-screen-of-death.

[2] Douglas Donnellan and Andy Lawrence, *Annual Outage Analysis 2024*, report (New York: Uptime Institute, March 27, 2024), 8, https://datacenter.uptimeinstitute.com/rs/711-RIA-145/images/2024.Resiliency.Survey.ExecSum.pdf?version=0&mkt_tok=NzExLVJJQS0xNDUAAAGSPCeKfdv0kYTrLS-6.

[3] Saba Weatherspoon and Zhenwei Gao, "The Great IT Outage of 2024 Is a Wake-up Call about Digital Public Infrastructure," *Atlantic Council*, August 6, 2024, https://www.atlanticcouncil.org/blogs/new-atlanticist/the-great-it-outage-of-2024-is-a-wake-up-call-about-digital-public-infrastructure/.

[4] UNDP, "Digital Public Infrastructure," accessed November 2, 2024, https://www.undp.org/digital/digital-public-infrastructure.

[5] Bill & Melinda Gates Foundation, "Digital Public Infrastructure," accessed November 16, 2024, https://www.gatesfoundation.org/our-work/programs/global-growth-and-opportunity/digital-public-infrastructure.

account of recent IT disruptions. These blackouts originate mainly from Big Tech companies, raising critical questions about the need to regulate the global digital economy. Drawing on the best practices and innovative measures, the paper offers an evidence-based array of policy measures that could minimise the probability of such unwanted occurrences.

The paper begins with elucidation of the theory of digital disconnection in the context of prevailing IT blackouts, followed by a comprehensive account of the causes of these disruptions. The causes range from technical factors and cyber-attacks to human errors. Subsequently, it analyses prominent IT outages while highlighting their widespread implications in different sectors. The last section offers actionable policy measures that may be undertaken at global, national, organisational and individual levels to prevent the likelihood of a digital crisis, paving the way for digital resilience and stability. The paper is a scholarly endeavour to evaluate the intricacies of IT meltdowns and contribute to the relatively limited literature in this domain.

Towards the Theory of Digital Disconnection

Digital disconnection is not a well-crafted theory per se but a set of scholarly ideas that may lead to the formation of a distinct theoretical stream. Disconnection in an increasingly digital age is often an inconvenient and unusual phenomenon, revealing society's deeply entrenched system dependencies and vulnerabilities. Historically, larger disruptions in modes of communication such as newspaper shortages or telephone breakdowns entailed certain social meaning. For instance, scholars studying telephonic disruptions have coined terms like 'imminent connectedness' and 'symbolic proximity' to make sense of people's reactions to this disruption.[6] Papacharissi explored the concept of 'networked self' – the individuals' attempts to make sense of their self in the age of technology.[7] Similarly, Lagerkvist coined the term 'digital exister' to evaluate people's vulnerabilities in the digital era.[8] Existential affiliation with technology may be deemed as a new cultural phenomenon that shapes individual thoughts and behaviour.

Being a subjective experience, it may not be fully possible to study the wide array of human responses during outages. For instance, breakdowns are also an opportunity for individuals to reflect on their digital entanglement and disentanglement.[9] Some cases of voluntary disconnection are undertaken as 'digital detox' by users to go back

[6] Alan H. Wurtzel and Colin Turner, "Latent Functions of the Telephone: What Missing the Extension Means," *MIT Press*, (2011) https://eric.ed.gov/?id=ED125026.

[7] Zizi Papacharissi, *A Networked Self and Birth, Life, Death* (London: Routledge, 2018).

[8] Amanda Lagerkvist, "Digital Existence: An Introduction," in *Digital Existence* (London: Routledge, 2018), 1–25.

[9] André Jansson and Paul C. Adams, *Disentangling: The Geographies of Digital Disconnection* (Oxford: Oxford University Press, 2021).

to what they deem as a more genuine and organic mode of being.[10] This may be the outcome of enduring tension between the traditional self and digital self of users in the age of perpetual connectivity. In this regard, the concept of digital well-being suggests individual agency to control and moderate their use of digital tools to maximise benefits and minimise risks.[11] This contrasts with Paasonen[12] and Lagerkvist's[13] assertion that users are as subject to the unpredictability and disruptiveness of technology as they are in control of it. In essence, the existing literature strives to qualitatively and quantitatively make sense of the subject-object relationship between technology and users in different contexts.

