REVISTA
TRIBUNA INTERNACIONAL

VOL. 14 NÚM. 26 (2025) • PÁGINAS 57-78 • DOI: 10.5354/0719-482X.2025.80959
RECIBIDO: 03/10/2025 • APROBADO: 12 /01/2026 • PUBLICADO: 30/01/2026

ARTÍCULOS

Internet Access in Wartime: A Human Right or an Enabler of Human Rights?

El acceso a Internet en tiempos de guerra: Un derecho humano o un facilitador de los derechos humanos

JAMSHID ZARGARI

University of Judicial Sciences and Administrative Services

ABSTRACT Internet shutdowns during wars have emerged as a critical human rights issue, particularly in recent wars like the Russia-Ukraine war and Iran-Israel war. Despite prior research on human rights, few studies have examined the humanitarian consequences of such disruptions in wartime. This study contributes by analyzing how internet blackouts affect civilian survival and rights under international law. The research aims to evaluate the impact of deliberate internet disruptions on civilians and advocate for recognizing internet access as a fundamental right during wars. Using a qualitative case study approach, it examines legal frameworks, NGO reports, and media coverage to assess the effects of shutdowns in the Russia-Ukraine war and Iran-Israel war. Findings reveal that internet shutdowns severely disrupt emergency alerts, medical assistance, and humanitarian coordination, disproportionately harming civilians and violating international humanitarian law principles. While some scholars debate whether internet access constitutes a human right, this paper argues for its explicit inclusion in legal instruments to enhance state accountability. Protecting digital connectivity during wars is essential for preserving human dignity and ensuring civilian survival. By recognizing internet access as a fundamental right, states would face stricter scrutiny for imposing restrictions, reducing civilian harm and upholding humanitarian principles in modern warfare.

KEYWORDS Human rights; International law; Internet access; Internet shutdown; War.

RESUMEN Los cortes de internet durante conflictos bélicos han surgido como un problema crítico de derechos humanos, especialmente en guerras recientes como las de Rusia-Ucrania e Irán-Israel. A pesar de investigaciones previas sobre derechos humanos, pocos estudios han analizado las consecuencias humanitarias de estas interrupciones en tiempos de guerra. Este estudio analiza cómo los apagones de internet afectan la supervivencia y los derechos de los civiles bajo el derecho internacional. Su objetivo es evaluar el impacto de las interrupciones deliberadas de internet en civiles y abogar por reconocer el acceso a internet como un derecho fundamental durante conflictos. Utilizando un enfoque de estudio de caso cualitativo, examina marcos legales, informes de ONG y cobertura mediática para evaluar los efectos de los cortes en las guerras mencionadas. Los hallazgos revelan que los apagones de internet perturban gravemente las alertas de emergencia, la asistencia médica y la coordinación humanitaria, afectando desproporcionadamente a civiles y violando principios del derecho internacional humanitario. Este artículo aboga por incluir explícitamente el acceso a internet en instrumentos legales para fortalecer la responsabilidad estatal y proteger la dignidad humana.

PALABRAS CLAVE Derechos humanos; Derecho Internacional; acceso a internet; corte de internet; guerra.

Introduction

In an era defined by global connectivity, access to the internet has transcended its initial perception as a luxury to become an indispensable lifeline (Azim, 2025). The deliberate disruption of internet services, often termed "shutdowns" or "blackouts," has emerged as a critical issue with profound humanitarian consequences (KeepItOn, 2019), especially in war zones (Hutchins, 2020). These disruptions, frequently enacted by governments under the guise of national security (De Gregorio and Stremlau, 2020), sever civilians' access to vital communication channels, real-time safety information, and essential services such as emergency healthcare coordination. Furthermore, decisions by private actors—such as internet service providers—to suspend services on grounds of safety, legal liability, or internal policy—may result in de facto disruptions to access. Such interruptions can have severe consequences for civilians, particularly with regard to evacuation procedures, access to critical information, and the provision of essential services. Recognizing internet access as a human right is critical in safeguarding civilian survival during wartime and ensuring accountability for violations.

The legal discourse surrounding internet access as a human right is both robust and contentious. These debates underscore the complexity of internet access within human rights frameworks, particularly in wartime contexts where its deprivation can directly threaten lives and dignity. Despite this growing literature, significant gaps and inadequacies persist. Many studies focus on internet access in peacetime, with limited attention to its critical role during armed wars. Furthermore, while international legal frameworks like the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) implicitly support internet access through provisions on freedom of expression, they lack explicit recognition of it as a distinct right. This ambiguity enables states to justify shutdowns under broad exemptions like national security, often without sufficient scrutiny of humanitarian impact. The absence of a unified legal standard complicates efforts to hold states accountable for violations, particularly in war zones where civilians bear the brunt of these disruptions.

This paper focuses on the Russia-Ukraine war and the Islamic Republic of Iran-Israel war[1] as a case study to examine the human rights implications of internet shutdowns. The article explores how do internet disruptions or shutdowns disproportionately affect civilians, particularly in terms of access to life-saving information and essential services? What motivates states to implement these shutdowns, and how do their stated justifications align with international legal standards? Moreover, can mechanisms within international law ensure accountability for such actions?

[1] Although the concept of war and its distinction from armed conflict in the literature of public international law and international humanitarian law is a highly vague and fluid concept with considerable disagreement, it can at least be considered a customary concept in international law and defined as a hostile conflict by means of armed forces carried on between nations (Garner, 2004).

The paper is structured as follows: The Literature Review synthesizes arguments for and against recognizing internet access as a human right. The Methodology outlines the qualitative case study approach, detailing data sources and thematic analysis to explore shutdowns in the recent wars. The Results section examines specific instances of shutdowns, distinguishing between those imposed by external forces and internal state actions, with reference to the Iran-Israel war and the Russia-Ukraine war for comparative insights. The Discussion refutes arguments against recognizing internet access as a human right, challenges legal justifications for shutdowns, and underscores the necessity of recognizing internet access as a standalone human right.

Literature Review

The debate over whether internet access is a human right is a key issue in international legal discussions, especially given the growing reliance on digital connectivity and frequent internet shutdowns. This literature review addresses arguments from supporters who view internet access as a human right and opponents who dispute it.

A 2010 global poll showed 79% of respondents across 26 countries viewed internet access as a fundamental right (Reuters, 2010). Countries like Estonia (2000) (Woodard, 2003), Greece (2001),[2] France (2009),[3] Finland (2009),[4] and the European Union (2009)[5] have legally recognized or ensured universal internet access. In his 2011 report, Frank La Rue, the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, emphasized that universal internet access should be a priority for all states, highlighting its crucial role in realizing human rights and addressing inequality. He mentioned that states have a positive obligation to ensure internet access is widely available, accessible, and affordable, with government-led disconnections seen as violations of some international conventions (La Rue, 2011). This was further reinforced by a 2016 non-binding resolution from the UN Human Rights Council, which, while not declaring a new standalone right, condemned intentional disruption of internet access.[6]

Proponents assert that internet access is an essential instrument for the realization of numerous pre-existing human rights, thereby justifying its recognition as either a standalone or derivative human right (Xiaowei, 2016; Mathiesen, 2012; Barry, 2014; Reglitz, 2020; Tabusca, 2010). The pervasive nature of the internet provides unparalleled opportunities for the dissemination of information, opinions, and ideas, serving as a catalyst for individuals to

[2] Article 5A of the Constitution of Greece; The Gazette (A/17.4.2001 84).

