

Arab Reform Initiative

TECH, POWER & CONFLICT DOSSIER

CONNECTIVITY AS SURVIVAL: INTERNET SHUTDOWNS, INFRASTRUCTURAL VIOLENCE, AND THE LIMITS OF CENSORSHIP FRAMEWORKS IN ARMED CONFLICT

Kassem Mnejja

Published by:

Arab Reform Initiative
The Arab Reform Initiative is an independent Arab think tank working with expert partners in the Middle East and North Africa and beyond to articulate a home-grown agenda for democratic change and social justice. It conducts research and policy analysis and provides a platform for inspirational voices based on the principles of diversity, impartiality, and gender equality.
https://www.arab-reform.net/

About the author

Kassem Mnejja is a digital rights researcher and campaigner, focusing on internet shutdowns, surveillance accountability, and freedom of expression across the MENA region. Kassem is Senior MENA Campaigner at Access Now. Previously, Kassem was a fellow with the Tahrir Institute for Middle East Policy (TIMEP) focusing on cyberspace in MENA and has been working for year with local grassroots organizations and civil society across the MENA region. The views expressed here are the author's own.

Disclaimer:

The information and views set out in this report are those of the author(s) and do not necessarily reflect the views of the Arab Reform Initiative, its staff, its board or its funders.

© 2026 Arab Reform Initiative.

This license allows re-users to distribute, remix, adapt, and build upon the material in any medium or format for non-commercial purposes only, and only so long as attribution is given to the creator. If you remix, adapt, or build upon the material, you must license the modified material under identical terms.

Cover photo: Doctors work as basic healthcare services are gradually becoming accessible again for returning civilians and local residents as hospitals resume operations in Khartoum, Sudan, on August 6, 2026.

© Nezar Abdallah Basheer/Anadolu Images

This paper is a part of the Tech, Power, and Conflict in MENA dossier, coordinated and edited by Nada Kabbary Mousa (Mozilla Fellow 2024-2026) and Andrew Findell-Aghnatios (Program Lead - Tech & Society) and co-funded by the Mozilla Foundation and ARI.

November 2026

Table of Contents

Introduction 4

Scholarship Review: How Internet Shutdowns Are Conceptualized 6

Theoretical Framework: From Censorship to Infrastructural Violence 9

- Identifying the Gaps 9
- From Censorship to Infrastructural Violence: Sudan as a Theory-Generating Site 10

Infrastructural Violence as an Extension of Structural Violence 12

Conclusion: Digital Infrastructure and the Future of Conflict 14

Introduction

On 15 April 2023, armed conflict erupted between the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF) across Khartoum and other Sudanese cities. In the weeks and months that followed, civilians lost access not only to safety but to the digital infrastructures on which their survival had come to depend; mobile banking systems through which remittances arrived,[1,2] humanitarian coordination platforms through which aid was organized,[3,4] and safety verification tools through which civilians identified safe routes and verified evacuation routes away from active fighting.[5] Civilian connectivity collapsed through a combination of means: shutdown orders and service suspensions imposed by the warring parties, and the physical destruction or seizure of telecommunications infrastructure. Because both produced the same effect on civilians, the distinction between them, while legally and evidentially relevant, is analytically secondary to the patterned effect on civilian life, a point this paper argues has consequences for how shutdowns in conflict are theorized and contested. Throughout this paper, "connectivity disruption" refers to the loss, degradation, or selective restoration of connectivity on which the civilian population depends, whatever its cause. Sudan was not unprecedented in this regard. In Yemen, Gaza, Myanmar, and Ukraine, connectivity disruption has become a defining feature of contemporary armed conflict.[6,7] Yet the dominant analytical frameworks for understanding communication shutdowns in conflict were not designed with internet-dependent societies in mind.

The prevailing literature conceptualizes internet shutdowns primarily as instruments of censorship: tools deployed by states to suppress dissent, restrict political communication, and manage informational flows during moments of regime vulnerability. This framing has generated important insights and continues to support vital advocacy,[8,9,10] but it rests on three further assumptions. It treats shutdowns as isolated, time-bound events, such as a blackout during an election or a protest. It treats connectivity primarily as a medium of communication. And it treats the main harm as a violation of rights rather than a material deprivation. These assumptions do not necessarily hold in contemporary armed conflict. When connectivity mediates financial transactions, humanitarian logistics, and the basic conditions of survival, its disruption cannot be adequately described only as censorship, meaning that a different theoretical vocabulary is required. As such, this paper argues that disruptions of the connectivity on which civilians depend cannot

1 ACAPS, *Implications of Financial Blockages in Sudan*, August 2023, available at https://www.acaps.org/file-admin/Data_Product/Main_media/20230811_ACAPS_thematic_report_in_Sudan_implication_of_financial_blockages.pdf (ACAPS, "Implications of Financial Blockages in Sudan").

2 Kassem Mnejja, "Internet in Conflict: Sudan's Battle for Connection", Tahrir Institute for Middle East Policy (TIMEP), 19 September 2024, available at https://timep.org/2024/09/19/internet-in-conflict-sudans-battle-for-connection/ (Mnejja, "Internet in Conflict").

3 Amnesty International, "Sudan: Internet Shutdown Threatens Delivery of Humanitarian and Emergency Services", March 2024, available at https://www.amnesty.org/en/latest/news/2024/03/sudan-internet-shutdown-threatens-delivery-of-humanitarian-and-emergency-services/ (Amnesty International, "Sudan: Internet Shutdown Threatens Delivery of Humanitarian and Emergency Services").