This paper does not analyse the cases of voluntary disconnection undertaken by users who willingly choose to isolate themselves from social media platforms or IT services. On the contrary, it analyses three dimensions of involuntary disconnection, with the third being the primary scope of this paper. The first involuntary disconnection is tantamount to shutdowns or blackouts imposed by repressive states in order to control the flow of information.[14] The second type is the everyday experience of users who face software and hardware breakdowns in their daily lives. This is limited in scope and usually generates an emotional response such as frustration and lack of control.[15] The analytical trajectory of the paper is solely driven by a third type of involuntary digital disconnection which is marked by widespread and unplanned infrastructural breakdowns. It is derived from the study on electric power blackouts by Nye who argues that a blackout is not merely a technical event but a social and cultural disruption.[16] This theoretical compass acquires a comprehensive scope when it is linked with the Atlantic Council's take on global IT outages as breakdowns in DPI.

Evolution of Infrastructural Breakdowns

The world has been dealing with varying levels of breakdowns in infrastructural systems such as electricity and telephone networks. Nye conducted one of the most comprehensive studies on electricity failures in the US from 1935 to 2003.[17] Notably, he covered the Great Northeastern Blackout of 1965, the New York City Blackout of

[10] Trine Syvertsen and Gunn Enli, "Digital Detox: Media Resistance and the Promise of Authenticity," *Convergence* 26, no. 5–6 (2020): 1269–83.

[11] Mariek MP Vanden Abeele, "Digital Wellbeing as a Dynamic Construct," *Communication Theory* 31, no. 4 (2021): 932–55.

[12] Susanna Paasonen, "As Networks Fail: Affect, Technology, and the Notion of the User," *Television & New Media* 16, no. 8 (2015): 701–16.

[13] Lagerkvist, "Digital Existence: An Introduction."

[14] Merlyna Lim, "The Politics and Perils of Dis/Connection in the Global South," *Media, Culture & Society* 42, no. 4 (2020): 618–25, doi:10.1177/0163443720914032.

[15] Jörgen Skågeby, "Critical Incidents in Everyday Technology Use: Exploring Digital Breakdowns," *Personal and Ubiquitous Computing* 23, no. 1 (2019): 133–44, doi:10.1007/s00779-018-1184-8.

[16] David E. Nye, *When the Lights Went Out: A History of Blackouts in America* (Massachusetts: MIT Press, 2010).

[17] Nye, *When the Lights Went Out*.

1977 and the massive 2003 electricity outage across North America. He essentially argues that such large-scale infrastructural disruptions are not merely a technical occurrence but a social phenomenon that unveils complex sociocultural conditions. For instance, the 1965 blackout cultivated collective ethos and cooperation while the 1977 breakdown led to substantial incidents of looting and plunder.[18] Similar incidents occurred in other parts of the world but they received little academic attention in those countries. The biggest-ever electricity blackout occurred in India in 2012 which affected over 600 million people, effectively pushing half of the country's population into darkness for two days.[19] Trains stopped, people were stranded on streets and traffic reached a screeching halt. However, there are scarce scholarly investigations on how it affected the sociocultural and psychological state of the population.

Telephone networks are another facet of connectivity that is directly correlated with the sociocultural makeup of societies. In 1975, a fire broke out in New York Telephone Company's major switching centre, leaving majority of the residents disconnected from the world for 23 days. Wurtzel and Turner studied this unusual occurrence and concluded that it prompted New Yorkers' shared feelings of isolation, exasperation and reduced control over their lives.[20] A similar situation was observed in New York when call traffic overload caused prolonged congestion in telephone networks in the backdrop of the 9/11 attacks.[21]

Nevertheless, modern technology has enabled rapid responses to restore normalcy in networks. For instance, cellular towers on wheels were deployed to undertake infrastructural recovery and rectify damages rapidly.[22] In contemporary times, the most disruptive breakdowns are associated with IT and digital networks. Prominent cases of IT outages are discussed in the subsequent sections.

Causes of Global IT Outages

Given the complexity of IT blackouts, a detailed and context-sensitive examination of their root causes is essential. A thorough assessment can equip relevant stakeholders with the insights needed to prevent recurrence and mitigate the cascading impacts

[18] Nye, *When the Lights Went Out*.

[19] Loi Lei Lai et al., "Investigation on July 2012 Indian Blackout," (paper presented at International Conference on Machine Learning and Cybernetics, China, 2013), 92–97, https://ieeexplore.ieee.org/abstract/document/6890450/.

[20] Alan H. Wurtzel and Colin Turner, "Latent Functions of the Telephone: What Missing the Extension Means," *MIT Press*, (1976), https://eric.ed.gov/?id=ED125026.

[21] Zayan El Khaled and Hamid Mcheick, "Case Studies of Communications Systems during Harsh Environments: A Review of Approaches, Weaknesses, and Limitations to Improve Quality of Service," *International Journal of Distributed Sensor Networks* 15, no. 2 (2019), doi:10.1177/1550147719829960.