[3] Conseil constitutionnel. (2009). Decision No. 2009-580 DC of June 10, 2009 - Act furthering the diffusion and protection of creation on the Internet.

[4] Ministry of Transport and Communications. (2009, October 22). Decree on the minimum rate of a functional Internet access as a universal service (732/2009).

[5] European Union Directive 2009/136/EC (amending Directive 2002/22/EC).

[6] United Nations Human Rights Council. (2016). The Promotion, Protection and Enjoyment of Human Rights on the Internet (Resolution A/HRC/RES/32/13). https://ap.ohchr.org/documents/dpage_e.aspx?si=a/hrc/res/32/13.

exercise their human rights and facilitating their fulfillment (Tully, 2014). Specifically, internet access is integral to: 1) Access to information,[7] as it enhances the ability to seek, receive, and share information across borders (Tabusca, 2010); 2) Political participation, freedom of assembly, and association,[8] having transformed democratic processes and enabled mobilization, as evidenced during events such as the Arab Spring (Shandler and Canetti, 2019; Ghannam, 2011); 3) Socio-economic rights, encompassing education, cultural participation, scientific progress, healthcare, and employment,[9] with its critical role underscored during the COVID-19 pandemic when many essential civic functions transitioned to online platforms (Das and Panda, 2021).[10]

Conversely, opponents of recognizing internet access as a human right argue it does not fit within traditional fundamental rights and could have negative consequences (Barry, 2014). First of all, Vinton Cerf, an internet pioneer, and other experts contend that technology like the internet is merely an enabler of rights, not a right itself (Souter, 2012; Cristiano, 2019; Skepys, 2012). They warn that tying human rights to specific technologies risks obsolescence, comparing it to claiming a right to a horse in the past. Instead, the focus should be on underlying values like freedom of speech and access to information that the internet supports (Cerf, 2012). However, this perspective fails to acknowledge the deep and extensive integration of the internet into essential facets of human life and societal operations. Access to the internet is vital for effective social participation, and its absence may result in social exclusion, potentially constituting a violation of human rights (O'Hara and Stevens, 2006; Tully, 2014). In other words, internet access has become a practically indispensable

[7] Articles 19 of the 1948 Universal Declaration of Human Rights (UDHR) and the 1966 International Covenant on Civil and Political Rights (ICCPR), Article 10 of the 1950 European Convention on Human Rights (ECHR), Article 9 of the 1981 African Charter on Human and Peoples' Rights (ACHPR), and Article 13 of the 1969 American Convention on Human Rights (ACHR).

[8] Articles 21, 22, and 25 of the ICCPR, Articles 20 and 21 of the UDHR, Article 11 of the ECHR (1950), Articles 10 and 11 of the ACHPR, and Articles 16 and 23 of the ACHR.

[9] Articles 6, 7, 12, 13, and 15 of the 1966 International Covenant on Economic, Social and Cultural Rights (ICESCR); Articles 22, 23, 25, 26, and 27 of the UDHR; Article 11 of the 1961 European Social Charter (ESC); Articles 14, 15, and 16 of the ACHPR; and Articles 10 and 11 of the Additional Protocol to the American Convention on Human Rights in the Area of Economic, Social and Cultural Rights (Protocol of San Salvador, 1988).

[10] The Internet, as a key tool for realizing the right to development, enshrined as an inalienable right in the United Nations Declaration on the Right to Development (adopted 1986), plays a pivotal role. According to Article 1, the right to development entails the active, free, and meaningful participation of individuals and communities in economic, social, cultural, and political development. The Internet facilitates this participation by providing access to information, education, and economic opportunities. Additionally, Article 8 emphasizes equality of opportunity in accessing basic resources such as education, which the Internet enhances as a platform for learning and knowledge exchange. Article 3 mandates international cooperation to create conditions conducive to development, and the Internet, through global connectivity and information sharing, supports this cooperation. Thus, the Internet, as a fundamental tool, reduces barriers to development and contributes to the full realization of the right to development.

prerequisite for ensuring secure access to other universally recognized fundamental human rights, including life, health, and access to information (Reglitz, 2020; Hutchins, 2020).

Secondly, critics argue that labeling internet access as a human right risks inflating the concept of human rights, potentially weakening the significance of more fundamental rights (De Hert and Kloza, 2012). Some scholars contend that while valuable, internet access is not essential for basic human experiences, and its denial should be seen as a threat to other rights rather than a violation of a standalone right (Skepys, 2012). To put it differently, they suggest it dilutes the force in human rights claims and could lead to a lack of authority for the concept itself (Wang, 2013). Nonetheless, this argument does not adequately recognize the distinctive and transformative influence of the internet on human capabilities and rights, particularly within a globally interconnected society. Internet access is sui generis, a singular right that cannot be reduced to or subsumed by any other individual right. It serves functions that cannot be replicated through alternative means, such as newspapers or public speaking venues (Reglitz, 2020). For instance, the internet enables real-time global communication, allowing individuals in remote areas to access educational resources, such as online courses from platforms like Coursera, which traditional media cannot provide. Furthermore, the internet facilitates access to critical information during crises, such as real-time updates on natural disasters or health pandemics via platforms like X or government websites, functionalities that public speaking or print media cannot match.

Additionally, some experts believed that existing human rights treaties do not explicitly recognize internet access as a distinct right; it is typically linked to pre-existing rights like freedom of expression (Pollicino, 2019; Tully, 2014). There is no global consensus within the international community on its status as a human right (Shandler and Canetti, 2019). Notwithstanding this perspective, it must be noted that, although Article 19 of both the UDHR and the ICCPR does not expressly articulate a right to internet access, the latter segment of this provision—affirming the right to seek, receive, and impart information and ideas through any media and irrespective of frontiers—implicitly encompasses such a right. This implicit acknowledgment is consistent with interpretive methodologies applied to other rights that, while not explicitly delineated, have been inferred from these instruments. For example, the right to digital privacy and data protection is derived from Article 17 of the ICCPR, and the right to a healthy environment is inferred from Article 6, concerning the right to life. In this context, the European Court of Human Rights (ECtHR) has adjudicated cases under Article 10 of the European Convention on Human Rights (ECHR), which is structured similarly to Article 19 of the UDHR and ICCPR. Notably, in Autronic AG v. Switzerland, the Court explicitly affirmed that Article 10 extends beyond the content of information to include the means of transmission and reception. It held that any restriction on such means constitutes an interference with the right to receive and impart information, thereby violating Article 10 of the ECHR.[11]

[11] European Court of Human Rights. (1990). Autronic AG v. Switzerland, Application No. 12726/87, Judgment of 22 May 1990, Series A no. 178.

Finally, opponents highlight that internet access can enable harm, including mass surveillance, propaganda, cyberattacks, anti-social behavior, and crimes like child pornography (Barry, 2014). Based on that, states often justify internet shutdowns or restrictions citing national security, public order, or the need to control dissent and misinformation, arguing that internet access must be balanced against other rights and public interests (Ryng and others, 2022; Tully, 2014). Although the potential harms associated with internet use are significant and merit serious consideration, they do not justify denying access to the internet. Rather, they highlight the necessity for robust governance, ethical regulation, and international cooperation to address these risks while preserving the substantial benefits of the internet (Reglitz, 2023). As certain scholars assert, the solution lies not in reducing internet access but in strengthening human rights protections and improving governance (Mathiesen, 2012). Restrictions on internet content are permissible under international human rights law, provided they adhere to stringent conditions. This framework enables the mitigation of harmful content without resorting to broad prohibitions on access.

