© The Author(s), 2026. Published by Cambridge University Press on behalf of American Society of International Law.

INTERNET SHUTDOWNS AND INTERNATIONAL LAW

This panel was convened on April 17, 2025 at 3:30 p.m. by its moderator, Gregory T. Nojeim, who introduced the panelists: Viviana Krsticevic, Asaf Lubin, and Evelyn Aswad.

Introductory Remarks by Gregory T. Nojeim

doi:10.1017/amp.2025.10059

I had the privilege of moderating the panel on internet shutdowns and international law with a true "dream team" of panelists. As the panelists explain, internet shutdowns vary in type and in extent, and are increasingly common. I would add two points: first, countries are becoming more adept at imposing internet shutdowns in a particular geographic area, and at imposing these shutdowns to target particular internet services. That is, sometimes, a shutdown will be limited to communications on Facebook or on another communications service. Second, countries are becoming more effective at coercing communication service providers to comply with shutdown mandates. This is because governmental officials can point to provider compliance in other geographies as precedent, and because countries increasingly require providers to locate data and personnel in-country. For providers, a localization mandate can increase the risk that non-compliance with a shutdown order will trigger the seizure of assets or the detention of personnel.

At the same time, the international law standards that apply internet shutdowns are quite strict, and it is fair to say that most of the internet shutdowns that have been documented do not meet international law requirements. Even when put in place to serve a legitimate public interest, internet shutdowns are seldom strictly necessary to achieve that governmental objective. This points up the problem of enforcement, and, indeed, the lack of an easily triggered and effective enforcement mechanism for unlawful internet shutdowns.

Finally, it must be recognized that internet shutdowns are a weighty imposition on the right to free expression, but also on the exercise of many, many other rights. As but one example, Article 25 of the International Covenant on Civil and Political Rights guarantees the right to vote. The internet facilitates the exercise of that right, regardless of whether internet voting is permissible. People use the internet to learn about candidates' positions and about their political parties, to assess whether the individual is qualified to vote in a particular jurisdiction, where the voting facility is located, how to get there, and whether they will face impediments to voting, such as intimidation. If the internet is shut down in the lead up to election and on election day, the right to vote is compromised.

Increasingly, we live our lives on-line. Internet connectivity is becoming key to jobs, friendships, familial relationships, food transportation, farming, children's education, entertainment—virtually all aspects of life. When that connectivity is severed by an act of government, the consequences can be dire.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 13:46:05, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2025.10059

International Human Rights Standards Relating to Internet Shutdowns

*By Evelyn Mary Aswad**

Freedom of expression is a key human right affected by various forms of Internet shutdowns. The global standard for freedom of expression is found in Article 19 of the International Covenant on Civil and Political Rights (ICCPR).[1] Article 19(2) of this treaty provides broad protections for expression on all topics, over any media and across frontiers.[2] It covers the right of speakers to convey information as well as the right of listeners to receive information.

That said, ICCPR Article 19 does allow governments to limit speech, but they bear the burden of proving that each part of a tripartite test is met. If one part of the test is not met, then the restriction is not permitted under this global standard. Specifically, Article 19(3) states that freedom of expression may "be subject to certain restrictions, but these shall only be such as are *provided by law* and are *necessary*: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals."[3]

The first test is called the "legality" test, which emerges from Article 19(3)'s requirement that restrictions be "provided by law." This test means that the law limiting speech be, *inter alia*, properly promulgated and clear.[4] So in analyzing the various forms of Internet shutdowns, this test would require an assessment of whether there was a properly promulgated law that authorized the shutdown, and whether such law was improperly vague.

The second test is the legitimacy test, which derives from Article 19(3)'s listing of legitimate public interest objectives. The test requires that the government's purpose in restricting speech be for one of those enumerated public interest objectives. Often governments improperly invoke these objectives when the real motivation is to protect themselves, including from criticism during protests or to prevent free elections. The UN Human Rights Committee (which monitors implementation of this treaty) has made clear that such pretextual reasons do not meet the legitimacy test.[5] Similarly, if such pretextual reasons were asserted in an Internet shutdown context, they too would fail this test.

