PROTECTING DIGITAL LIFELINES: ENSURING CIVILIAN INTERNET ACCESS DURING ARMED CONFLICTS

Pratyaksh Sharma*

ABSTRACT

Access to civilian internet plays a very crucial role in times of armed conflict. It is a very important contributor in enabling communication, humanitarian coordination, and freedom of expression. However, national governments and non-state actors increasingly impose shutdowns in order to disrupt civilian access to these life-saving resources and critical information. This article examines the legal and ethical implications of such restrictions under the ambit of international humanitarian and human rights law. While states often try to justify these shutdowns on security grounds, they often violate civilian rights. Meanwhile, non-state actors like terrorist groups exploit digital vulnerabilities to spread their propaganda among the masses and disrupt aid efforts. In order to safeguard connectivity, a stronger legal framework, ethical accountability for states and private actors, and practical cybersecurity measures, such as decentralised networks and satellite internet, are necessary.

Keywords: Civilian Internet Access, Armed Conflict, International Humanitarian Law.

INTRODUCTION

The world's 4.39 billion internet users spend, on average, over six hours online every day. What would happen if the internet were destroyed or inaccessible for a day, week, month, or longer? This dire hypothetical is a reality for millions of people around the world.[1] In the Contemporary world that we are living in, the internet is of utmost importance during warfare. The Internet is more than just a communication tool - it serves as a very crucial resource for assessing real-time information, arranging humanitarian aid, and making sure that the

*BBA LLB, THIRD YEAR, DELHI METROPOLITAN EDUCATION, NOIDA.

[1] T. Hutchins, "Safeguarding Civilian Internet Access During Armed Conflict: Protecting Humanity's Most Important Resource in War," *Science and Technology Law Review,* vol. 22, no. 1, pp. 127 - 180, 2020.

fundamental freedom of the common people remains intact. When state forces internet shutdowns under the semblance of national security and concern, or when terrorist organisations disturb networks intending to spread fear and disinformation, it is the common civilians who, unfortunately, have to bear the dismal consequences of these actions undertaken by the state and non-state actors. The absence of the internet means numerous things for the people present in that area. Struggle in receiving emergency alerts, little to no access to healthcare of any sort, and inability to contact agencies for humanitarian aid are a few examples of that. All the things just mentioned worsen the situation even further and exacerbate the challenges faced by the public. Given the important role that the internet plays in crisis management, safeguarding this connectivity has become a very pressing humanitarian concern. To address this issue, we require stronger legal protection under domestic and international laws, ethical accountability from the governments and tech companies, and the execution of technological solutions such as decentralised networks and satellite-based communication, to name a few. Without undertaking such strong measures, digital blackouts will continue as a threat to human lives, depriving people of essential resources, and will worsen the humanitarian impact of conflicts worldwide.

THE IMPORTANCE OF CIVILIAN INTERNET ACCESS DURING ARMED CONFLICT

Having proper internet connectivity during times of armed conflict is of utmost importance as it serves as a critical tool for people stuck between the conflict and the chaos. During such difficult times, the ability to access information and communicate with the world becomes very important. The Internet offers a lifeline and serves as a ray of hope to those who are in danger, giving them the ability to share real-time updates, caution and alert their loved ones, and gain access to emergency services, all of which are of utmost importance during such critical times of crisis. An example of this is the important role played by the internet during the conflict that erupted during the Civil War in Syria. Social media platforms overcoming the challenges put forward by the government-imposed censorship and military interference became a very important tool for the civilians. Both activists and ordinary citizens used social media platforms like X (Twitter), Facebook, YouTube, etc., to document and put forward to the world the human rights violations and the war crimes which were taking place in Syria. These real-time reports not only helped in drawing international attention to this matter but also started a worldwide conversation about the desperate need for intervention. Social media also helped the Syrians in

organising protests, mobilising the resources at their disposal, and communicating with the outside world when traditional communication mediums were either broken totally or controlled.

Something similar to this was seen in Yemen, where conflict continues to devastate the people there, and the internet has emerged as a lifeline for the humanitarian organisations and citizens both. Despite facing numerous enormous challenges like infrastructure damage and irregular connectivity, the internet has allowed the Non-Government Organisations (NGOs) to initiate aid efforts, give out resources, and spread information. Relief organisations use online mediums to give real-time updates regarding the safe zones, medical centres, and available food or water resources. From the civilian's point of view, the internet gives them a medium to convey information about secure routes to safety, get access to educational resources, and stay in touch with their loved ones even during war.