4 OCHA, *Sudan Humanitarian Update*, December 2023, available at https://www.unocha.org/publications/report/sudan/sudan-humanitarian-update-7-december-2023

5 Amnesty International, "Sudan: Internet Shutdown Threatens Delivery of Humanitarian and Emergency Services".

6 Al Jazeera, "Conflicts Trigger Globe's Highest Rate of Internet Shutdowns in 2024: NGO", 24 February 2025, available at https://www.aljazeera.com/news/2025/2/24/conflicts-trigger-globes-highest-rate-of-internet-shutdowns-in-2024-ngo

7 Casey Coombs, "In Yemen, the Internet Is a Key Front in the Conflict", Coda Story, 10 March 2020, available at https://www.codastory.com/authoritarian-tech/yemen-internet-conflict/

8 Human Rights Watch, "Shutting Down the Internet to Shut Up Critics", 2020, available at https://www.hrw.org/world-report/2020/country-chapters/global-5

9 Zach Rosson and Felicia Anthonio, *Rising repression meets global resistance: Internet shutdowns in 2025*, Access Now, March 2026, available at https://www.accessnow.org/wp-content/uploads/2026/03/KeepItOn-Internet-Shutdowns-2025-Annual-Report.pdf (Rosson & Anthonio, *Rising repression meets global resistance*).

10 Anuradha Bhasin v. Union of India, (2020) 3 SCC 637, Supreme Court of India, Writ Petition (Civil) No. 1031 of 2019, decided 10 January 2020, available at https://www.sci.gov.in/supremecourt/2019/40453/40453_2019_Judgement_10-Jan-2020.pdf (Anuradha Bhasin v. Union of India).

be adequately understood as acts of censorship, because they disrupt not only communication but also the financial, logistical, and humanitarian systems on which civilian survival depends. In the digital age, disconnecting civilians from objects, goods, and services essential for their survival is a matter of humanitarian protection, even more so than of freedom of expression. The concept of infrastructural violence, developed here as an extension of Galtung's structural violence framework[11] into the digital domain, offers a better-suited account of this harm, grounded in survival and structural pattern rather than expression and singular intent.

This paper proposes the concept of infrastructural violence as the manipulation, degradation, or withholding of digital infrastructure on which the civilian population depends – whether deliberate or structurally produced – in ways that produce structured vulnerability and mediate survival. It presents the concept and an accompanying research agenda as a first theoretical step but does not yet test the framework empirically. The concept extends Johan Galtung's foundational framework of structural violence into the digital domain. For Galtung, structural violence refers to harm produced not by direct physical force but by institutional arrangements that systematically constrain individuals' access to basic needs: harm that is patterned, cumulative, and embedded in governance systems, and for which no identifiable actor need be responsible.[12] The resemblance to the legal category of crimes against humanity, which also addresses widespread or systematic harm to civilian populations, is limited. While the category attaches criminal responsibility to identifiable perpetrators, infrastructural violence describes the structure of the harm itself. The present paper retains this analytical logic while departing from it in one key respect by proposing that intentionality be treated as one possible mechanism of infrastructural violence as opposed to its defining criterion. What the concept requires is not proof of deliberate command, nor of a plan or policy in the sense used in international criminal law, but evidence that the pattern of disruption and restoration systematically tracks the distribution of military and political control. This is a correlation observable in outcomes, not a purposive design attributed to any actor. The distinction matters in conflict settings such as Sudan, where deliberate shutdowns and infrastructure destruction produce comparable civilian harm regardless of which mechanism generated them.

Sudan is the paper's primary analytical site and is used as a theory-generating site, given its nature as a context in which conditions increasingly common across contemporary conflicts are present in concentrated form, and in which the limitations of the censorship framework become unmistakably visible. The four features that make Sudan analytically productive – the layering of deliberate shutdown and infrastructure damage, with disruption and restoration that track territorial control; the centrality of connectivity to financial survival; the stratification of access produced by alternative satellite systems; and contested attribution between the warring parties – are each examined as pressure points that the existing literature cannot adequately account for.

Each pressure point challenges one or more of the assumptions identified in the scholarship review, all of which build on the first, that shutdowns are instruments of speech suppression. Layered mechanisms challenge the assumption that shutdowns are discrete events; the centrality of connectivity to financial survival challenges the assumption that connectivity is primarily a medium of communication; stratification challenges the related assumption that shutdowns are uniform, population-wide events; and contested attribution challenges the assumption that the primary normative harm is legal, since legal accountability depends on attributing a violation to an identifiable actor.

The paper proceeds as follows. The first section reviews the dominant literature on internet shutdowns, organized around four shared assumptions that together define its analytical limits. This is then followed by a development of the theoretical framework, positioning Sudan as a theory-generating site, constructing the concept of infrastructural violence, and specifying the analytical chain it generates. Finally, the paper concludes by drawing out the broader implications of the framework for research, accountability, and humanitarian response; with particular attention to the conditions now visible in Gaza and Lebanon; and by identifying the research agenda the concept opens.

11 Johan Galtung, "Violence, peace, and peace research", *Journal of Peace Research* 6, no. 3 (1969), pp. 167-191, available at https://doi.org/10.1177/002234336900600301 (Galtung, "Violence, peace, and peace research").

12 Galtung, "Violence, peace, and peace research".

Scholarship Review: How Internet Shutdowns Are Conceptualized

The dominant literature on internet shutdowns, spanning political science, media studies, international relations, law, and economics, rests on a set of shared assumptions that have shaped both research agendas and advocacy frameworks. Across these fields, shutdowns are primarily understood as instruments of speech suppression; analysis is typically event-based, tied to discrete moments of political unrest rather than to enduring systemic patterns; connectivity is treated as a medium of communication and expression rather than as a life-sustaining infrastructure; and the normative emphasis falls on legal rights rather than on material survival. These assumptions have generated important insights, but they also produce systematic blind spots – particularly in contexts of civil war and armed conflict, where connectivity is increasingly entangled with financial systems, humanitarian logistics, and the basic conditions of civilian survival.[13,14] Identifying these assumptions as assumptions, rather than as neutral analytical starting points, is the first step toward understanding the gaps in the existing literature.