[22] El Khaled and Mcheick, "Case Studies of Communications Systems during Harsh Environments."

such disruptions can have on the digitality or digital functioning of governments, organisations, and the public.

Technical Factors

Technical factors may be characterised by but not limited to power supply, cooling systems, third-party providers, hardware/software and networking equipment. Uptime Institute's *Annual Outage Analysis Report 2024* reveals that a whopping 95% of IT outages are attributed to technical factors: interrupted power supply (52%), cooling equipment failure (19%), third-party provider issues (9%), hardware/software malfunction (8%) and networking equipment disruptions (7%).[23] Notably, the Google Cloud Outage 2019 was caused by a software misconfiguration[24] whereas the Microsoft Outage 2024 originated from a technical glitch in a third-party provider named CrowdStrike.[25]

The absolute preponderance of technical malfunction is a testament to the fact that technological advancements are prone to innate gaps and anomalies that are yet to be addressed through R&D. Mere emphasis on advancements, without adequately providing for contingencies, may be counterproductive to the seamless functioning of DPI.

Fire and Fire Suppression

Incidents involving fire outbreaks and gas-based fire suppression systems can have severely detrimental consequences for digital infrastructure. The overheating of equipment or lightning strikes could ignite the equipment which may engulf the whole infrastructure. It is crucial to note that fire breakouts and fire suppressing attempts are responsible for approximately 3% of IT blackouts globally.[26] For instance, an accidental release of fire suppression gas led to Microsoft's Azure cloud outage in 2017.[27] Thus, no matter how sophisticated the IT systems are, they are as vulnerable to natural vulnerabilities as simple urban infrastructure. While fire incidents caused by arsonist elements have not yet been reported, they cannot be ruled out as potential triggers for future digital crises.

Cyber-Attacks

The digital domain has increasingly become a strategic battleground for malicious actors seeking to exploit system vulnerabilities. Given the deeply interconnected

[23] Donnellan and Lawrence, *Annual Outage Analysis 2024*, 7.

[24] Google, "Google Cloud Status Dashboard," June 6, 2019, https://status.cloud.google.com/incident/cloud-networking/19009.

[25] Milmo et al., "Slow Recovery from IT Outage Begins as Experts Warn of Future Risks."

[26] Donnellan and Lawrence, *Annual Outage Analysis 2024*, 7.

[27] Yevgeniy Sverdlik, "Microsoft Says Azure Outage Caused by Accidental Fire-Suppression Gas," *Data Center Knowledge*, October 5, 2017, https://www.datacenterknowledge.com/outages/microsoft-says-azure-outage-caused-by-accidental-fire-suppression-gas-release.

architecture of DPI, the compromise of a single node can trigger cascading failures across the entire ecosystem. However, despite their destructive potential and visibility, cyber-attacks remain among the less frequent causes of global IT outages, suggesting that infrastructural fragilities and technical failures pose even greater systemic risks. Evidently, a mere 1% of incidents of IT blackouts are caused by cyber-attacks.[28] Having the capability to cripple IT networks, these could be marked by ransomware attacks or Denial of Service (DoS) attacks. For instance, the WannaCry ransomware attack by a hacker group called 'Shadow Brokers' intruded into approximately 300,000 devices across 150 countries.[29] Additionally, a DoS attack prompted the Sony PlayStation Network Outage in 2011, compromising the private data of 77 million users worldwide.[30] Although cyber-attacks might not be as frequent as technical factors causing an IT meltdown, their occurrence raises critical questions regarding the evolving national security spectrum in the era of Industry 4.0.

Human Error

To err is human but to err in a heavily interconnected DPI reflects the inability of humans to keep pace with technological advancements. The Uptime Institute terms human error as a 'contributing factor' rather than a primary one in causing around two-thirds to four-fifths of all IT meltdown incidents.[31] Prevailing instances of human error may be indicative of inadequacy of training, failure to follow procedures and staff fatigue. Debate regarding the need to curtail human error came to the global fore when a faulty command by Facebook's (Meta) engineers disconnected the company's data centres from the rest of the world, effectively leading to what was termed as the 'Facebook Outage' in 2021.[32] Therefore, human error as one of the causes of IT blackouts deserves as much policy attention as the rest of the causes.

Prominent Cases of Global IT Outages

Global-scale IT blackouts often originate from single points of failure within Big Tech firms that exert substantial control over global digital networks. Given their far-reaching impact, it is imperative to examine major IT meltdowns that plunged critical systems worldwide into disarray.

[28] Donnellan and Lawrence*, Annual Outage Analysis 2024*, 7.

[29] Maxat Akbanov, Vassilios G. Vassilakis, and Michael D. Logothetis, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms," *Journal of Telecommunications and Information Technology*, no.1 (2019), 114, https://bibliotekanauki.pl/articles/309353.pdf.