Methodology

This study adopts a qualitative case study approach to investigate the legal status of internet access during wartime, with a particular focus on instances of internet shutdowns. This methodology is chosen to delve deeply into specific cases, enabling a nuanced exploration of the tension between security necessities and human rights obligations in war settings. By examining individual instances of internet shutdowns, the research seeks to uncover the contextual factors driving these actions and their implications for civilian populations. The qualitative case study approach is particularly effective for this purpose, as it facilitates a detailed analysis of complex social phenomena, capturing the interplay of governmental policies, legal frameworks, and human rights impacts.

The data for this research is derived from a variety of primary and secondary sources, carefully selected to provide both normative and empirical insights. International laws and documents serve as the foundation for understanding the legal obligations surrounding internet access. Key texts include the UDHR, the ICCPR, and resolutions from the United Nations Human Rights Council (UNHRC). These legal frameworks are complemented by reports from non-governmental organizations (NGOs) such as Access Now, which offer detailed accounts of internet shutdowns and their effects on affected populations. Additionally, UN documentation, including reports from the Special Rapporteurs, provides authoritative perspectives on the global human rights implications. Media accounts from reputable outlets like Reuters and Times are also incorporated, supplying real-time narratives and firsthand testimonies that enrich the factual basis of the case studies.

Data collection entailed a systematic process of gathering these sources, with an emphasis on ensuring their credibility, relevance, and timeliness. Sources were prioritized based on the reputation of the publishing entities, favoring established NGOs, official UN repositories, and internationally recognized news organizations. NGO and UN reports were accessed through their official websites and databases, such as the UN Digital Library, while media accounts

were drawn from the archives of selected outlets. To enhance reliability, events described in these sources were cross-verified across multiple reports where possible, ensuring a robust evidentiary foundation.

The analysis of this data employed thematic analysis, a method well-suited to identifying patterns and themes within qualitative data. Documents were coded for recurring concepts, such as "security justifications," "human rights violations," and "civilian impacts." This coding process enabled a structured comparison of governmental rationales for restricting internet access with the resulting human rights outcomes, as reported by NGOs, the UN, and media sources. By synthesizing these findings, the analysis illuminates the broader dynamics of security and human rights in wartime settings, highlighting how internet shutdowns reflect and exacerbate these tensions.

This study is subject to certain limitations inherent in its methodology. The reliance on secondary sources introduces potential challenges related to bias or incomplete information. For instance, NGO reports may reflect organizational agendas, while media accounts could be shaped by editorial priorities or restricted access to war zones. Additionally, the focus on specific case studies, while providing depth, may limit the applicability of the findings to other wartime contexts. To address these constraints, the research triangulates data from diverse sources and critically evaluates their reliability, striving to present a balanced and well-supported analysis of internet access rights during war.

Results

Internet shutdowns during times of war have become a prominent strategy utilized by states. These shutdowns entail the intentional disruption of internet access, impacting either an entire country or occupied territories. This section is organized into two primary methods of implementing internet shutdowns during wars: those imposed by an external force (enemy) and those enacted by an internal force (state). Examples of such scenarios are provided within the context of two contemporary war: the ongoing war between Russia and Ukraine and the recent war between the Islamic Republic of Iran and Israel.

By an External Force

Since Russia's full-scale invasion of Ukraine commenced on February 24, 2022, internet shutdowns and disruptions have been a recurrent strategy, particularly in occupied regions. Shortly after the invasion began, Russian forces allegedly conducted a cyberattack on Viasat's KA-SAT satellite system, disrupting Ukraine's satellite broadband services (NetBlocks, 2022). NetBlocks reported significant connectivity losses in cities under intense attack; for example, Kharkiv's internet providers ceased functioning during explosions, and Mariupol experienced a significant internet disruption due to the destruction of its telecommunications infrastructure (Reuters, 2022). A notable tactic has involved rerouting internet traffic through Russian-controlled networks, as observed in areas such as Kherson. These rerouting exposes internet users to Russian censorship, disconnecting access to Ukrainian news websites and

social media platforms, including Facebook, Instagram, and X, thereby enabling narrative control and limiting access to independent information (Krapiva and others, 2023).

In 2022, at least 12 of the 22 documented internet shutdowns in Ukraine, attributed to Russia in cities such as Bucha, Irpin, and Mariupol (Winninger and Coppi, 2024). For instance, Russian forces targeted 4G transmission units in Mariupol, disrupting connectivity and impeding civilians' ability to communicate or access critical safety information (Judah, 2022). A subsequent Russian cyberattack in December 2023 targeting Kyivstar, Ukraine's largest mobile operator, reportedly destroyed the network's core, affecting 24 million users (Balmforth, 2024). Despite these localized shutdowns, Ukraine's overall network infrastructure has remained largely operational, supported by backup satellite systems such as Starlink, preventing a nationwide internet blackout. However, the role of private intermediaries should not be regarded solely as a positive factor. Actions taken by these actors can also restrict access to critical services. For instance, reports have documented the temporary suspension of Starlink services in certain areas, prompted by decisions from the company's chief executive officer (Mishchenko, 2025). This case illustrates how corporate decisions can lead to de facto access disruptions, thereby directly affecting civilians' ability to survive and obtain essential information.

The Russian Federation has not officially disclosed its rationale for disrupting Ukraine's internet infrastructure. However, the following reasons can be inferred based on expert analysis and observations:

1) Control of occupied territories: Reports indicate that in regions under Russian occupation, local communication networks are promptly disabled and supplanted with systems controlled by Russian authorities. According to TIME magazine, "the first thing that the Russians do when they occupy [Ukrainian] territories is cut off the networks," resulting in an information blackout (Times, 2022). This isolates residents, preventing access to independent news and communication with family, thereby consolidating Russian control over these areas.

2) Information control and propaganda: Experts assert that disrupting internet access is a component of Russia's broader information warfare strategy aimed at manipulating the narrative accessible to Ukrainian civilians. By severing connections to independent media and social platforms, Russia creates an information vacuum, which it fills with state-sponsored propaganda (Antoniuk, 2022). As noted in TIME, disconnected individuals "don't know what's happening in Ukraine…they don't know whether their relatives are alive or not" (Times, 2022). This enables Russia to promote its narrative, such as framing the invasion as a liberation, while suppressing evidence of its actions until territories are reclaimed.

3) Psychological and civilian impact: Independent analysts highlight that attacks on the internet and utility infrastructure, including electricity and water, are designed to demoralize and intimidate the civilian population. U.S. cybersecurity officials have observed that such cyberattacks are intended to break the will of everyday citizens (Miller, 2023). Disrupting

internet access is thus seen as a tactic of psychological warfare, aimed at undermining civilian morale and weakening support for the Ukrainian government.