The first assumption, that shutdowns are primarily instruments of speech suppression, runs through the core of the field. Political science and media studies frame shutdowns as tools deployed during moments of regime vulnerability, used as tactics for restricting dissent, containing protest, and managing risk during elections, uprisings, or large-scale demonstrations.[15] Literature on digital authoritarianism extends this logic by situating internet shutdowns within a broader toolkit of state power, examining how governments deploy connectivity control alongside surveillance infrastructure, disinformation campaigns, and platform manipulation to consolidate political authority.[16,17] Within this broader literature on digital authoritarianism, election-focused studies treat shutdowns as strategic interventions in moments of heightened political contestation, analyzing them as mechanisms for manipulating information flows, restricting electoral transparency, and constraining opposition mobilization across autocratic and hybrid regimes.[18,19] Human rights literature reinforces this framing, treating shutdowns as violations of freedom of expression, access to information, and the right to peaceful assembly. Access Now, ARTICLE 19, Human Rights Watch, and UN experts have been instrumental in documenting the frequency and geographic distribution of internet shutdowns and in applying the standards of legality, necessity, and proportionality to specific national contexts. Access Now's documentation of Sudan's nationwide shutdown following the June 2019 massacre and

13 International Committee of the Red Cross (ICRC), "International Humanitarian Law and Connectivity Disruptions during Armed Conflict", July 2025, available at https://blogs.icrc.org/law-and-policy/2025/07/03/international-humanitarian-law-and-connectivity-disruptions-during-armed-conflict/.

14 ICRC, "Offline and in Danger: The Humanitarian Consequences of Connectivity Disruptions", July 2025, available at https://blogs.icrc.org/law-and-policy/2025/07/01/offline-and-in-danger-the-humanitarian-consequences-of-connectivity-disruptions/ (ICRC, "Offline and in Danger").

15 Phillip N. Howard, A. Duffy, D. Freelon, M. Hussain, W. Mari and M. Maziad, *Opening closed regimes: What was the role of social media during the Arab Spring?*, Project on Information Technology and Political Islam, 2011, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595096

16 Alina Polyakova and Chris Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese Models*, Brookings Institution, August 2019, available at https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

17 Steven Feldstein, *The rise of digital repression: How technology is reshaping power, politics, and resistance*, Oxford University Press, 2021.

18 Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India", SSRN working paper, 2019, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413

19 Matthias Grömping and Holly Ann Garnett, "Election-Related Internet Shutdowns in Autocracies and Hybrid Regimes", *Journal of Elections, Public Opinion and Parties* 33, no. 4 (2022), pp. 705-725, available at https://doi.org/10.1080/17457289.2022.2090950

the October 2021 military coup analyzed both episodes against these principles;[20,21] Human Rights Watch underscored Sudan's obligations under international human rights law, including the rights to freedom of expression and peaceful assembly;[22] a position reinforced by UN human rights experts who denounced the shutdown as a clear violation of international human rights law that cannot be justified under any circumstances;[23] and by ARTICLE 19, which specifically invoked Sudan's obligations under Article 19 of the ICCPR.[24] Legal scholarship similarly operates within this expressive framing, assessing shutdowns under constitutional and international human rights frameworks and emphasizing that blanket or indefinite disruptions are presumptively disproportionate restrictions on speech, including under principles derived from Article 19 of the ICCPR and constitutional emergency powers doctrines applied in national courts.[25] Across all of these fields, the organizing harm is the suppression of expression and information, and the organizing question is whether that suppression meets lawful standards.

The second assumption, that shutdowns are discrete events (that is, isolated, time-bound events with a clear trigger) rather than elements of broader patterns of governance or violence, shapes how the literature periodizes and analyzes connectivity disruption. Event-based analysis at times tends to treat shutdowns as uniform, population-wide events, overlooking differences in who loses connectivity and who retains it. This means that it is appropriate when shutdowns are genuinely episodic; for example, a coup might trigger a blackout, which would then end and let normal connectivity resume. But this analytical frame struggles when disruptions are prolonged, cumulative, or territorially uneven, as in contexts of armed conflict where connectivity loss may result from a combination of deliberate action, infrastructure destruction, and shifting frontlines. The economic costs literature illustrates both the value and the limits of event-based analysis. Studies estimating GDP losses, investment deterrence, and productivity declines[26] are valuable in demonstrating aggregate harm and bolstering advocacy arguments, but their aggregation abstracts away from the micro-level, cumulative implications of connectivity loss for individuals and communities whose access to income, health services, and safety information depends on networked infrastructure.

The third assumption, that connectivity is primarily a medium of communication, is perhaps the most consequential and the least examined. In conflict studies and cybersecurity scholarship, shutdowns and related network disruptions are typically treated as subordinate tactics within larger theories of cyber statecraft, analyzed as instruments of strategic signaling, deterrence, or information warfare rather than as civilian-facing governance measures.[27,28,29] This framing privileges state-to-state competition over the shared lived experience of civilian populations. Meanwhile, work in science and technology studies and infrastructure studies has shown how infrastructures organize social life by becoming invisible until they fail, revealing their political and distributive properties only in

20 Access Now, "#KeepItOn in Times of War: Sudan's Communications Shutdown Must Be Reversed Urgently", 9 February 2024, available at https://www.accessnow.org/press-release/keepiton-sudan-shutdown/ (Access Now, "#KeepItOn in Times of War").

21 Access Now, "Internet shutdowns and blockings continue to hide atrocities of military coup in Sudan", 23 November 2021, available at https://www.accessnow.org/press-release/update-internet-shutdown-sudan/ (Access Now, "Internet shutdowns and blockings").

22 Human Rights Watch, "Sudan: End network shutdown immediately", 12 June 2019, available at https://www.hrw.org/news/2019/06/12/sudan-end-network-shutdown-immediately (Human Rights Watch, "Sudan: End network shutdown immediately").

23 OHCHR, "Sudan: UN Experts Denounce Internet Shutdown, Call for Immediate Restoration", July 2019, available at https://www.ohchr.org/en/press-releases/2019/07/sudan-un-experts-denounce-internet-shutdown-call-immediate-restoration.

24 ARTICLE 19, "Sudan: Free Expression Must Be Protected amidst Violence", 10 May 2023, available at https://www.article19.org/resources/sudan-free-expression-amidst-violence/.