[30] Liana B. Baker and Jim Finkle, "Sony PlayStation Suffers Massive Data Breach," *Reuters*, April 27, 2011, https://www.reuters.com/article/technology/sony-playstation-suffers-massive-data-breach-idUSTRE73P6WB/.

[31] Donnellan and Lawrence, *Annual Outage Analysis 2024*, 9.

[32] Santosh Janardhan, "More Details about the October 4 Outage," *Engineering at Meta*, October 5, 2021, https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/.

Sony PlayStation Network Outage | 2011

The gaming community woke up to unsettling news in 2011 when Sony's PlayStation Network (PSN) was heavily compromised, leaving the global conglomerate in turmoil. Launched in 2006, PSN is essentially a digital entertainment service that offers games, media and an online marketplace to users worldwide. On April 17, it fell prey to a DoS cyber-attack that led to the breach of around 77 million users' data such as names, passwords, email addresses, physical addresses and credit card details.[33] The incident uncovered the innate vulnerabilities and technical shortcomings in Sony's digital PSN. Sony's failure to promptly disclose the attack, coupled with the extended three-week suspension of the PSN, worsened the crisis and undermined stakeholder confidence.[34]

Intrusions of such massive scale often take financial toll on a company, not to mention the loss of prestige and erosion of user confidence. Sony incurred direct losses of approximately USD 171 million and indirect losses of over USD 1 billion, while it became a target of online rage and criticism by users.[35] The fallout intensified as Sony faced a series of lawsuits aimed at attributing legal responsibility for the breach. A notable case, *Kristopher Johns v. Sony*, accused the company of gross negligence in data protection, specifically its failure to implement adequate firewall safeguards and maintain a robust cybersecurity framework.[36] Although Sony upgraded its encryption protocols and enhanced cyber defence mechanisms, it was targeted yet again through DoS attacks in 2014 and 2015, though these were not as destructive as the one in 2011.[37] To date, the hacker/s behind these cyber assaults have not been identified.

Google Cloud Outage | 2019

The global IT meltdown in 2019 emanated from one of the integral elements of Google's DPI: Google Cloud which is essentially a leading cloud service provider that offers storage, computing and networking tools to users as well as organisations worldwide. On June 2, Google Drive, G Suite, YouTube and other Google Cloud-hosted applications experienced severe congestion for hours, starting from Eastern US and quickly spreading to users globally.[38] As reported by Google, it was primarily caused by 'two normally-benign misconfigurations' that led to cascading disruptions.[39] The

[33] Baker and Finkle, "Sony PlayStation Suffers Massive Data Breach."

[34] Tom Phillips, "Five Years Ago Today, Sony Admitted the Great PSN Hack," *Euro Gamer*, April 26, 2016, https://www.eurogamer.net/sony-admitted-the-great-psn-hack-five-years-ago-today.

[35] Sigi Goode et al., "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony Playstation Network Breach," *MIS Quarterly* 41, no.3 (2017), 704.

[36] "Kristopher Johns vs. Sony" (United States District Court: Northern District of California, 2011), accessed November 07, 2024, http://static1.1.sqspcdn.com/static/f/201542/11950208/1303927115923/JohnsvSony-%C2%AD-Complaint-%C2%AD-FINAL.pdf?token=CO01uT6f9Rp8IngDoFL6Ibts2bc%3D.

[37] Matt Peckham, "Is It Really Time to Abandon Sony's PlayStation Network?" *TIME*, February 3, 2015, https://time.com/3693575/sony-playstation-outages-down/.

[38] Google, "Google Cloud Status Dashboard."

[39] Google, "Google Cloud Status Dashboard."

dependency of global users on such centralised systems of Big Tech companies aptly explains the domino effect of the outage and the dynamics of involuntary digital disconnection.

Although the company did not release an estimate of financial losses, it reported a 2.5% viewership drop in YouTube and a 30% traffic reduction in Google Cloud Storage.[40] What remains particularly concerning is the absence of any effort by international bodies or national authorities to assess user-end losses or to initiate legal action against the company for negligence or technical failings. The incident also brings to the fore pressing questions about the reliability of 'highly-automated', centralised cloud infrastructures that operate with minimal human oversight.[41]

Facebook Outage | 2021

The year 2021 was Meta/Facebook's turn to be at the epicentre of another global IT outage. On October 4, Facebook and its overarching family of applications such as WhatsApp, Messenger, and Instagram along with third-party applications were rendered inaccessible to billions of people worldwide for over six hours.[42] The blackout was a considerable source of distress for users and businesses that relied on these platforms for communication and commercial purposes. Facebook's investigation concluded that, during routine maintenance, a faulty command by its engineers disconnected the company's data centres from the rest of the world.[43] Facebook's internal audit protocols are designed to identify and preclude such commands from taking effect but 'a bug in that audit tool prevented it from properly stopping the command.'[44] Sarah Aoun, Vice President for security at the Open Technology Fund, labelled this blackout as 'a big infrastructure collapse,'[45] reflecting the fact that Facebook is not only an essential facet of contemporary DPI but also a detrimental entity for its integrity.