4) Intelligence gathering and surveillance: Analysts identify espionage and surveillance as additional motives for internet disruptions. By compromising Ukrainian telecommunications infrastructure, Russian military intelligence gains access to sensitive data and communication channels. In the case of the Kyivstar breach, Ukraine's security service reported that attackers could have extracted personal information, tracked device locations, intercepted messages, and compromised messaging applications (Balmforth, 2024). Furthermore, rerouting Ukrainian internet traffic through Russian servers subjects users to Moscow's surveillance and censorship mechanisms, including those enforced by Roskomnadzor (Antoniuk, 2022). This facilitates Russian intelligence operations and suppresses dissent in occupied regions.

In summary, the disruption of Ukraine's internet infrastructure serves multiple strategic objectives, including territorial control, information manipulation, psychological warfare, and enhanced surveillance capabilities. However, these actions lack justification under international law and legal frameworks.

By an Internal Force

The war between the Islamic Republic of Iran and Israel, which started on June 13, 2025, following Israeli airstrikes on Iran's military and nuclear facilities, prompted significant internet restrictions imposed by the Iranian government. The authorities stated that these measures were enacted to mitigate Israeli cyberattacks and neutralize enemy drones during a period of heightened military operations to safeguard national security (Fararu, 2021; Young Journalists Club, 2025; Kalhor, 2025). In effect, connectivity was severely disrupted: Kentik, an analysis firm, reported a national bandwidth reduction of approximately 54% on June 13, followed by an additional 49% decline on June 17. From June 18 to 21, Iran experienced a near-total internet outage, with a connectivity drop of approximately 90% from normal levels (Burgess, 2025). Internet monitoring organizations, including NetBlocks and Cloudflare, noted that only a minimal percentage of regular connections remained operational, with numerous providers going offline. After approximately 62 hours of shutdowns, partial recovery of internet connectivity commenced on June 21 (Kalhor, 2025).

Although it has never been officially announced which government body made the decision to implement the internet shutdown, there is little doubt that the Supreme National Security Council (SNSC) played the central role, in accordance with the Constitution of the Islamic Republic of Iran. The SNSC serves as the country's principal security authority and is chaired by the President. Its key responsibilities include: 1) Determining national defense and security policies; 2) Coordinating political, intelligence, and social activities related to general defense and security measures; 3) Mobilizing the nation's resources to confront internal and

external threats.[12] In light of these responsibilities, there are instances indicating that the SNSC has ordered internet shutdowns and restrictions (Hamshahrionline, 2023).

The impact on Iranian civilians, especially during the war, was more significant because Iran had approximately 84.82 million internet users by 2024, corresponding to an internet penetration rate of 94.45% (Statista, 2024). Of this total, an estimated 70% is attributed to access to the international Internet (Nikbakht, 2020). With internet connectivity severely curtailed, millions were unable to access global platforms, including WhatsApp, Telegram, and international news websites, resulting in limited access to information about the ongoing war (Burgess, 2025). This was particularly critical in cities such as Tehran, where approximately 10 million residents were advised on the international internet to evacuate due to Israeli airstrikes but lacked access to real-time safety alerts. Following the disruption of international internet access, the government suggested that citizens use domestic applications, such as Bale and Eitaa, on the National Information Network (NIN) rather than the international Internet (Kalhor, 2025).

During the recent Iran-Israel war, the Iranian government asserted that Israeli forces were utilizing domestic SIM card internet services to guide their drones, thereby justifying the implementation of widespread internet blackouts (Fararu, 2021; Young Journalists Club, 2025). However, Ehsan Chit-Saz, Deputy Minister of Communications, shortly thereafter disclosed in an Instagram post that a drone shot down in Qom was equipped with a sophisticated American satellite modem—the A3LA-R-MOD from NAL—featuring an Iridium 9534 transceiver. This device enabled the drone to connect directly to the Iridium satellite network, a global constellation of 66 low-Earth orbit satellites that provides stable, high-speed, and secure communication, even in remote and polar regions (Asriran, 2025). This revelation clearly indicates that the drones operated independently of Iran's internet infrastructure, instead relying on satellite technology. As a result, the government's justification for the international internet shutdown appears to lack credibility in preventing drones from guiding. Nonetheless, there was another reason for the disruption, that is the prevention of enemy cyberattacks in order to safeguard national security.

In this regard, there are several legal justifications under international law that permit states to restrict or cut off internet access in situations involving national security. Firstly, Article 19 of the ICCPR recognizes the right to freedom to seek, receive, and impart information and ideas. However, it also allows for certain limitations, provided they are prescribed by law and are necessary for legitimate aims, such as the protection of national security, public order, or public morals. Secondly, the Constitution of the International Telecommunication Union (ITU) offers further legal grounds for member states to restrict telecommunication services, including internet access. Specifically, Articles 34 and 35 of the ITU Constitution permit states to suspend telecommunication services for reasons of national security (Mehrotra, 2021). In addition, the principle of national sovereignty, enshrined in Article 2(1) of the Charter of the UN, reinforces a state's authority to regulate and control its telecommunication infrastructure

[12] Article 176 of the Constitution of Iran: https://rc.majlis.ir/fa/law/show/133730

within its territory (De Gregorio and Stremlau, 2020). Finally, the right to self-defense, as recognized under Article 51 of the UN Charter, may also be invoked to justify internet shutdowns, particularly in response to cyber-attacks (Joyner and Lotrionte, 2001). Cyber operations targeting a country's telecommunication infrastructure are increasingly recognized as potential uses of force that can endanger critical services, disrupt civilian life, and pose significant national security risks (Dinstein, 2002; Mix, 2014).

Discussion

Recent wars, including those between Russia and Ukraine and Iran and Israel, have revealed a troubling tactic: the deliberate disruption or shutdown of civilian internet access (Ryng and others, 2022). This practice, now common in warfare, threatens human rights, as internet connectivity is critical for civilian life and health during wars (Hutchins, 2020). The COVID-19 pandemic underscored this, with billions relying on the internet for communication, business, health services, education, and family connections (Villadiego, 2022; Vardanyan, Kocharyan, and Hamuľák, 2024). Internet access is essential to human survival in war zones. This discussion will address arguments against recognizing internet access as a human right and legal justifications for its disruption, emphasizing its necessity for recognizing it as a human right.

Refuting Arguments Against Recognizing Internet Access as a Human Right

Opponents of recognizing internet access as a human right often argue that its technological nature, the risk of rights inflation, and the absence of explicit recognition in treaties preclude its classification as such. However, these arguments fail to acknowledge the internet's transformative and indispensable role in modern life, particularly in the extreme context of war, where it serves as a critical lifeline for survival, health, and dignity.

In wartime, the internet's role transcends that of a mere tool, becoming essential for preserving fundamental human rights. Access to real-time information about safety, evacuation routes, aid distribution, and emergency services can mean the difference between life and death. Without internet access, civilians may be unable to navigate safe corridors or receive warnings about imminent threats (Satriawan, Elven, and Lailam, 2023). Similarly, in regions with disrupted infrastructure, telemedicine and online health resources are vital for managing medical emergencies and chronic conditions (George, 2024). Moreover, the ability to communicate with loved ones, confirm their safety, or access psychological support through online platforms is crucial for mental resilience when traditional communication channels are severed (Smith, 2012).

The internet's unparalleled scale, speed, and global reach (Reglitz 2023), demonstrated during events like the Arab Spring, where social media facilitated the dissemination of critical information and documentation of human rights violations (Joseph, 2012; Satriawan, Elven, and Lailam, 2023), make it a non-substitutable mechanism for coordinating humanitarian efforts and safeguarding life and dignity. Denying its status as a human right based on concerns

about rights inflation ignores its foundational necessity in the digital age, particularly when lives are at stake.