The third test is the "necessity" test, which is linked to ICCPR Article 19(3)'s requirement that any speech restriction be "necessary." This test entails an analysis of the following two factors: (1) is the speech restriction the least intrusive means to achieve the legitimate public interest objective; and (2) is the speech restriction proportional, e.g., the burden on speakers and listeners must not be greater than the anticipated benefit from the restriction.[6]

In assessing whether a restriction is the least intrusive means to achieve a legitimate public interest aim, it is important to consider three questions.[7] First, can the aim be achieved without

* Evelyn Aswad is the Herman G. Kaiser Chair in International Law at the University of Oklahoma College of Law where she also serves as the Director of the International Business Law Online Graduate Degree Program and the Director of the Center for International Business & Human Rights. She thanks her fellow panelists for an illuminating discussion on the various aspects of analyzing Internet shutdowns.

[1] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 UNTS 171 [hereinafter ICCPR].

[2] *Id.* Art. 19(2).

[3] *Id.* Art. 19(3) (emphasis added).

[4] UN Human Rights Comm., General Comment No. 34, para. 35, UN Doc. CCPR/C/GC/34 (Sept. 12, 2011) [hereinafter GC 34].

[5] *Id.*, para. 30.

[6] *Id.*, para. 34.

[7] *See* David Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, para. 52, UN Doc. A/74/486 (Oct. 9, 2019).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 13:46:05, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2025.10059

burdening speech? If so, the restriction is not the least intrusive way to achieve the objective. But if the answer is no, then the second question is: of the range of tools that burden speech (e.g., civil versus criminal sanctions), is the selected tool the least burdensome on speech interests? If it is not, then the government has not selected the "least intrusive means," and the speech restriction is improper. Third, speech regulators must assess whether the speech restriction that has been imposed is effective in achieving the aim. If it is not, then the measure is not appropriate as it is burdening speech without furthering the legitimate objective. These rigorous tests will often mean that it will prove difficult for governments to demonstrate that an Internet shutdown was the "least intrusive means" of achieving a legitimate objective.

Two items are worth highlighting about ICCPR Article 19(3)'s three-part test. First, this test forces us to consider a series of principled questions. It is not an amorphous balancing test among competing rights.[8] Second, it is important to keep in mind that the UN human rights machinery's approach to freedom of expression is broader than that of certain regional systems, including with respect to the jurisprudence of the European Court of Human Rights.[9] For example, the UN Human Rights Committee has rejected assessing freedom of expression through the use of the European-developed "margin of appreciation" doctrine (which provides a measure of deference to governmental choices in various contexts).[10] In addition, the UN system applies both the least intrusive means and proportionality tests while the European Court focuses on the proportionality test, which results in the UN system affording greater protection for speech.[11]

It should be noted as well that ICCPR Article 4 allows governments to derogate from their obligations relating to certain rights, including the right to freedom of expression, in exceptional circumstances if specific conditions are met. First, there must be a "public emergency which threatens the life of the nation and the existence of which is officially proclaimed."[12] Second, the derogation is permissible solely to the "extent strictly required by the exigencies of the situation."[13] Third, the derogation cannot violate the country's other international law obligations. Fourth, the derogation cannot be implemented in a way that discriminates "solely on the ground of race, colour, sex, language, religion or social origin."[14] Fifth, the derogating state must give official notice to the UN about its derogation. These are significant hurdles for a government to properly derogate from its obligations. In the context of an Internet shutdown, it will be particularly important to analyze the extent to which an Internet shutdown is truly "strictly required" to deal with the public emergency that threatens the life of the nation.