Forbes reported that the outage cost Facebook around USD 65 million whereas Zuckerberg's net worth plummeted by approximately USD 5.9 billion.[46] Similar to

[40] Google Cloud, "An Update on Sunday's Service Disruption," June 4, 2019, https://cloud.google.com/blog/topics/inside-google-cloud/an-update-on-sundays-service-disruption.

[41] Rich Miller, "Google Outage Sharpens Focus on Cloud Network Reliability," *Data Center Frontier*, June 4, 2019, https://www.datacenterfrontier.com/featured/article/11429579/google-outage-sharpens-focus-on-cloud-network-reliability.

[42] Sheila Dang, "Maintenance Error Caused Facebook's 6-Hour Outage, Company Says," *Reuters*, October 6, 2021, https://www.reuters.com/technology/facebook-says-maintenance-error-caused-mondays-6-hour-outage-2021-10-05/.

[43] Janardhan, "More Details about the October 4 Outage."

[44] Janardhan, "More Details about the October 4 Outage."

[45] Eileen Guo and Patrick Howell O'Neill, "Millions of People Rely on Facebook to Get Online. The Outage Left Them Stranded.," *MIT Technology Review*, October 5, 2021, https://www.technologyreview.com/2021/10/05/1036479/facebook-global-outage/.

[46] Abram Brown, "Facebook Lost About $65 Million During Hours-Long Outage," *Forbes*, October 5, 2021, https://www.forbes.com/sites/abrambrown/2021/10/05/facebook-outage-lost-revenue/.

trends observed in the previous outage, there are no credible estimates on how much losses users and businesses suffered globally. This phenomenon also points to gaps in international law and multilateral frameworks that offer little legal recourse to hold Big Tech accountable for such episodes of disruptions that take a toll on the financial, social and psychological well-being of people.

Microsoft Windows Outage | 2024

The more the world becomes digitalised over the years, the greater the global scale of outages it endures. On July 19, 2024, systems running on Microsoft's Windows operating system were frozen by a 'blue screen of death' triggered by what is now labelled as the 'largest outage in history.'[47] Multiple sectors across the world such as aviation, banking, healthcare and media were heavily disrupted. The source of the blackout was the Falcon cyber security software of CrowdStrike – a third-party cyber security provider employed by Microsoft to secure Windows. A faulty update by CrowdStrike to the Falcon software froze the Windows which rapidly morphed into a cascading IT blackout across the globe.[48]

The scale and extent of the damage is unlike anything seen in history. Owing to these reasons perhaps, the scrutiny aimed at Microsoft and CrowdStrike was greater than that aimed at companies involved in previous outages. Hence, efforts were made worldwide to measure the degree of damage inflicted upon users and organisations. Approximately 8.5 million devices crashed while Fortune500 companies, excluding Microsoft, suffered losses worth over USD 5 billion.[49] Healthcare and banking sectors were the hardest hit, recording estimated losses of USD 1.94 billion and USD 1.15 billion, respectively.[50] Additionally, nearly 3,300 flights were cancelled globally which ensued chaos in the aviation sector.[51] The incident also prompted debates on global supply chain security and how a single point of failure could uproot connected networks. Nevertheless, it is crucial to note that China remained largely unscathed from the blackout.[52] This could be attributed to China's growing policy inclination towards technological sovereignty and reliance on indigenous operating systems. The abovementioned information is presented below in tabular form.

[47] Milmo et al., "Slow Recovery from IT Outage Begins as Experts Warn of Future Risks."

[48] Milmo et al., "Slow Recovery from IT Outage Begins as Experts Warn of Future Risks."

[49] Brian Fung, "We Finally Know What Caused the Global Tech Outage - and How Much It Cost," *CNN*, July 24, 2024, https://www.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause/index.html.

[50] Fung, "We Finally Know What Caused the Global Tech Outage."

[51] Summer Raemason, "Summer Holidays Ruined & 3,000 Flights Grounded in Microsoft Outage," *Scottish Sun*, July 19, 2024, https://www.thescottishsun.co.uk/news/13184471/worldwide-microsoft-outage-trains-travel/.