International human rights frameworks increasingly support the recognition of internet access as a right. While Article 19 of the UDHR and the ICCPR do not explicitly mention internet access, their provision for the right to seek, receive, and impart information "through any media and regardless of frontiers" implicitly encompasses it. The ECtHR has similarly affirmed in cases like Autronic AG v. Switzerland that Article 10 of the ECHR, , which is similarly structured to Article 19 of the UDHR and ICCPR, extends to the means of transmission and reception, with restrictions constituting an interference with the right to information.[13] Furthermore, UN human rights bodies, including the Committee on Civil and Political Rights, have expressed concern over state-imposed internet restrictions and urged governments to ensure access, particularly for political activists.[14] The 2002, and 2011 reports by UN Special Rapporteurs emphasized the internet's role as an indispensable tool for realizing human rights, advocating for universal access as a state priority (La Rue, 2011; Hussain, 2002). In 2016, the UN Human Rights Council's non-binding resolution condemned intentional internet disruptions and called for a human rights-based approach to facilitating access.[15] While it did not declare a new right, it enumerated existing rights for which the internet has become an indispensable means (Szoszkiewicz, 2018). Although explicit treaties recognizing internet access as a standalone right may lag, the consensus among international bodies and the internet's critical role in wartime underscore its status as an inherent necessity.

In addition to the above implicit protections, the right to internet access is also grounded in the International Covenant on Economic, Social and Cultural Rights (ICESCR). Specifically, Article 15(1)(b) establishes the right of everyone to enjoy the benefits of scientific progress and its applications. In the contemporary world, the internet is the primary conduit for accessing these benefits. The Committee on Economic, Social, and Cultural Rights (CESCR) affirmed this link in its General Comment No. 25 (2020),[16] stating that internet access is an essential component of the right to participate in and enjoy the benefits of scientific progress. This includes access to scientific knowledge, participation in research, and the use of technologies like telemedicine and online learning platforms, which are direct applications of scientific progress. Denying internet access, therefore, is tantamount to

[13] European Court of Human Rights. (1990). Autronic AG v. Switzerland, Application No. 12726/87, Judgment of 22 May 1990, Series A no. 178.

[14] Human Rights Committee. (2005). *Concluding observations on the Syrian Arab Republic*, 3 October 2005, A/60/40 (Vol. I), 94(13); Human Rights Committee. (2011). *General Comment No. 34: Freedoms of opinion and expression (Article 19)*, 12 September 2011, CCPR/C/GC/34; 19 IHRR 303 (2012), 12.

[15] United Nations Human Rights Council. (2016). The Promotion, Protection and Enjoyment of Human Rights on the Internet (Resolution A/HRC/RES/32/13). https://ap.ohchr.org/documents/dpage_e.aspx?si=a/hrc/res/32/13.

[16] General comment No. 25 (2020) on article 15: science and economic, social and cultural rights, Para. 16: https://docs.un.org/en/E/C.12/GC/25

denying individuals their right to benefit from advancements that are crucial for health, education, and overall well-being, especially during a war.

Concerns about potential harms, such as cyberattacks, misinformation, or propaganda, do not justify denying internet access, especially in wartime. While these risks are real, the denial of access is a disproportionate response when civilian lives depend on timely information, emergency communication, and aid coordination. The immediate threats posed by lack of access, such as inability to receive warnings or to locate safe havens, far outweigh the risks of misuse, which can be addressed through targeted regulation and education rather than blanket restrictions.

Refuting Legal Justifications for Internet Disruption in Wartime

States often justify internet disruptions or shutdowns during wartime by invoking national security, sovereignty, and self-defense. However, these justifications must be scrutinized against the fundamental principles of human rights law, which prioritize the protection of civilian life, health, and dignity.[17]

Internet shutdowns for maintaining national security can be justified by the framework of Article 19 of the ICCPR (Young Journalists Club, 2025; Ryng and others, 2022; Chutel, 2019; Howard, 2011; Micek, 2016; Wilson, 2019). While Article 19 guarantees freedom to seek, receive and impart information and ideas, it also includes provisions for permissible restrictions. The application of these restrictions is subject to compliance with conditions, including being necessary. In other words, necessary is key, meaning the measures must be the minimum required to achieve the legitimate aim (Tully, 2014). Blanket internet shutdowns in wartime typically fail this necessity test, as they disrupt far more than targeted information, impeding access to vital information for civilians such as safe zone locations, emergency aid, medical facilities, and family communication (Lim and Sexton, 2011). The UN Special Rapporteur has deemed such measures disproportionate, violating Article 19(3) of the ICCPR (La Rue, 2011), as less intrusive alternatives, such as enhanced cybersecurity or targeted warnings, could address security concerns without compromising civilians' access to life-preserving information (Satriawan, Elven, and Lailam, 2023; Hutchins, 2020). Similarly, Articles 34 and 35 of the ITU Constitution permit states to restrict telecommunications, including internet access, for reasons of national security, public order, or morality. However,

[17] Articles 1, 3, and 5 of the UDHR; Articles 6, 7, and 10 of the ICCPR; Article 12 of the ICESCR; Article 2 of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT); Articles 6 and 24 of the Convention on the Rights of the Child (CRC); Article 10 and 17 of the Convention on the Rights of Persons with Disabilities (CRPD); Article 3 of the Geneva Conventions of 12 August 1949; Article 12 of the First Geneva Convention; Article 27 of the Fourth Geneva Convention; Articles 48, 51, 52, and 75 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I); Articles 4 and 7 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II); and the Human Rights Council Resolution 9/12 (2008) on the Protection of Civilians in Armed Conflict.

these provisions do not override human rights obligations (Reglitz, 2023; Ryng and others, 2022; Hutchins, 2020).

While states may attempt to justify internet shutdowns during wartime by invoking national security under the limitation clause of ICCPR Article 19(3), a more potent justification might be sought through the derogation regime under Article 4. This article permits states to temporarily suspend certain obligations during a public emergency which threatens the life of the nation, provided such measures are strictly required by the situation. As Article 19 is not listed among the non-derogable matters in Article 4(2), states could, in theory, derogate from their duty to protect it. However, even under a state of derogation, blanket internet shutdowns remain highly problematic and often unlawful for several critical reasons.

First, Article 4 itself imposes strict constraints: any derogation must be proportional to the exigencies of the situation, must not be inconsistent with their other obligations under international law, and must not be discriminatory. A total internet blackout, which indiscriminately affects the entire civilian population, rarely meets the strict necessity and proportionality test required even for derogation. More importantly, while Article 19 may be derogable, the consequences of an internet shutdown directly impact rights that are non-derogable. Article 4(2) explicitly forbids derogation from fundamental rights such as the right to life (Article 6) and the prohibition of torture or cruel, inhuman or degrading treatment (Article 7).