25 Anuradha Bhasin v. Union of India.

26 Deloitte, *The Economic Impact of Disruptions to Internet Connectivity: A Report for Facebook*, October 2016, available at https://www.deloitte.com/ug/en/Industries/tmt/perspectives/the-economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html

27 Thomas Rid, *Cyber war will not take place*, Oxford University Press, 2013 .

28 Lucas Kello, *The virtual weapon and international order*, Yale University Press, 2017.

29 Joseph S. Nye, "Deterrence and dissuasion in cyberspace", *International Security* 41, no. 3 (2017), pp. 44-71, available at https://doi.org/10.1162/ISEC_a_00266.

moments of breakdown.[30,31] Michael Mann's notion of infrastructural power further underscores the state's capacity to penetrate and coordinate society through material and administrative systems.[32] These theoretical resources remain largely underutilized in shutdown scholarship, even as they point toward exactly what the dominant literature cannot see: that connectivity infrastructure, like roads, water systems, or electrical grids, is constitutive of social life rather than merely facilitative of communication.

The fourth assumption, that the primary normative harm of shutdowns is legal rather than material, follows from the first three. When shutdowns are understood as speech restrictions triggered by discrete political events, the appropriate response is legal. Lawyers and human rights defenders are called to assess the restriction against proportionality standards, document the violation, and advocate for restoration. Classic political theory offers resources for a more expansive normative analysis that the shutdown literature has rarely mobilized systematically. Michel Foucault's concept of biopolitics directs attention to the governance of populations through the regulation of circulation, communication, and life-sustaining systems; read through this lens, shutdowns function not merely as speech restrictions but as techniques of population management, interrupting digital flows of information, remittances, humanitarian coordination, and medical communication.[33] Achille Mbembe's theory of necropolitics extends this by foregrounding the sovereign power to expose populations to conditions of slow death through infrastructural deprivation, a framework with direct relevance to contexts where connectivity loss isolates communities from emergency services and humanitarian aid.[34] Pierre Bourdieu's concept of symbolic violence offers a further analytical lens. For Bourdieu, symbolic violence is the power to impose meanings as legitimate while concealing the power relations that make that imposition possible, operating not through force but through the misrecognition of domination as something natural or necessary.[35] Applied to internet shutdowns, this framework explains how the bureaucratic and technocratic language through which shutdowns are routinely justified – invoked as security measures, temporary precautions, or public order interventions – functions not merely as justification but as a mechanism that renders extraordinary control socially intelligible and politically tolerable. Scholars working with Bourdieusian frameworks in digital contexts have shown how power relations are similarly embedded and naturalized within digital governance structures,[36] though the specific application of symbolic violence to the legitimation of internet shutdowns remains underexplored.

These frameworks are illuminating but carry theoretical commitments that limit their utility as the primary anchor for the present paper's argument. Necropolitics is particularly close in analysis to what this paper proposes in that it examines the exposure of populations to slow death through infrastructural means, which is precisely the harm that connectivity disruption in conflict produces. However, necropolitics remains organized around sovereign decision, or the deliberate political choice to expose certain populations to death while protecting others. In contexts such as Sudan's civil war, where the distinction between deliberate shutdown and war-induced infrastructure collapse is often impossible to establish at the level of individual events, a framework that requires the identification of a sovereign subject of that decision runs into its own attribution problem. I propose the concept of infrastructural violence as an extension of structural violence into the digital domain: the manipulation,

30 Susan L. Star, "The ethnography of infrastructure", *American Behavioral Scientist* 43, no. 3 (1999), pp. 377-391, available at https://doi.org/10.1177/00027649921955326.

31 Brian Larkin, "The politics and poetics of infrastructure", *Annual Review of Anthropology* 42 (2013), pp. 327-343, available at https://doi.org/10.1146/ANNUREV-ANTHRO-092412-155522.

32 Michael Mann, "The autonomous power of the state: Its origins, mechanisms, and results", *European Journal of Sociology* 25, no. 2 (1984), pp. 185-213, available at https://doi.org/10.1017/S0003975600004239

33 Michel Foucault, Security, Territory, Population: Lectures at the Collège de France, 1977-1978, edited by Michel Senellart, translated by Graham Burchell, Palgrave Macmillan, 2007.

34 Achille Mbembe, "Necropolitics", *Public Culture* 15, no. 1 (2003), pp. 11-40, available at https://doi.org/10.1215/08992363-15-1-11.

35 Pierre Bourdieu, *Language and symbolic power*, Harvard University Press, 1991.

36 G. Ignatow and L. Robinson, "Pierre Bourdieu: Theorizing the Digital", *Information, Communication & Society* 20, no. 7 (2017), pp. 950-966, available at https://doi.org/10.1080/1369118X.2017.1301519

degradation, or withholding of digital infrastructure on which the civilian population depends – whether deliberate or structurally produced – in ways that produce structured vulnerability and mediate survival. The concept of infrastructural violence developed in this paper draws on this tradition, keeping the framework of necropolitics to analyze the political stakes of connectivity while grounding it in a tradition that can operate without proof of sovereign command. What Galtung's framework provides, and what the present paper extends into the digital domain, is the capacity to identify structural harm through its cumulative pattern rather than through any singular act.

Taken together, these four assumptions – shutdowns as speech suppression; shutdowns as discrete events; connectivity as a medium of communication; harm as primarily legal – have generated a field well-equipped to analyze shutdowns as censorship and poorly equipped to analyze them as interventions in life-sustaining infrastructures. This is the gap the present paper addresses.

Theoretical Framework: From Censorship to Infrastructural Violence

Identifying the Gaps

The blind spots produced by these assumptions become most visible in contexts of civil war and armed conflict, and their visibility is increasing. Access Now's 2025 #KeepItOn's annual report documented at least 304 internet shutdowns across 55 countries in 2024, with conflict serving as the leading trigger for a second consecutive year – accounting for 103 conflict-related shutdowns across 11 countries including Sudan, Palestine, Myanmar, and Bahrain.[37] The following year, Access Now's 2026 report documented at least 313 shutdowns across 52 countries in 2025, with conflict retaining its position as the dominant trigger for a third consecutive year, accounting for 125 conflict-related shutdowns across 14 countries, and with perpetrators targeting Low Earth Orbit (LEO) satellite systems 14 times across seven countries – a dramatic escalation from four such incidents the previous year, and notably including Syria and Yemen, confirming that the suppression of alternative connectivity infrastructure has become a feature of conflict in the MENA region itself.[38] What these figures reflect is a structural shift toward the weaponization of connectivity during wartime consolidating as a defining feature of contemporary armed conflict rather than an exception to it.