[52] Wency Chen, Coco Feng, and Che Pan, "China Escapes Microsoft Outage, Thanks to Beijing's Tech Self-Sufficiency Drive," *South China Morning Post*, July 19, 2024, https://www.scmp.com/tech/big-tech/article/3271171/microsoft-outage-leaves-china-largely-untouched-tech-self-sufficiency-campaign-pays.

Table I: Global IT Outages in Recent Years

Sr No.	Outage	Cause	Losses
1	Sony PlayStation Network Outage, 2011	DoS Cyber Attack	-77 million users affected -USD 171 million loss incurred by Sony
2	Google Cloud Outage, 2019	Human error (software misconfigurations)	-30% traffic reduction in Google Cloud Storage -No estimate of financial losses incurred by Google
3	Facebook Outage, 2021	Human error (faulty computer command)	-3.5 billion users affected -USD 65 million worth of losses incurred by Facebook
4	Microsoft Windows Outage, 2024	Technical factor (glitch in cyber security software)	-8.5 million devices affected -USD 5 billion losses incurred by Fortune500 companies -No estimates to date of Microsoft's losses.

Source: Author's own.

Blueprint for Digital Resilience

Despite the complexity of the challenge, it is reasonable to argue that policy institutions at global, national, and organisational levels possess the analytical capacity and collective responsibility to develop effective, actionable solutions. What is needed is a clearly articulated policy blueprint that addresses vulnerabilities in digital infrastructure across multiple layers, from international protocols to institutional safeguards and individual digital hygiene.

Global Frameworks for Digital Resilience

IT meltdowns over the years have laid bare an unsettling reality: multilateral regulatory frameworks and international law have not been able to catch up with the accelerated pace of globalised digital networks. The dearth of mutually agreed and binding global norms undermines the principles of accountability, resilience and fairness in the face of digital crisis. The recent Global IT outage was labelled as a 'wake-up call about DPI,' reflecting the fact that the intangible nature of digital infrastructure, as opposed to physical infrastructure, makes it harder to govern and manage IT blackouts.[53] Nevertheless, states can initiate the formulation of multilateral treaties, ideally under the auspices of the United Nations, to reduce the likelihood of future large-scale IT disruptions. Such treaties should establish binding obligations for

[53] Weatherspoon and Gao, "The Great IT Outage of 2024 Is a Wake-up Call about Digital Public Infrastructure."

IT service providers and associated stakeholders to invest in the resilience, interoperability, and security of their digital infrastructure.

Given the global operational footprint and systemic influence of Big Tech firms, there is a growing argument for recognising them as relevant actors under the evolving landscape of international law, particularly in matters concerning digital infrastructure and cross-border disruptions. However, to date, no precedent exists of such entities being held accountable in any international tribunal for causing or enabling IT outages. As such, future multilateral treaties should enshrine the principle of corporate accountability in the digital domain and establish clear mechanisms, whether through the International Court of Justice (ICJ), ad hoc tribunals, or newly mandated international arbitration forums, for pursuing legal recourse in cases of gross negligence or failure to maintain critical infrastructure standards.

The digital economy remains disproportionately dominated by technologically advanced countries,[54] rendering the Global South heavily dependent on the DPI of the Global North and thereby increasingly vulnerable to single points of failure originating from these systems. Bridging this global digital divide must be prioritised as a shared international responsibility. In recognition of this, the UN Secretary-General has proposed the Global Digital Compact,[55] a framework that could be formalised through UN resolutions to promote equitable digital development. However, while multilateral efforts are essential, it is equally imperative for individual states, particularly those in the Global South, to invest in their own digital resilience strategies, including infrastructure redundancy, local capacity building, and regulatory safeguards.

National Frameworks for Digital Resilience

The prevention of global IT outages is not only a technical exercise but also a policy endeavour that countries should employ in letter and spirit. Importantly, countries may emulate the US government's Network Outage Reporting System (NORS)[56] which mandates service providers to report outages within 120 minutes, followed by a detailed report submitted to the government within three days. The purpose is to take all stakeholders on board and ensure transparency in order to minimise risks to public life and property.

Moreover, technological sovereignty is gaining traction as a policy choice for various economic and security reasons.[57] It is essentially aimed at indigenisation and strategic control over technologies that may be imperative for preventing global IT outages.

[54] UN Conference on Trade and Development, *Technology and Innovation Report 2023*, report (New York: UNCTAD, 2023), https://unctad.org/system/files/official-document/tir2023_en.pdf.

[55] United Nations, "Global Digital Compact," accessed November 22, 2024, https://www.un.org/en/summit-of-the-future/global-digital-compact.

[56] Federal Communications Commission, "Network Outage Reporting System (NORS)," accessed November 22, 2024, https://www.fcc.gov/network-outage-reporting-system-nors.