In a modern war, internet access is a critical enabler for the realization of these non-derogable rights. For instance: 1) Right to Life: Internet shutdowns prevent the dissemination of life-saving information, such as warnings about impending attacks, locations of safe zones, and access to emergency medical services (telemedicine). By cutting off this vital lifeline, a state actively endangers civilian lives, thus infringing upon the non-derogable right to life. 2) International Humanitarian Law: A state's measures cannot be inconsistent with its other obligations under international law, which prominently includes IHL. Principles of IHL, such as distinction and proportionality, require parties to a war to distinguish between civilians and combatants and to ensure that attacks do not cause disproportionate harm to civilians. A blanket internet shutdown is inherently indiscriminate, harming civilians and disrupting essential civilian infrastructure (hospitals, humanitarian aid coordination) far beyond any potential military advantage. 3) Prohibition of Inhuman Treatment: The inability to communicate with family members, confirm their safety, or access humanitarian support during a war can inflict severe mental suffering, potentially amounting to inhuman or degrading treatment, from which no derogation is permitted. Therefore, the right to internet access operates robustly even within a derogation framework. Its legal force is not derived solely from the derogable Article 19, but from its instrumental role in safeguarding non-derogable rights and upholding core principles of international humanitarian law.

Just as states may try to justify shutdowns under the ICCPR, they might also invoke the limitation clause of the ICESCR. Article 4 of the ICESCR permits states to subject the rights

in the Covenant to limitations "determined by law... compatible with the nature of these rights and solely for the purpose of promoting the general welfare in a democratic society." However, a blanket internet shutdown during wartime fails to meet this strict standard. Such a measure is not compatible with the nature of the right to enjoy scientific progress, as it completely severs access. Furthermore, it actively works against the general welfare by preventing civilians from accessing life-saving health technologies (telemedicine), critical safety information systems, and educational resources. Therefore, even under the ICESCR's own limitation clause, a general internet blackout is a disproportionate and unjustifiable measure that undermines, rather than promotes, general welfare.

Furthermore, the principle of national sovereignty, grounded in Article 2 of the UN Charter, allows states to control internal affairs, including internet access, to safeguard national security or development objectives (De Gregorio and Stremlau, 2020). Yet, sovereignty is not absolute; it is constrained by international human rights obligations (Reglitz, 2020). In wartime, internet shutdowns justified by sovereignty directly undermine civilians' rights to life and dignity, hinder documentation of human rights violations, and exacerbate suffering by denying access to essential services, thus failing to meet human rights standards (O'Meara, 2025). Finally, the right to self-defense, as outlined in Article 51 of the UN Charter, permits states to respond to armed attacks but requires compliance with international humanitarian law's principles, including precautions and distinction.[18] The principle of precautions obliges parties to a war to take all feasible precautions to avoid, and in any event to minimize, incidental loss of civilian life, injury to civilians, and damage to civilian objects. Moreover, the principle of distinction necessitates the limitation of attacks to military objectives. Internet shutdowns, even if framed as defensive measures, are inherently indiscriminate, affecting civilians and combatants alike and disrupting access to critical resources managed online, such as medical aid (Hutchins, 2020; Satriawan, Elven, and Lailam, 2023). Even if internet infrastructure were considered a military objective, disrupting it would be unlawful if it causes disproportionate civilian harm. Consequently, invoking self-defense to justify widespread internet blackouts is untenable when such actions risk significant civilian suffering by denying access to indispensable services and information.

The Role of Responsibility of Private Intermediaries

While this article has primarily focused on governmental actions and justifications for internet shutdowns, recent wartime experiences—particularly in Ukraine—have highlighted the critical and complex role of private intermediaries. Satellite connectivity providers, through their internal decisions to suspend services, can indirectly contribute to access disruptions.

[18] International Committee of the Red Cross (ICRC). (1977). *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Article 48*, 8 June 1977, 1125 U.N.T.S. 3.

This underscores the necessity of engaging with the "Business and Human Rights" framework, particularly the United Nations Guiding Principles on Business and Human Rights (UNGPs).[19] Under these principles, companies bear a responsibility to respect human rights. This responsibility extends beyond mere compliance with domestic laws and encompasses the obligation to conduct human rights due diligence—that is, to identify, prevent, mitigate, and account for adverse human rights impacts arising from their activities. Consequently, any legal framework aimed at protecting internet access during wartime must extend beyond state obligations to encompass the responsibilities of private actors, thereby ensuring comprehensive protection for civilians.

The Imperative of Recognizing Internet Access as a Human Right

The experience of recent wars has underscored that internet access is not merely a convenience but a critical lifeline for preserving life and dignity during wartime. Recognizing internet access as a human right would affirm its indispensable role in protecting human values amid the chaos. Establishing internet access as a standalone human right would impose both positive and negative obligations on states. Positively, governments would be required to promote universal access, bridging digital divides that disproportionately affect marginalized communities. Negatively, they would be obligated to refrain from arbitrary interference, such as widespread internet shutdowns, particularly during wartime. Such recognition would elevate the internet to a fundamental component of a minimally decent life in the digital age, akin to access to food or shelter.

By enshrining internet access as a human right, the international community would significantly raise the political and diplomatic costs for states that impose internet blackouts. Governments engaging in such practices would face the stigma of violating a recognized human right, inviting condemnation from international bodies, human rights organizations, and other states. This heightened scrutiny would deter arbitrary or disproportionate internet restrictions, as the label of human rights violator carries substantial reputational consequences, including potential sanctions or loss of international credibility. In wartime, where the temptation to control information flows is strong, this framework would act as a powerful deterrent, ensuring that states weigh the severe humanitarian impact against any perceived strategic advantage.

To eliminate interpretive disputes and harness the benefits of a unified approach, it is recommended that human rights treaties and conventions explicitly recognize the right to internet access as a fundamental human right, rather than implicitly deriving it from existing rights. Such clarity would resolve ambiguities, strengthen accountability, and ensure that the

[19] United Nations Human Rights Council. (2011). *Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" framework* (UN Document A/HRC/17/31). https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

internet's significance is universally acknowledged, guaranteeing that no one is left disconnected when access to information can mean the difference between life and death.

Conclusion

This study set out to investigate the human rights implications of internet shutdowns during wartime, with a specific focus on the Russia-Ukraine and Iran-Israel wars. It aimed to explore how these disruptions and shutdowns disproportionately affect civilians, the motivations behind state-imposed shutdowns, and the potential of international legal mechanisms to ensure accountability. By examining these questions, the paper sought to contribute to the discourse on whether internet access should be recognized as a human right, particularly in the context of wars where connectivity is vital for civilian survival and dignity.

The findings reveal that internet shutdowns, whether imposed by external forces, as seen in Russia's actions in Ukraine, or by internal state authorities, as in Iran's response to the war with Israel, have profound humanitarian consequences. In Ukraine, Russian forces disrupted internet access in occupied regions to control information, enable surveillance, and demoralize civilians, severing access to critical safety information and communication channels. In Iran, government-imposed blackouts, justified as measures to counter cyberattacks and drone threats, isolated millions from global platforms and real-time safety alerts. These disruptions hinder access to life-saving information, emergency services, and humanitarian aid coordination, underscoring the internet's indispensable role in wartime survival. The qualitative case study approach, drawing on international legal frameworks, NGO reports, and media accounts, highlighted the tension between states' security justifications and human rights obligations, revealing that blanket shutdowns often fail the necessity test required by international law. Furthermore, this study has demonstrated that actions by private actors can be equally impactful in disrupting access to critical services. This finding underscores the imperative to extend accountability frameworks to technology companies in order to ensure comprehensive protection for civilians during armed conflict.