Up until now we have been discussing the global standard on freedom of expression as applied to state actors. But what about corporate actors? Do they have human rights responsibilities if faced with orders or requests to enable Internet shutdowns? In 2011, the UN Human Rights Council adopted the UN Guiding Principles on Business & Human Rights (UNGPs), which set forth the international community's expectations of companies.[15] The UNGPs call on companies

[8] *See* David Kaye, *Against Balancing* (May 4, 2020), *at* https://dkisaway.medium.com/against-balancing-5ecc5dc2beb5.

[9] Evelyn Aswad & David Kaye, *Convergence & Conflict: Reflections on Global and Regional Human Rights Standards on Hate Speech*, 20 NW. J. HUM. RTS. 165, 190–98 (2022).

[10] GC 34, *supra* note 4, para. 36.

[11] Aswad & Kaye, *supra* note 9, at 208.

[12] ICCPR, *supra* note 1, Art. 4.

[13] *Id.*

[14] *Id.*

[15] Human Rights Council Res. 17/4, UN Doc. A/HRC/RES/17/4 (July 6, 2011); John Ruggie, Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises to the Human Rights Council, Prin. 11, UN Doc. A/HRC/17/31 (Mar. 21, 2011).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 13:46:05, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2025.10059

to respect international human rights standards by seeking to avoid infringing on human rights in their operations and addressing harms. The UNGPs are pegged to UN human rights standards.[16] This means companies are expected to, *inter alia,* engage in human rights due diligence (i.e., "know" their human rights risks) and be able to "show" what measures they have undertaken to avoid or mitigate the risks.[17]

A multistakeholder initiative called the Global Network Initiative (GNI) exists that brings together companies, investors, academics, and NGOs to seek to help Information, Communication & Telecommunications (ICT) companies understand how their operations risk free expression and privacy harms and to take measures to seek to avoid infringing on those rights.[18] If those ICT companies receive governmental requests to remove speech, including assisting with an Internet shutdown, they pledge to assess whether those requests, laws, and orders are consistent with global human rights standards on freedom of expression. If the governmental laws or requests are inconsistent with the global standards, those ICT companies pledge to seek to resist implementing those laws or requests to the extent possible. This can be done by, *inter alia,* interpreting requests narrowly, suing the governments in local courts, and enlisting the help of other actors, such as UN human rights watchdogs and other governments.[19] While the UNGPs and GNI do not require companies to violate local law, they do call on companies to conduct due diligence to understand the human rights risks of their operations and to take measures to avoid those harms.

Overall, ICCPR Article 19 makes it quite difficult for governments to engage in Internet shutdowns in a manner that is consistent with global freedom of expression standards. Moreover, corporate actors have been pulled into illicit governmental requests, pressure, and orders to assist in various forms of Internet shutdowns. These corporate actors should seek to abide by the UNGPs and respect Article 19's free expression protections. Though each particular Internet shutdown will present its own context and factors for consideration, global human rights standards compel the international community, including governments and corporate actors, to examine those situations by asking a series of principled questions and answering them in a disciplined and transparent manner, which makes these global standards relevant, if not crucial, in the digital age.

The Law and Politics of Internet Shutdowns

*By Asaf Lubin**

In June 2025, the Islamic Republic of Iran orchestrated one of the most sweeping internet shutdowns in its recent history, severing digital communications nationwide at a moment of acute societal and geopolitical uncertainty. The measures coincided with an intensifying war with Israel

[16] *Id.*, Prin. 12 and commentary.

[17] *See* Evelyn Aswad, *The Future of Freedom of Expression Online*, 17 Duke L. & Tech. Rev. 26, 38–40 (2018).

[18] Global Network Initiative, *at* https://globalnetworkinitiative.org.

[19] *Implementation Guidelines*, Glob. Network Initiative, *at* https://globalnetworkinitiative.org/implementation-guidelines.