THREAT TO CIVILIAN INTERNET ACCESS IN CONFLICT ZONES

In recent times, the number of civilian internet shutdowns has significantly increased. In 2023, Access Now and the #KeepItOn coalition documented 283 shutdowns in 39 countries. These are staggering results, marking the highest number of shutdown incidents in a single year since the monitoring began in 2016.[2] The primary reason behind these internet shutdowns is the fact that internet is turning up as a viable tool used by authoritarian regimes to suppress and takedown resentful voices of the sufferers and the critics, attack free speech, and encourage state violence, often with very minute to no regard for important factors like rule of law or human rights. These internet shutdowns thrust upon the people by the governments or factions in conflict areas limit the civilians' access to important and essential resources, along with vital information. A real-world example of this is the current ongoing crisis in the country of Sudan, where a near-total communication blackout can be observed that has negatively affected the ability of millions of Sudanese people to effectively communicate, take safe shelters, and gain access to critical assistance during the ever-increasing violence. Since the outbreak of conflict in April 2023, both the Sudanese Armed Forces and the Rapid Support Forces have systematically cut off internet services, exacerbating an already devastating humanitarian

[2] accessnow, "accessnow," accessnow, 15 May 2024. [Online]. Available: https://www.accessnow.org/internet-shutdowns-2023/?t [Accessed 22 April 2025].

disaster that has led to over 14,600 deaths and millions of displaced individuals.[3] Something very similar to this was unfortunately seen in India in Manipur, where a prolonged blackout lasted for a mind-numbing 212 days. During this period, the state government of Manipur issued 44 consecutive orders to disable broadband and mobile networks, affecting a total number of 3.2 million people. This disruption not only hindered access to critical information but also made it significantly more difficult to document the widespread atrocities committed against minorities during violent clashes between the Meitei and Kuki-Zo tribes, including murder, rape and other forms of gender-based violence.[4] These real-life incidents just go on to show the harmful impact that internet shutdowns have on civilian rights and their ability to get access to life-saving resources like medical assistance and many others during such hard times.

ROLE OF NON-STATE ACTORS IN DAMAGING CIVILIAN INTERNET ACCESS

It is not always the state that undermines the civilian internet access during any conflict, but non-state actors like terrorist organisations do the same through a range of their actions. Actions like leveraging the internet as a tool to support their objectives, spread their propaganda and stop people from sharing critical information with the world severely hinder people's rights and make them helpless. These groups may target physical infrastructures like cell towers or influence the internet service providers (ISPs) to disrupt connectivity. They also launch targeted cyberattacks against websites that provide essential services or information, or force ISPs to shut down or censor access. For example, ISIS notoriously restricted internet access in areas under its control, using it for propaganda while suppressing dissent.[5] Terrorist organisations also utilise generative AI to create propaganda and disinformation, manipulating images and videos to instigate violence and spread misinformation.[6] On top of that, terrorist groups use cyber mercenaries to target government websites, growing their reach and influence. The above-mentioned are some of the numerous ways these non-state terrorist organisations not only hinder and damage civilian internet access but moreover, use the internet as a medium to propagate their ideas and influence. The proliferation of offensive cyber

[3] A. International, "Amnesty International," 8 March 2024. [Online].Available: https://www.amnesty.org/en/latest/news/2024/03/sudan-internet-shutdown-threatens-delivery-of-humanitarian-and-emergency-services
[4] A. Rajvanshi, "Time," 16 May 2024. [Online]. Available: https://time.com/6978512/internet-shutdowns-india-report/.
[5] E. Kaplan, "Council on Foreign Relations," 8 January 2009. [Online]. Available:https://www.cfr.org/backgrounder/terrorists-and-internet[Accessed 15 February 2024]
[6] C. Nelu, "ICCT," 10 June 2024. [Online]. Available: https://icct.nl/publication/exploitation-generative-ai-terrorist-groups [Accessed 15 February 2025].

capabilities and low barriers to acquiring and deploying some of these powerful tools suggest that the cyber capacities of non-state armed groups will only continue to grow.[7] To counter this threat, nations and international organisations have to come together as one and take stringent steps like the use of AI and cybersecurity tools to detect and take down online extremist content and propaganda. Moreover, international organisations like the International Criminal Court (ICC) and the UN Security Council (UNSC) can also investigate non-state actors like ISIS, Al-Shabaab, etc., for war crimes and human rights violations, including interference with humanitarian communication or censorship.