The implications of these findings for the field of human rights are significant. Recognizing internet access as a standalone human right would provide a robust framework to protect civilians in wartime, ensuring access to vital information and services. It would impose positive obligations on states to promote universal connectivity and negative obligations to refrain from arbitrary disruptions, particularly during wars. Such recognition would also elevate the political and diplomatic costs of internet shutdowns, deterring states from employing them as tools of control or warfare. By integrating internet access into existing human rights treaties, the international community could resolve interpretive ambiguities and strengthen accountability mechanisms. This legal evolution would align with the internet's transformative role in modern society, where it serves as a lifeline for human survival and dignity, especially in crises.

In wartime, when civilians face heightened risks, connectivity is not a luxury but a necessity for survival, enabling access to real-time safety alerts, telemedicine, and communication with loved ones. The deliberate denial of this access, often justified under

vague national security pretexts, exacerbates human suffering and undermines human rights. By advocating for the recognition of internet access as a human right, this study underscores the urgent need to prioritize civilian protection in war zones, ensuring that no one is left disconnected when access to information can mean the difference between life and death.

Use of artificial intelligence

xAI (2025). Grok AI model. https://grok.com/. Used exclusively for improving grammar and syntax. No third-party funding was involved in this process.

Bibliography

#KeepItOn (2019). «Targeted, Cut off, and Left in the Dark: The #KeepItOn Report on Internet Shutdowns in 2019». Access Now. https://www.accessnow.org/wp-content/uploads/2020/02/KeepItOn-2019-report-1.pdf.

ANTONIUK, Daryna (2022). «People under Russian Occupation Cut off from Internet, Mobile Connection». The Kyiv Independent. https://kyivindependent.com/russia-descends-iron-curtain-over-occupied-land-cuts-people-off-internet/.

Asriran (2025). «Deputy Minister of Communications: The Drone Shot down in Qom Was Carrying an American Satellite Modem». Asriran. https://www.asriran.com/fa/news/1071125/.

AZIM, Saadia (2025). «Why Shutting Down the Internet in Wartime Is a Humanitarian Failure». Internet Society. https://pulse.internetsociety.org/blog/why-shutting-down-the-internet-in-wartime-is-a-humanitarian-failure.

BALMFORTH, Tom (2024). «Russian Hackers Were inside Ukraine Telecoms Giant for Months». Reuters. https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/.

BARRY, Jack (2014). «Don't Be Evil: Should Access to the Internet Be Conceptualized as an Instrumental Human Right?». *SSRN Electronic Journal*, August: 1-24. https://doi.org/10.2139/SSRN.2480243.Burgess, Matt (2025). «Iran's Internet Blackout Adds New Dangers for Civilians Amid Israeli Bombings». Wired. https://www.wired.com/story/iran-internet-shutdown-israel/.

CERF, Vinton G. (2012). «Internet Access Is Not a Human Right». The New York Times. https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html.

CHUTEL, L. (2019). «Zimbabwe's Government Shut down the Internet after Fuel Price Protests Turned Deadly». Quartz Africa. https://qz.com/africa/1524405/zimbabwe-protest-internet-shut-down-military-deployed-5-dead/.

CRISTIANO, Fabio (2019). «Internet Access as Human Right: A Dystopian Critique from the Occupied Palestinian Territory». In Andreas von Arnauld, Kerstin von der Decken, and Mart Susi (eds.), *The Cambridge Handbook on New Human Rights*. Cambridge: Cambridge University Press, 249–268.

DAS, Mousumi and Sambedan Panda (2021). «Internet Accessibility as a Fundamental Right». *Asiatic Society for Social Science Research (ASSSR)*, 3 (1): 8-15. https://doi.org/10.46700/ASSSR/2021/V3/I1/209830.

DINSTEIN, Yoram (2002). «Computer Network Attacks and Self-Defense». *International Law Studies*, 76: 99–120.

Fararu (2021). «Government Spokesperson's Explanation about Internet Shutdown». Fararu. https://fararu.com/fa/tiny/news-877142.

GARNER, Bryan A. (2004). Black's Law Dictionary, Eighth, Thomson West.

GEORGE, A. Shaji (2024). «Universal Internet Access: A Modern Human Right or a Path to Digital Colonialism». *Partners Universal International Innovation Journal*, 2 (2): 55–74.

GHANNAM, Jeffrey (2011). «Social Media in the Arab World: Leading up to the Uprisings of 2011». *Center for International Media Assistance*.

GREGORIO, Giovanni De and Nicole Stremlau (2020). «Internet Shutdowns and the Limits of Law». *Documents of the African Commission on Human and Peoples' Rights*, 14: 1–19. https://doi.org/10.5040/9781472562432.CH-001.

Hamshahrionline (2023). «The Instagram Filter Decision Was Made in the Secretariat of the Supreme National Security Council». Hamshahrionline. https://hamshahrionline.ir/x8hQG.

HERT, Paul De and Dariusz Kloza (2012). «Internet (Access) as a New Fundamental Right: Inflating the Current Rights Framework?». *European Journal of Law and Technology*, 3 (3): 1-15.

HOWARD, Philip (2011). «When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media». *The Communication Review*, 14 (3): 216–232.

HUSSAIN, Abid (2002). «Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression». UN Doc. E/CN.4/2002/75.

HUTCHINS, Todd Emerson (2020). «Safeguarding Civilian Internet Access During Armed Conflict: Protecting Humanity's Most Important Resource in War». *Science and Technology Law Review*, 22 (1): 127–180. https://doi.org/10.52214/STLR.V22I1.8056.

JOSEPH, Sarah (2012). «Social Media, Political Change, and Human Rights». *Boston College International and Comparative Law Review*, 35 (1): 145–188.

JOYNER, Christopher C. and Catherine Lotrionte (2001). «Information Warfare as International Coercion: Elements of a Legal Framework». *European Journal of International Law*, 12 (5): 825–865.

JUDAH, Tim (2022). «How Kyiv Was Saved by Ukrainian Ingenuity as Well as Russian Blunders». The Financial Times. https://www.ft.com/content/e87fdc60-0d5e-4d39-93c6-7cfd22f770e8.

KALHOR, Hanieh (2025). «War and Internet Blackout: Disruption and Disconnection Amid Cyberattacks». Zoomit. https://www.zoomit.ir/tech-iran/442482-war-and-internet-outage/.

KRAPIVA, Natalia, Carolyn Tackett, Anastasiya Zhyrmont, Leanna Garfield, and Alexia Skok (2023). «Updates: Digital Rights in the Russia-Ukraine Conflict». Access Now. https://www.accessnow.org/digital-rights-ukraine-russia-conflict/.

LIM, Young Joon and Sarah E. Sexton (2011). «Internet as a Human Right: A Practical Legal Framework to Address the Unique Nature of the Medium and to Promote Development». *Washington Journal of Law, Technology & Arts*, 7: 296–318.

MATHIESEN, Kay (2012). «The Human Right to Internet Access: A Philosophical Defense». *The International Review of Information Ethics*, 18: 9–22. https://doi.org/10.29173/IRIE299.

MEHROTRA, Abhinav (2021). «Access to Internet as a Human Right – Justification and Comparative Study». *Comparative Law Review*, 27 (1): 313–327.

MICEK, Peter (2016). «Internet Disrupted in Bahrain around Protests as Wrestling Match Sparks Shutdown in India». Access Now. https://www.accessnow.org/internet-disrupted-bahrain-around-protests-wrestling-match-sparks-shutdown-india/.