* Asaf Lubin is an Associate Professor at Indiana University Maurer School of Law and a Faculty affiliate at both Harvard's Berkman Klein Center for Internet and Society and Yale's Information Society Project. Prof. Lubin served on the Organizing Committee of the 119th American Society of International Law Annual Meeting. I wish to thank Katelyn Horne and Nawi Ukabiala for the invitation to join the panel and to Gregory Nojeim, Evelyn Aswad, and Viviana Krsticevic for an excellent session which helped me tremendously in the development of these remarks.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 13:46:05, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2025.10059

that included airstrikes, missile launches, and heightened military alerts across the region.[1] Beginning with network throttling on June 13 and escalating to a near-total blackout by June 18, the shutdown left millions of Iranians abruptly cut off from the outside world.[2]

In a televised address, government spokesperson Fatemeh Mohajerani defended the blackout as "temporary, targeted, and controlled, aimed at countering cyberattacks."[3] The Iranians had good reason to worry. In the days leading up to the shutdown, the hacker collective Predatory Sparrow publicly claimed responsibility for a series of sophisticated cyberattacks, including disabling Iran's Bank Sepah,[4] and draining "more than $90 million from Nobitex, Iran's largest cryptocurrency exchange."[5] Still, the severity, scope, and timing of the blackout suggest a deeper political calculus—one oriented less toward defending networks, than toward quelling political unrest. For nearly a week, Iranians were effectively sealed off from the outside world, with domestic platforms barely operational and international communication dependent on VPNs or satellite relays such as Starlink.[6] One digital rights analysis observed that the "extensive censorship and internet disruption" were employed by the regime primarily to control information, especially in and around the city of Tehran.[7] The tactic was not without precedent. The city of Tehran had already witnessed this playbook during the 2022 regional blackouts that followed the death of Mahsa Amini.[8]

As courts, lawmakers, and international bodies grapple with the legal frameworks governing such disruptions, Iran's June blackout offers a stark reminder of what is at stake. The episode underscores how internet shutdowns have emerged as dual-use instruments of statecraft. These instruments are readily adaptable to serve a broad spectrum of sovereign interests, from legitimate security objectives to more troubling agendas of censorship, suppression, and control.

I. Defining Internet Shutdowns

An "internet shutdown" is a state-imposed disruption of online access—whether full or partial, temporary or indefinite. While no customary definition of the term is available, the #KeepItOn Coalition, comprised of 334 local, national, regional, and international organizations and led by Access Now, has developed a definition it has crowdsourced through consultation with its members: "Internet shutdown: An intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information."[9]

[1] Emmanuel Fabian, *The Israel-Iran War by the Numbers, After 12 Days of Fighting*, Times of Israel (June 24, 2025), *at* https://www.timesofisrael.com/the-israel-iran-war-by-the-numbers-after-12-days-of-fighting.

[2] Kevin Collier, *Iran Plunged into an Internet Near-Blackout During Deepening Conflict*, NBC News (June 17, 2025), *at* https://www.nbcnews.com/tech/internet/iran-plunged-internet-blackout-deepening-conflict-rcna213544.

[3] Tina Nguyen, *Iran Is Going Offline to Prevent Purported Israeli Cyberattacks*, Verge (June 17, 2025), *at* https://www.theverge.com/politics/688875/iran-cutting-off-internet-israel-war.

[4] *Cyberattack on IRGC-Controlled Bank Causes Disruptions, Iranian Media Claims*, Jerusalem Post (June 17, 2025), *at* https://www.jpost.com/middle-east/iran-news/article-858033.

[5] Gabe Levin, *Hackers Reportedly Wipe Out $90 Million from Largest Iranian Cryptocurrency Exchange*, PBS News (June 19, 2025), *at* https://www.pbs.org/newshour/world/hackers-reportedly-wipe-out-90-million-from-largest-iranian-cryptocurrency-exchange.