LEGAL AND ETHICAL IMPERATIVES FOR PROTECTING CIVILIAN INTERNET IN CONFLICT ZONES

The legal and ethical imperatives for protecting civilian internet access in conflict-stricken zones are increasingly recognised as paramount to upholding human rights and humanitarian principles. International Humanitarian Law (IHL) and Human Rights Law place great importance on the freedom of expression and communication, particularly during times of armed conflict. The Geneva Conventions (1949) and numerous human rights treaties, such as the International Covenant on Civil and Political Rights (ICCPR),[8] affirm that civilians must be protected from arbitrary restrictions on their rights, including access to information and communication technologies. Article 19 (2) of the International Covenant on Civil and Political Rights (ICCPR) states that "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds" This provision applies at all times, including during armed conflicts. Denying access to the internet only increases the suffering of the people by hindering the ability to report human rights violations, seek help, and share vital information with people worldwide using apps like X (Twitter). The United Nations underscores that states have the responsibility to promote universal internet access and cannot justify cutting off access to entire populations, even in the name of national security or public order. This principle of the U.N. is reinstated by the recognition that internet connectivity is absolutely necessary to enable other human rights, such as the right to life, health, and education. By understanding and acknowledging the critical role of the internet in protecting civilian lives and supporting humanitarian efforts, the international

[7] S. Handler, "Atlantic Council," 26 October 2022. [Online]. Available: https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-non-state-armed-groups-in-cyber-conflict/[Accessed 15 February 2025].
[8] L. Cotula, "Democracy and International Investment Law," *Leiden Journal of International Law (2017),* vol. 30, pp. 351 - 382, 2017.

community can better and more efficiently manage the people stuck in conflict zones and ensure the protection of their basic rights.

MECHANISMS TO SAFEGUARD INTERNET ACCESS DURING ARMED CONFLICTS

Protecting civilian internet access during the time of armed conflict requires a detailed and well thought after approach that integrates legal, ethical, and practical measures. Strengthening International Humanitarian Law (IHL) is of utmost importance, as the existing framework has been failing to protect internet infrastructure and connectivity. Therefore, it is a pressing need to advocate for new legal paradigms precisely addressing these concerns. The United Nations has affirmed that states cannot lawfully justify the complete disruption of internet access for the majority of the population even during times of crisis. From an ethical standpoint, policies must do everything possible to uphold freedom of expression and ensure the protection of journalists and media personnel even during times of armed conflict. Simultaneously, Internet Service Providers (ISPs) should acknowledge their duty and play their part in sustaining connectivity and access for civilian internet users in areas of conflict. On a more practical level, a clear separation between civilian and military communication networks can help prevent collateral damage to essential services. Undertaking targeted cyber operations rather than aimless measures further reduces the potential harm to civilian infrastructure. By integrating the above-specified legal, ethical, and technological safeguarding mechanisms, a robust framework can be established that not only protects internet access but simultaneously upholds fundamental rights and mitigates the humanitarian impact of digital disruption in conflict-stricken zones.

CONCLUSION

Ensuring uninterrupted internet access during the time of armed conflict is not only a matter of technological resilience but also a fundamental human right that needs to be protected. As the reliance of modern warfare on digital infrastructure continues to go up, protecting civilian internet connectivity is becoming more and more essential for smoother access to information, coordinating human aid, and upholding freedom of expression. Reinforcing International Humanitarian Law (IHL) to directly safeguard internet infrastructure, applying ethical and moral obligations on states and private bodies, and executing cybersecurity measures that are realistic and practical are all very important parts of an extensive protection framework that is

a need of the hour. By laying more and more emphasis on aspects like legal clarity, ethical and moral responsibilities, and last but not least, technological resilience, we can keep ourselves at an arm's length from the disastrous effects of digital blackouts. By doing so, we take a big leap forward in promoting the principles of human dignity and security, which is very important during armed conflicts.