Three specific gaps follow from this. First, the survival dimension of connectivity disruption has not been systematically engaged in existing frameworks. Contemporary civilian life is deeply digitally mediated, with financial transactions, remittances, humanitarian coordination, evacuation planning, medical referrals, and safety verification increasingly dependent on networked infrastructures.[39,40,41] By conceptualizing shutdowns primarily as discrete acts of censorship, existing frameworks cannot adequately account for what is at stake when these systems fail in a war zone. Second, there is insufficient integration with conflict and humanitarian scholarship. Shutdowns in war zones are analyzed either as collateral damage or as tactical information control, without a framework linking connectivity disruption to patterned civilian harm. Existing frameworks have rarely been equipped to distinguish between incidental infrastructure damage and deliberate connectivity control. This paper treats this distinction as legally and evidentially important, even if, as the Yemen case demonstrates, it cannot always be resolved at

37 Zach Rosson, Felicia Anthonio and Carolyn Tackett, *Emboldened offenders, endangered communities: Internet shutdowns in 2024*, Access Now, February 2025, available at https://www.accessnow.org/wp-content/uploads/2025/02/KeepItOn-2024-Internet-Shutdowns-Annual-Report.pdf (Rosson et al., "Emboldened offenders, endangered communities").

38 Rosson & Anthonio, *Rising repression meets global resistance*.

39 ACAPS, "Implications of Financial Blockages in Sudan".

40 Mnejja, "Internet in Conflict".

41 ICRC, "Offline and in Danger".

the level of individual events.[42,43] Research in conflict settings confirms that combatants do selectively manage connectivity during war, but the mechanisms through which deliberate disruption and incidental damage interact remain undertheorized.[44] Third, the normative vocabulary of censorship is ill-equipped to describe slow, indirect, and distributive forms of violence mediated through connectivity systems. The language of rights violations captures illegality but not the cumulative, systemic harm produced when digital infrastructures underpin survival.

One might argue that existing international human rights law already provides adequate tools for contesting the material harms the paper describes. Economic and social rights – the right to food, the right to health, the right to an adequate standard of living under the International Covenant on Economic, Social and Cultural Rights – are formally recognized under international law, and their violation through connectivity disruption could in principle be contested through existing legal mechanisms. The concept of infrastructural violence does not dispute this. What it identifies is a structural limitation that no extension of the existing rights catalogue addresses: international human rights law is organized around establishing that a specific actor committed a specific violation against a specific right. In armed conflict settings where attribution between deliberate shutdown orders and war-induced infrastructure collapse is often impossible to establish with precision, and where multiple actors simultaneously impose disruptions while contesting responsibility for each other's actions, the legal framework's attribution requirement becomes a poor fit, as it is not merely difficult to meet in practice, but ill-suited to cumulative harm. Infrastructural violence is therefore a structural account of harm that makes visible harm produced by control-aligned patterns rather than identifiable acts, something that rights frameworks are not designed to see.

International humanitarian and criminal law also reach part of this terrain, including the rules protecting objects indispensable to civilian survival, the prohibition of starvation as a method of warfare, and crimes against humanity involving the deprivation of conditions of life. These regimes, however, are organized around individual responsibility, identified perpetrators, and a mental element. Infrastructural violence is not offered as a substitute for them but as a complementary lens, rendering visible the cumulative pattern that such frameworks would then need to attribute and informing arguments about the widespread or systematic character of harm. Whether connectivity can itself count as an object indispensable to civilian survival is contested; the framework does not assume that it does but offers a way of showing why the question matters.

From Censorship to Infrastructural Violence: Sudan as a Theory-Generating Site

This paper treats Sudan as a site from which conceptual limitations in current shutdown debates are exposed rather than an empirical case study to which existing frameworks are applied. Sudan reveals conditions that are increasingly common in contemporary conflicts: the entanglement of connectivity with financial survival;[45,46,47]

42 NetBlocks, "Internet Connectivity Knocked Out in Yemen after Airstrike", 21 January 2022, available at https://netblocks.org/reports/internet-connectivity-knocked-out-in-yemen-after-airstrike-PAYbNoBe (NetBlocks, "Internet Connectivity Knocked Out in Yemen").

43 Access Now, "Internet shutdowns in Yemen: Telecommunications infrastructure is not a military target", 28 January 2022, available at https://www.accessnow.org/press-release/yemen-internet-shutdown-statement/ (Access Now, "Internet shutdowns in Yemen").

44 Nadiya Kostyuk, Jon Lindsay, Eunji Emily Kim, Aniket Anand, Zachary Bischof, Amanda Meng and Alberto Dainotti, "Strategic Interdependence: Using Internet Outage Data to Study How Combatants Manage Collective Institutions During War", *British Journal of Political Science* 56 (2026), e17, pp. 1-19, available at https://doi.org/10.1017/S0007123426101379

45 ACAPS, "Implications of Financial Blockages in Sudan".

46 Mnejja, "Internet in Conflict".

47 Marwa Fatafta and Kassem Mnejja, *Internet Shutdowns in Armed Conflict: A Typology of Harms*, Access Now, December 2025, available at https://www.accessnow.org/publication/internet-shutdowns-typology-of-harms/

contested attribution between warring parties over responsibility for specific disruptions, compounded by the simultaneous occurrence of deliberate shutdown orders and physical infrastructure damage;[48,49,50] the stratification of access along lines of military and institutional power, with Starlink distributed to state officials and humanitarian organizations while remaining unaffordable for displaced civilians;[51,52,53] and the entanglement of communicative and material dimensions of connectivity loss in ways that resist separation at the level of lived experience.