[57] Francesco Crespi et al., "European Technological Sovereignty: An Emerging Framework for Policy Strategy," *Intereconomics* 56, no. 6 (2021), 6, doi: https://doi.org/10.1007/s10272-021-1013-6.

This is substantiated by the fact that China was the least harmed in the recent global crisis triggered by the Windows blackout.[58] The country has its indigenous operating system which is least susceptible to external single points of failure. Hence, developing countries may undertake multi-stakeholder engagement aimed at devising policies to diversify their key sources of digital technology and opt for indigenous alternatives.

Data localisation policies are increasingly seen as a means to advance technological sovereignty, particularly for countries in the Global South. The geographic concentration of data centres in the Global North not only reflects the persistent global digital divide but also raises systemic concerns about the risk of cascading outages stemming from failures in centralised DPI. The 2021 global IT disruption caused by a malfunction in Facebook's data centres illustrates the vulnerabilities inherent in such centralised architectures, where a single point of failure can paralyse services used by billions worldwide.[59] Therefore, countries ought to prioritise building indigenous data centres to localise data flows and prevent the cascading effects of IT blackouts. Indigenous data centre infrastructure would essentially require seamless internet connectivity, uninterrupted power supply, cooling systems and requisite hardware and software. BRICS countries are making significant headways in data localisation and data sovereignty that could be emulated by other countries as per their own techno-social contexts.[60] Needless to say, the implementation of these policies would require institutional strength and a whole-of-government approach.

Organisational Frameworks for Digital Resilience

Organisations and corporations often occupy a dual role in IT outages, both as originators and as victims of cascading disruptions. The cases discussed above exemplify instances where corporations were positioned at the initial node of digital crises, highlighting systemic vulnerabilities within core infrastructure. These incidents underscore the urgent need for robust contingency protocols, risk mitigation frameworks, and remedial mechanisms to prevent the recurrence of similar outages in the future. For instance, after the disastrous IT outage triggered by the Windows blackout, Microsoft outlined technical steps such as extensive testing frameworks and a backup system to prevent similar incidents.[61] However, it is unclear if these steps are robust enough to mitigate blackouts in future. Therefore, both global and national regulatory frameworks should scrutinise these organisations and the effectiveness of their digital resilience protocols. These frameworks should mandate third-party

[58] Chen, Feng and Pan, "China Escapes Microsoft Outage."

[59] Janardhan, "More Details about the October 4 Outage."

[60] Luca Belli, Water B. Gaspar, and Shilpa Singh Jaswant, "Data Sovereignty and Data Transfers as Fundamental Elements of Digital Transformation: Lessons from the BRICS Countries," *Computer Law & Security Review* 54 (2024): 106017.

[61] David Weston, "Windows Security Best Practices for Integrating and Managing Security Tools," *Microsoft Security Blog*, July 27, 2024, https://www.microsoft.com/en-us/security/blog/2024/07/27/windows-security-best-practices-for-integrating-and-managing-security-tools/.

evaluations to ascertain the robustness of their remedial measures. In this regard, experts have proposed a *'Systemic Safety Management System'* (SSMS) that visually models interdependence among digital networks.[62] SSMS continually scans critical infrastructure for anomalies and conducts thorough risk assessments. Simultaneously, it accords adaptability and resilience to systems during any disruption.

Organisations at the receiving end of IT outages often bear the most immediate and severe consequences. To strengthen their resilience, such entities should align their operational strategies with national policy objectives aimed at achieving technological sovereignty. Specifically, reducing dependence on dominant proprietary operating systems such as Windows and iOS and transitioning toward open-source alternatives like Linux, can diversify risk, enhance customizability, and reduce vulnerability to single-vendor failure. Additionally, regular vulnerability assessments and testing should be conducted to plug any gaps therein. Artificial Intelligence (AI) and Machine Learning may be leveraged for predictive maintenance to identify and rectify vulnerabilities.[63] Importantly, advanced cyber security mechanisms need to be put in place to protect against potential breaches and malicious attempts. In this regard, AI-driven testing, advanced encryption tools and multi-factor authentication may be prudent measures. However, organisational frameworks would not be effective without well-trained human resources.