[6] Farnoush Amiri, *Iran's Internet Blackout Leaves Public in Dark And Creates an Uneven Picture of the War with Israel*, AP (June 20, 2025), *at* https://apnews.com/article/iran-internet-blackout-israel-war-6aa315eff871579f8bfc220ce3930e5f.

[7] Matt Burgess, *Iran's Internet Blackout Adds New Dangers for Civilians Amid Israeli Bombings*, Wired (June 18, 2025), *at* https://www.wired.com/story/iran-internet-shutdown-israel.

[8] Weronika Strzyżyńska, *Iran Blocks Capital's Internet Access as Amini Protests Grow*, Guardian (Sept. 22, 2022), *at* https://www.theguardian.com/world/2022/sep/22/iran-blocks-capitals-internet-access-as-amini-protests-grow.

[9] Deji Olukotun & Peter Micek, *No More Internet Shutdowns! Let's #KeepItOn*, Access Now (Mar. 30, 2016, last updated Jan. 26, 2023), *at* https://www.accessnow.org/no-internet-shutdowns-lets-keepiton.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 13:46:05, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2025.10059

As this definition demonstrates, internet shutdowns can take many forms depending on the techniques used, the scope of the interruption intended, and the motivations behind the shutdown.[10] The definition rightly notes that internet shutdown are most frequently used to "exert control over the flow of information." In so doing, the disrupting government seeks to suppress resistance, contain protest or association, and distort or redirect public discourse. Yet there are other reasons why a country may choose to shut down parts of the internet. For example a government may claim that it is responding to a security concern, either physical or in cyberspace, which the shutdown could presumably help prevent or mitigate. Moreover, internet shutdowns can also be used as a tactic in war. In this context, a belligerent may seeks to gain some battlefield advantage through attacking or disrupting the internet communications of their adversary.

The most sweeping form of an internet shutdown is a complete national blackout, where a government orders internet service providers to disable all traffic, effectively cutting off the country from the global internet. A striking example of this occurred in Myanmar in February 2021, following the military coup. The junta imposed nightly Internet blackouts and, eventually, multi-day shutdowns in an attempt to stifle organizing by pro-democracy protesters.[11] A similar approach had been deployed in Egypt in January, 2011. At the height of the revolution against former President Mohamed Hosni Mubarak, "Egyptians experienced a complete shutdown of all mobile services, including internet access, by the three telecommunication operators, namely Vodafone, Mobinil, and Etisalat, with no prior notice, in an effort to limit the extent of demonstrations."[12]

A slightly more targeted approach involves regional shutdowns, in which access is selectively disabled within particular geographic areas facing political unrest. Between 2019 and 2021, the Indian government employed such a measure in Jammu and Kashmir, suspending landline, mobile, and internet services in response to its decision to revoke the region's constitutional autonomy.[13] And at the most selective end of the spectrum lies platform-specific blocking. These tactical shutdowns are designed to disrupt the core tools of coordination and public messaging, while preserving access to other services in order to mitigate the broader economic consequences typically associated with a nationwide or regional blackout. For example, during anti-government protests in 2021, the Cuban authorities blocked access to messaging apps like Telegram, Signal, and WhatsApp to hinder the organization of demonstrations.[14]

Internet shutdowns, however, are more than just domestic tools of repression. They have also been weaponized to support war efforts. Consider Russia's 2022 invasion of Ukraine. In the hours preceding the kinetic assault, a cyberattack on the Viasat satellite network disabled internet connectivity for tens of thousands of users across Europe, including key Ukrainian governmental

[10] *See, e.g.*, Steven Feldstein, *Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?*, Carnegie Endowment Int'l Peace, 7–19 (Working Paper, Mar. 2022), *at* https://carnegieendowment.org/research/2022/03/government-internet-shutdowns-are-changing-how-should-citizens-and-democracies-respond?lang=en#trends.

[11] *Myanmar: New Internet Blackout "Heinous and Reckless,"* Amnesty Int'l (Feb. 6, 2021), *at* https://www.amnesty.org/en/latest/press-release/2021/02/myanmar-new-internet-blackout.