The first pressure point is layered mechanisms, where deliberate shutdown, infrastructure destruction, and selective restoration operate at the same time. Sudan has a documented history of deliberate state-imposed shutdowns, including during the June 2019 post-massacre crackdown and the October 2021 military coup, establishing a pattern of intentional connectivity control that predates the current conflict.[54,55,56] Since April 2023, disruptions have taken on an additional dimension, combining possible deliberate action with physical destruction of telecommunications infrastructure, including reported attacks on exchanges, data centers, and power grids, as documented by Cloudflare and SMEX.[57,58] This layering is not a Sudan-specific anomaly; in Yemen, airstrikes on telecom facilities in Hudaydah in January 2022 produced a four-day nationwide internet blackout absent any explicit censorship order, with NetBlocks confirming that the outage resulted directly from kinetic impact on infrastructure rather than deliberate shutdown.[59,60] The censorship framework struggles in these contexts because it requires a single identifiable actor making a discrete, attributable decision. In Sudan, both the SAF and the RSF deliberately imposed connectivity disruptions while simultaneously targeting each other's telecommunications infrastructure, meaning multiple actors, multiple mechanisms, and contested inter-party attribution operate at the same time, within the same events.[61,62,63] What matters analytically is therefore not the singular act of command but the patterned, control-aligned effect and whether disruptions and restorations systematically track the distribution of military and political control. In Sudan, telecommunications infrastructure is geographically concentrated in Khartoum and other contested urban centers, making it directly entangled in territorial warfare from the first days of the conflict.[64,65] As control shifts, connectivity is intermittently restored in consolidated areas while remaining inaccessible in zones of active fighting or infrastructural

48 Mnejja, "Internet in Conflict".

49 Freedom House, *Sudan: Freedom on the Net 2024 Country Report*, 16 October 2024, available at https://freedomhouse.org/country/sudan/freedom-net/2024 (Freedom House, *Sudan: Freedom on the Net 2024*).

50 Eiman Mohamed, "Sudan's Digital Battleground: The Weaponisation of Internet Shutdowns in Conflict", LSE Middle East Centre, 31 March 2025, available at https://blogs.lse.ac.uk/mec/2025/03/31/sudans-digital-battleground-the-weaponisation-of-internet-shutdowns-in-conflict/ (Mohamed, "Sudan's Digital Battleground").

51 PAEMA, *Unlocking Civilian Protection in Sudan Through Telecoms Access*, 13 April 2025, available at https://www.paema.ngo/reconnect-sudan

52 Freedom House, *Sudan: Freedom on the Net 2024*.

53 Norwegian Refugee Council (NRC) et al., "Joint Statement: Telecommunications Blackout in Sudan", 13 May 2024, available at https://www.nrc.no/news/2024/may/sudan-telecommunications-joint-statement (NRC et al., "Telecommunications Blackout in Sudan").

54 Access Now, "Internet shutdowns and blockings".

55 Human Rights Watch, "Sudan: End network shutdown immediately".

56 Human Rights Watch, "Sudan: Military Takeover Threatens Rights", 26 October 2021, available at https://www.hrw.org/news/2021/10/26/sudan-military-takeover-threatens-rights

57 João Tomé, "Effects of the Conflict in Sudan on Internet Patterns", Cloudflare Blog, 2 May 2023, available at https://blog.cloudflare.com/sudan-armed-conflict-impact-on-the-internet-since-april-15-2023/

58 Salma Ahmad, "Starlink in Sudan: A Thriving Black Market during Times of War", SMEX, 15 October 2024, available at https://smex.org/starlink-in-sudan-a-thriving-black-market-during-times-of-war/ (Ahmad, "Starlink in Sudan").

59 NetBlocks, "Internet Connectivity Knocked Out in Yemen".

60 Access Now, "Internet shutdowns in Yemen".

61 Freedom House, Sudan: Freedom on the Net 2024.

62 Mohamed, "Sudan's Digital Battleground".

63 Dabanga, "Communications Blackout Continues in Large Parts of Sudan", 19 February 2024, available at https://www.dabangasudan.org/en/all-news/article/communications-blackout-continues-in-large-parts-of-sudan

64 Mnejja, "Internet in Conflict".

65 Access Now, "#KeepItOn in times of war".

destruction.[66,67] The pattern of disruption and restoration tracks the pattern of military dominance, and it is this alignment, rather than any singular act of intent, that the framework must be equipped to capture.

The second pressure point concerns what connectivity actually mediates. In a context of banking collapse and cash scarcity, mobile money and digital remittances become primary mechanisms of economic survival. Connectivity here is a financial lifeline, and its disruption directly mediates access to food, medicine, and transportation.[68] This forces an extension of the censorship framework, which has developed primarily around informational and political harms. As previously discussed, to account for Sudan, one needs a framework that recognizes contemporary civilian infrastructure as digitally entangled with daily life. When systems are degraded, withheld, or selectively restored, the harm is not only informational silence but also structured exposure to deprivation. This point also reframes what may initially appear as counterexamples. Sudan's recurrent shutdowns during secondary school examination periods,[69] replicated across the MENA region and justified as measures to prevent exam leaks, do not implicate survival in an immediate sense. When read through the framework proposed here, however, they are legible as one mechanism through which connectivity control enacts governance over social rhythms by regulating institutional temporality, disciplining digital circulation, and asserting centralized authority over national infrastructure. Governance, in other words, is one of the modalities through which infrastructural violence operates, sitting within the broader claim of the "survival" argument rather than pulling against it.

The third pressure point is stratification. The emergence of LEO satellite systems (most visibly SpaceX's Starlink) has introduced new asymmetries into contexts of connectivity disruption. Because LEO satellites bypass terrestrial infrastructure, they can provide connectivity even where fixed networks have been destroyed or shut down, as demonstrated most prominently in Ukraine following Russia's invasion and in Iran.[70,71] In Sudan, access to these systems has remained largely limited to elites, international actors, and specific regions, producing a situation in which connectivity becomes a scarce resource distributed along existing lines of power.[72] This stratification is invisible to frameworks organized around shutdowns as uniform, population-wide events.

The fourth pressure point is contested attribution. In Sudan, the difficulty of attributing disruptions – to intentional state action, infrastructure damage, or their interaction – illustrates a defining feature of structural harm: namely, that it can be systematic without being singular and patterned without being commanded. This is precisely the terrain that Galtung's structural violence framework was developed to address, where harm is systematic, patterned, and cumulative without any discrete originating event.[73] Sudan's attribution problem is not an analytical weakness of the framework proposed here; it is the condition that makes a structural account necessary in the first place.