MILLER, Maggie (2023). «Russia's Cyberattacks Aim to 'Terrorize' Ukrainians». POLITICO. https://www.politico.com/news/2023/01/11/russias-cyberattacks-aim-to-terrorize-ukrainians-00077561.

MIX, Cassondra (2014). «Internet Communication Blackout: Attack Under Non-International Armed Conflict». *J.L. & Cyber Warfare*, 3 (1): 70-90.

NetBlocks (2022). «Internet Disruptions Registered as Russia Moves in on Ukraine». NetBlocks. https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K.

NIKBAKHT, Banafsheh (2020). «The Ratio of Domestic to International Internet Traffic Will Be 70 to 30». Zoomit. https://www.zoomit.ir/tech-iran/345524-internet-ratio-domestic-internet-international/.

O'HARA, Kieron and David Stevens (2006). *Inequality.Com: Politics, Poverty and the Digital Divide*. Oxford: Oneworld Publications.

O'MEARA, Chris (2025). «Self-Defence in Outer Space: Anti-Satellite Weapons and the Jus Ad Bellum». *Leiden Journal of International Law*, 38: 1–23. https://doi.org/10.1017/S0922156524000670.

POLLICINO, Oreste (2019). «Right to Internet Access: Quid Iuris?». In Andreas von Arnauld, Kerstin von der Decken, and Mart Susi (eds.), *The Cambridge Handbook on New Human Rights*. Cambridge: Cambridge University Press, 1–12.

REGLITZ, Merten (2020). «The Human Right to Free Internet Access». *Journal of Applied Philosophy*, 37 (2): 314–331. https://doi.org/10.1111/JAPP.12395.

REGLITZ, Merten (2023). «The Socio-Economic Argument for the Human Right to Internet Access». *Politics, Philosophy & Economics*, 22 (4): 441–469. https://doi.org/10.1177/1470594X231167597.

Reuters (2010). «Four in Five Believe Web Access a Fundamental Right». Reuters. https://www.reuters.com/article/technology/four-in-five-believe-web-access-a-fundamental-right-idUSTRE6261XQ/.

Reuters (2022). «Russia Reroutes Internet Traffic in Occupied Ukraine to Its Infrastructure». Reuters. https://www.reuters.com/world/europe/russia-reroutes-internet-traffic-occupied-ukraine-its-infrastructure-2022-05-02/.

RUE, Frank La (2011). «Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression». UN Doc. A/HRC/17/27. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf.

RYNG, Julia, Guillemette Guicherd, Judy Al Saman, Priyanka Choudhury, and Angharad Kellett (2022). «Internet Shutdowns: A Human Rights Issue». *The RUSI Journal*, 167 (4–5): 50–63. https://doi.org/10.1080/03071847.2022.2156234.

SATRIAWAN, Iwan, Tareq Muhammad Aziz Elven, and Tanto Lailam (2023). «Internet Shutdown in Indonesia: An Appropriate Response or a Threat to Human Rights». *Sriwijaya Law Review*, 7 (1): 19–46.

SHANDLER, Ryan and Daphna Canetti (2019). «A Reality of Vulnerability and Dependence: Internet Access as a Human Right». *Israel Law Review*, 52 (1): 77–98. https://doi.org/10.1017/S0021223718000262.

SKEPYS, Brian (2012). «Is There a Human Right to the Internet». *Journal of Politics and Law*, 5: 15–29.

SMITH, Peter Scharff (2012). «Imprisonment and Internet-Access: Human Rights, the Principle of Normalization and the Question of Prisoners Access to Digital Communications Technology». *Nordic Journal of Human Rights*, 30 (4): 454–482. https://doi.org/10.1080/18918131.2012.10749861.

SOUTER, David (2012). «Human Rights and the Internet: A Review of Perceptions in Human Rights Organisations». Association for Progressive Communications.

Statista (2024). «Internet - Iran». Statista. https://www.statista.com/outlook/co/digital-connectivity-indicators/internet/iran.

SZOSZKIEWICZ, Łukasz (2018). «Internet Access as a New Human Right? State of the Art on the Threshold of 2020». *Przegląd Prawniczy Uniwersytetu Im. Adama Mickiewicza*, 8: 49–62.

TABUSCA, Silvia-Maria (2010). «The Internet Access as a Fundamental Right». Romanian-American University.

Times (2022). «The Battle for Control Over Ukraine's Internet». Times. https://time.com/6222111/ukraine-internet-russia-reclaimed-territory/.

TULLY, Stephen (2014). «A Human Right to Access the Internet? Problems and Prospects». *Human Rights Law Review*, 14 (2): 175–195. https://doi.org/10.1093/HRLR/NGU011.

VARDANYAN, Lusine, Hovsep Kocharyan, and Ondrej Hamuľák (2024). «The Right to Internet Access: A New Fundamental Right or a New 'Platform' for Fundamental Rights». In *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law*, 70–92.

VILLADIEGO, Laura (2022). «Internet Access: A New Human Right?». Equal Times. https://www.equaltimes.org/internet-access-a-new-human-right?lang=en.

MISHCHENKO, Taras. (2025). «Musk switched off Starlink during Ukrainian counteroffensive in Kherson Oblast in 2022». Reuters. Ukrainska Pravda. https://www.pravda.com.ua/eng/news/2025/07/25/7523419/

WANG, Xiaowei (2013). «Time to Think about Human Right to the Internet Access: A Beitz's Approach». *Journal of Politics and Law*, 6 (3): 67–77. https://doi.org/10.5539/JPL.V6N3P67.

WANG, Xiaowei (2016). «A Human Right to Internet Access: A Gewirthian Approach». *Frontiers of Philosophy in China*, 11 (4): 652–670. https://doi.org/10.3868/S030-005-016-0044-3.

WILSON, T. (2019). «Sudan Internet Blackout Forces Battered Protesters to Rethink». Financial Times. https://www.ft.com/content/b1848126-8c0f-11e9-a1c1-51bf8f989972.

WINNINGER, Laura and Giulio Coppi (2024). «What They Did in the Shadows: Internet Shutdowns and Atrocities in Ukraine». Access Now. https://www.accessnow.org/internet-shutdowns-and-atrocities-in-ukraine/.

WOODARD, Colin (2003). «Estonia, Where Being Wired Is a Human Right». Christian Science Monitor. https://www.csmonitor.com/2003/0701/p07s01-woeu.html.

Young Journalists Club (2025). «Many Enemy Drones Are Controlled via the Internet / If We Are Forced to, the Internet Will Be Nationalized». Young Journalists Club. https://www.yjc.ir/00bcIx.

About the author

JAMSHID ZARGARI holds a Master of Laws (LL.M) at the University of Judicial Sciences and Administrative Services and is an Attorney at Law at the Iran Central Bar Association in Tehran, Iran. He is a Visiting Lecturer at the University of Applied Science and Technology. His postal address is Iran Central Bar Association, Tehran, Iran and his email is jamshidzargari94@gmail.com. ORCID: orcid.org/0000-0002-8004-2969.

Disclaimer

This article concerns an ongoing armed conflict. The opinions expressed herein are the sole responsibility of the author and do not necessarily reflect the official stance of the Faculty of Law of the University of Chile.