Individual Training and Awareness

Governments, organisations and corporations are spearheaded by the collective effort of individuals who adhere to a set of standard procedures in order to pursue shared objectives. Any lapse or shortcoming in individual action might be detrimental not only in terms of causing an IT blackout but also with regard to preventing similar occurrences in the future. The Facebook Outage was set off by human error of a few engineers who issued a faulty command. Therefore, it is crucial for digital firms to cultivate a culture of continual training and individual responsibility. Professionals should be offered comprehensive training programmes consisting of workshops, webinars and certifications focused on digital resilience, cyber security and crisis management. To be precise, they could be trained in diagnostic mechanisms such as Batch Server Outage Diagnostics (BSODiag).[64] It is a diagnostic as well as analytical framework with twofold tasks: root cause localisation and failure propagation path inference. The former identifies root cause of the outage while the latter minimises

[62] Jaime Santos-Reyes, "Planning for the Unexpected: Exploring the 2024 Global IT Outage (GITO) Impact on Critical Infrastructures," *Sustainable Futures* 9, (2025).

[63] Lucian Florin Ilca, Ogruţan Petre Lucian, and Titus Constantin Balan, "Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response," *Sensors* 23, no.15 (2023).

[64] Tao Duan et al., *BSODiag: A Global Diagnosis Framework for Batch Servers Outage in Large-Scale Cloud Infrastructure Systems*, report (New York: Cornell University, 2025), http://arxiv.org/abs/2502.15728.

cascading failures across systems by accounting for historical disruptions as well as current vulnerabilities among systems.

People working in government institutions and non-tech organisations need to be given basic awareness of digital technologies and the intricate nature of globalised IT networks. Additionally, employees should undergo simulations and mock exercises so that they may be able to prevent and respond to potential digital disruptions. Particularly, IT firms should have an online feedback mechanism through which employees can report and identify anomalies. In essence, a digital infrastructure and organisational framework is only as strong as the human resource handling it. Human error cannot be completely eliminated because to err is human but it can be minimised to a substantial extent through well-thought training and awareness programmes.

Conclusion

The increasingly blurred boundaries between digitality and sociality demand a more nuanced understanding of how disruptions in the digital domain reverberate across the social fabric. In this context, developing a robust technical and analytical understanding of global IT outages becomes critically important not only for diagnosing their causes but also for anticipating their broader societal implications. A closer assessment of the breakdowns in DPI over the years reflects a gradual trend towards higher intensity and scope of the damages inflicted worldwide. A single point of failure is now raising legitimate questions regarding the global population's over-reliance on a few Big Tech companies. Furthermore, although IT blackouts are predominantly attributed to technical malfunctions and software/hardware issues, cyber-attacks and human error also require due assessment.

Countries/organisations should align their policy initiatives with the goal of technological sovereignty to acquire greater control over domestically/internally used technologies, explore indigenous alternatives and empower their human resource to guard against disruptive occurrences. However, mere national, organisational and individual remedial measures would not suffice to guard the digital as well as social frontiers against the outbreak of disruptions. Given the scale of implications, there is a pressing need for global frameworks that prioritise legal and financial accountability and resilience. Despite the inherent unpredictability of DPI, coordinated efforts by national governments and international institutions can strengthen safeguards, reduce systemic risks, and ensure more dependable digital infrastructure worldwide.

ABOUT THE AUTHOR

***Shah Muhammad** is a Research Assistant at the Centre for Aerospace & Security Studies (CASS), Islamabad. His research interests include emerging technologies, national security, defence modernisation and global governance. Previously, he completed a research fellowship with Hanns Seidel Foundation (HSF). Shah Muhammad is also member of a global policy network 'Future Leaders Connect' (FLC), jointly hosted by British Council and Cambridge University. He is a gold medallist in MPhil Peace and Conflict Studies from the National University of Sciences and Technology (NUST), Islamabad.*

ABOUT CASS

The Centre for Aerospace & Security Studies (CASS), Islamabad, was established in 2018 to engage with policymakers and inform the public on issues related to aerospace and security from an independent, non-partisan and future-centric analytical lens. The Centre produces information through evidence-based research to exert national, regional and global impact on issues of airpower, emerging technologies and security.

VISION

To serve as a thought leader in the aerospace and security domains globally, providing thinkers and policymakers with independent, comprehensive and multifaceted insight on aerospace and security issues.

MISSION

To provide independent insight and analysis on aerospace and international security issues, of both an immediate and long-term concern; and to inform the discourse of policymakers, academics, and practitioners through a diverse range of detailed research outputs disseminated through both direct and indirect engagement on a regular basis.

CORE AREAS OF RESEARCH

Aerospace

Emerging Technologies

Security

Strategic Foresight

CASS www.casstt.com
CENTRE FOR AEROSPACE
& SECURITY STUDIES, ISLAMABAD
Independence | Analytical Rigour | Foresight

Old Airport Road, Islamabad, Pakistan
cass.thinkers@casstt.com
in Centre for Aerospace & Security Studies
☎ +92 051 5405011
www.casstt.com
cassthinkers
@CassThinkers
cass.thinkers