Infrastructural Violence as an Extension of Structural Violence

The concept of structural violence, as developed by Galtung, explains the pattern of harm, the way institutional arrangements systematically constrain life chances across populations. What it does not specify is the mechanism through

66 Mohamed, "Sudan's Digital Battleground".

67 NRC et al., "Telecommunications Blackout in Sudan".

68 Amnesty International, "Sudan: Internet Shutdown Threatens Delivery of Humanitarian and Emergency Services".

69 Access Now, "Tell MENA Authorities: #NoExamShutdown", available at https://www.accessnow.org/campaign/no-exam-shutdown-2025/, accessed 8 September 2026.

70 Laviniu Bojor, T. Petrache and C. Cristescu, "Emerging technologies in conflict: The impact of Starlink in the Russia–Ukraine war", *Land Forces Academy Review* 29, no. 2 (2024), pp. 185-194, available at https://www.researchgate.net/publication/381758551.

71 "Iran's Latest Internet Blackout Extends to Phones and Starlink", The Conversation, 16 January 2026, available at https://theconversation.com/irans-latest-internet-blackout-extends-to-phones-and-starlink-273439

72 Ahmad, "Starlink in Sudan".

73 Galtung, "Violence, peace, and peace research".

which that pattern is enacted in an era where connectivity underpins daily life. This is the contribution of the present paper. I propose the concept of **infrastructural violence**, defined in the Introduction, as an extension of structural violence into the digital domain: the manipulation, degradation, or withholding of digital infrastructure on which the civilian population depends – whether deliberate or structurally produced – in ways that produce structured vulnerability and mediate survival. The concept admits intentionality as one possible mechanism without requiring it. Instead, what the concept requires is not proof of deliberate command, nor of a plan or policy in the sense used in international criminal law, but evidence that the pattern of disruption and restoration systematically tracks the distribution of military and political control. This is a correlation observable in outcomes, not a purposive design attributed to any actor. Such a pattern may be relevant as circumstantial evidence in legal proceedings, but the concept does not depend on it being so.

There is a further point of divergence with Galtung, whose structural violence describes a condition, or a static arrangement of institutional power that systematically constrains life chances without requiring a triggering event or a causal sequence. The analytical chain proposed below operates differently, complementing Galtung and tracing how a specific connectivity disruption produces downstream consequences through identifiable mechanisms. The structural dimension – the control-aligned pattern of disruption and restoration that tracks military and political control – is what connects the framework to Galtung's tradition and distinguishes infrastructural violence from mere accident or incidental damage. The causal chain – from disruption through institutional breakdown to material harm – is what makes the structural harm empirically traceable and practically contestable. Together, they constitute the framework proposed by this paper, identifying harm as structural in character while specifying the mechanisms through which it is produced in practice.

The analytical chain this generates is as follows. Disruptions of the connectivity on which the civilian population depends, whether produced by shutdown orders, physical destruction or seizure of infrastructure, partial service reduction, or selective restoration in areas under consolidated military control, produce institutional breakdown through financial system paralysis, remittance blocking, humanitarian coordination failure, and information vacuums.[74] Institutional breakdown produces structured vulnerability: economic precarity; inability to verify safety routes; delayed evacuation; and heightened exposure to misinformation.[75] Structured vulnerability produces material harm: deprivation, preventable mortality, and displacement. The mechanisms linking these stages are concrete. Financial disruption severs access to income and remittances, feeding food insecurity. Information vacuums enable misinformation to proliferate, increasing exposure to physical danger. Humanitarian coordination failures produce delayed or misallocated aid, elevating mortality risk. Uneven territorial restoration stratifies access to services across populations along lines of power already established by military control.

The analytical chain proposed here is a theoretical model of how connectivity disruption produces material harm in armed conflict settings. Establishing the empirical strength of each causal link in specific contexts requires integrating network measurement data with humanitarian outcomes data in ways the current literature has not yet attempted and constitutes the primary methodological challenge this framework opens for future research.

This framework does not convert all connectivity loss into violence by definition. Incidental infrastructure damage, technical fragility, and war-induced destruction are real, and the analytical distinction between these and patterned, control-aligned disruption must be maintained. Nor does the concept extend to outages that affect only military or state communications. Rather, it applies where civilian access to basic needs is mediated by the connectivity that is lost. It must also be noted that telecommunications infrastructure is dual-use – the same towers, exchanges, and power supplies serve military and civilian ends. The framework does not turn on whether a given facility is a lawful military objective, which is a question

74 K. V. Bhatia, M. Elhussein, B. Kreimer and T. Snapp, "Protests, Internet Shutdowns, and Disinformation in a Transitioning State", *Media, Culture & Society* 45, no. 4 (2023), available at https://dx.doi.org/10.1177/01634437231155568

75 CDAC Network, *Sudan's Information War: How Weaponised Online Narratives Shape the Humanitarian Crisis and Response*, September 2025, available at https://www.cdacnetwork.org/resources/sudan-information-war-2025

for international humanitarian law. It turns on civilian dependence and on the pattern of harm that follows when that connectivity is disrupted. What the Sudan case demonstrates is that the distinction between incidental damage and patterned, control-aligned disruption cannot be resolved at the level of individual events or singular intentions; it must be established through the cumulative pattern. It is precisely this patterned, cumulative character that connects infrastructural violence to the Galtungian tradition. What makes harm structural is whether the pattern of disruption and restoration systematically constrains civilian access to basic needs, regardless of which actor issued which order, or whether any order was issued at all.

Conclusion: Digital Infrastructure and the Future of Conflict

The argument of this paper is ultimately a shift in what counts as the object of analysis. Disruption of the connectivity on which civilians depend during armed conflict should not be analyzed only as the interruption of communication or as a discrete act of censorship. Where digital connectivity has become embedded in financial, humanitarian, logistical, medical, and safety infrastructures, its disruption can reorganize the conditions under which civilians survive.

Sudan demonstrates that connectivity has developed into more than simply a medium through which conflict is communicated; it is part of the infrastructure through which conflict is waged and endured. The concept of infrastructural violence names this transformation and makes it analytically tractable. By extending Galtung's structural violence framework into the digital domain, it becomes possible to account for forms of civilian harm that censorship-centric analysis cannot see. This harm is patterned rather than singular, cumulative rather than episodic, and mediated through the financial and logistical systems on which survival depends rather than through the suppression of speech alone.

This is not a Sudan-specific condition. Access Now data make it clear that connectivity control is consolidating as a standard feature of contemporary internal conflict.[76,77] In Gaza, the systematic destruction of telecommunications infrastructure and recurrent connectivity blackouts during active military operations have disrupted not only communication but the coordination of medical care, humanitarian aid delivery, and civilian movement, conditions documented by Access Now, NetBlocks, and Cloudflare across multiple prolonged outages since October 2023.[78,79] In Lebanon, bombardment during the September 2024 military escalation damaged at least 18 telecommunications towers and destroyed internet stations across the south of the country, disrupting connectivity for months and intersecting with financial systems already dependent on mobile banking in the context of a pre-existing economic collapse.[80,81,82] These cases do not require new theoretical frameworks of their own. They are evidence that the conditions Sudan brings into analytical focus are now structurally present wherever connectivity is deeply embedded in civilian survival and wherever its disruption tracks the distribution of military and political control. Infrastructural violence offers analytical purchase across all of these contexts that censorship-centric frameworks cannot.

Beyond its theoretical impact, the practical implications of this reframing quickly become clear. If shutdowns in armed conflict are forms of infrastructural violence rather than merely

76 Rosson et al., "Emboldened offenders, endangered communities".

77 Rosson & Anthonio, Rising repression meets global resistance.

78 Marwa Fatafta, Ali Sibai, Zach Rosson, Kassem Mnejja, Hanna Kreitem and Sage Cheng, *Palestine unplugged: How Israel disrupts Gaza's internet*, Access Now, November 2023, available at https://www.accessnow.org/publication/palestine-unplugged/.

79 Lorenzo Franceschi-Bicchierai, "Internet Access in Gaza Is Collapsing as ISPs Fall Offline", TechCrunch, 27 October 2023, available at https://techcrunch.com/2023/10/27/internet-access-in-gaza-is-collapsing-as-isps-fall-offline/

80 World Bank, "Lebanon", available at https://www.worldbank.org/ext/en/country/lebanon, accessed 8 September 2026.

81 Freedom House, *Lebanon: Freedom on the Net 2025 Country Report*, 2025, available at https://freedomhouse.org/country/lebanon/freedom-net/2025

82 Zeinab Ismail, "Digital Rights During the War on Lebanon: October 4-7, 2024", SMEX, 7 October 2024, available at https://smex.org/digital-rights-during-the-war-in-lebanon-october-4-7-2024

censorship, then the various communities that monitor, contest, and respond to them are each operating with an inadequate conceptual foundation.

For the measurement and research community, the challenge is methodological. Network measurement tools operated by NetBlocks, IODA, and Cloudflare Radar capture connectivity loss with precision, but they cannot capture the downstream material harm that connectivity loss produces. Closing this gap requires integrating network measurement data with humanitarian outcomes data – remittance flows, food security indicators, displacement patterns, and aid delivery records – in ways that current monitoring methodologies do not attempt. This is the primary empirical research agenda the concept of infrastructural violence opens.

For accountability and legal practitioners, the challenge is architectural. The current human rights legal framework, organized around legality, necessity, and proportionality, requires establishing that a specific actor committed a specific violation. In armed conflict settings where attribution between deliberate shutdown orders and infrastructure destruction is often impossible to establish with precision, and where multiple actors simultaneously impose disruptions while contesting responsibility, this attribution requirement is often difficult or impossible to meet for individual acts. Accountability frameworks capable of establishing patterned, control-aligned harm without proof of singular command are needed – frameworks that can take account of the cumulative pattern of disruption and restoration alongside the individual act.

For advocates and policymakers, the challenge is normative. The legal standards of necessity and proportionality have been developed and applied primarily in relation to freedom of expression – the question asked is whether a shutdown is a proportionate restriction on speech. These standards must be extended not only to the silencing of speech but to the severing of the connectivity on which civilian survival depends. A shutdown that severs access to mobile banking during a famine, or that prevents humanitarian coordination during a siege, must be assessed against a standard adequate to that harm, not merely against the standards developed for political censorship in peacetime.

The broader implication is that digital infrastructures are no longer the terrain on which conflicts are communicated to the outside world; they are part of the battlefield itself, shaping mobility, finance, aid, and survival. The escalating use of connectivity control as a feature of contemporary armed conflict – confirmed across three consecutive years of Access Now data and now extending to the targeting of LEO satellite systems – demands a robust and updated theoretical response. The concept of infrastructural violence is offered as a contribution to that response, positioning itself as a starting point for future discussions and open questions as opposed to a complete and comprehensive framing. What patterns of disruption and restoration are control-aligned? What downstream material harms can be traced to connectivity loss in specific conflict settings? What accountability frameworks can establish structural harm without requiring proof of singular intent? Sudan has made these questions urgent. Gaza, Lebanon, Myanmar, and the conflicts that follow will make them more urgent still.

About the Arab Reform Initiative

The Arab Reform Initiative is an independent Arab think tank working with expert partners in the Middle East and North Africa and beyond to articulate a home-grown agenda for democratic change and social justice. It conducts research and policy analysis and provides a platform for inspirational voices based on the principles of diversity, impartiality, and gender equality.

About the Tech & Society Program

ARI's Tech & Society Program explores how the accelerating deployment of technologies is affecting political life, economic activities, and the environment in MENA. Grounded in ARI's approach which centers political participation and social justice, the program seeks to strengthen public scrutiny, democratic oversight, and civic participation in the deployment of these technologies. For us, the whole tech ecosystem – not just the end-user interfaces – needs to be scrutinized and debated in order to push for safer and more just societies as we move towards an ever-more digitized future.

contact@arab-reform.net
Paris - Beirut - Tunis