[12] Columbia U. Glob. Freedom Expression Initiative, *The Case of Communications Suspension and Internet Shutdown During the 2011 Egyptian Revolution*, *at* https://globalfreedomofexpression.columbia.edu/cases/communications-suspension-and-internet-shutdown-case-during-the-2011-egyptian-revolution.

[13] Human Rights Watch, *"No Internet Means No Work, No Pay, No Food,"* (June 14, 2023), *at* https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic.

[14] Sarah Marsh & Elizabeth Culliford, *Faced with Rare Protests, Cuba Curbs Social Media Access, Watchdog Says*, Reuters (July 13, 2021), *at* https://www.reuters.com/world/americas/cuba-curbs-access-facebook-messaging-apps-amid-protests-internet-watchdog-2021-07-13.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 13:46:05, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2025.10059

and military systems.[15] Western intelligence agencies attributed the attack to Russian operatives. Once Russian forces were able to secure control over parts of eastern Ukraine, they moved to re-route all internet traffic from the occupied territories through Russian infrastructure, an act that subjected the local population to further censorship, surveillance, and disinformation.[16]

II. Why Are Internet Shutdowns So Difficult to Regulate?

The #KeepItOn Coalition's Shutdowns Tracker Optimization Project (STOP) provides the most comprehensive annual documentation and analysis of the global landscape of internet shutdowns. Its findings paint a troubling picture: both the frequency and geographic spread of shutdowns have increased markedly over the past decade. In 2016, there were seventy-eight recorded incidents of internet shutdowns worldwide. By 2024, that number had nearly quadrupled, reaching 296 documented cases. Equally notable is the growing number of states resorting to this tactic. Whereas shutdowns were reported in twenty-seven countries in 2016, by 2024 that figure had doubled to fifty-four—signaling a steady diffusion of this digital playbook across diverse political regimes and regions (see Figure 1).

The sharp rise in internet shutdowns poses a serious threat to fundamental human rights. Each disruption severs access to essential services—interrupting work, education, healthcare, and banking—while further silencing journalism and stifling dissent. In times of armed conflict, shutdowns can block life-saving information and hinder humanitarian efforts. Why, then, has international law struggled to restrain them?

Internet shutdowns are difficult to regulate because they unfold in legal and evidentiary gray zones. Attribution poses a central obstacle: these operations are frequently conducted in secret, through opaque channels, further obscured by the technical complexity of network interference. Identifying who authorized the shutdown, for what purpose, and by what means is often a fraught undertaking.

To complicate matters even further, recall that internet shutdowns are not by themselves inherently illegal. They can serve legitimate purposes. Yet, as Giovanni de Gregorio and Nicole Stremlau have noted, "[d]etermining whether, and under what circumstances, Internet shutdowns might be justified is challenging."[17] The difficulty lies in the application of international human rights law (IHRL) and international humanitarian law (IHL) in each of these cases.

Under IHRL, internet shutdowns routinely implicate rights to expression, access to information, privacy, education, health, and non-discrimination. Yet none of these rights is absolute. States may impose restrictions on these rights for national security or public order, provided they satisfy the tests of legality, necessity, and proportionality. During declared emergencies, certain rights may even be derogated outright, to the extent strictly required by the exigencies of the situation. Consider the Iranian case study with which this article began. Given the crippling cyberattacks the country endured and the ongoing threat of further attacks, was it legitimate for the government to impose such a shutdown? Did the Iranians have alternative less intrusive measures? Were the cyberattacks the real motivation and not population control? Is population control in times of crisis and war ever legitimate? These are hard questions to answer as a matter of both law and fact.

[15] Cyber Peace Inst., *Case Study: Viasat*, *at* https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

[16] Adam Satariano & Scott Reinhard, *How Russia Took Over Ukraine's Internet in Occupied Territories*, N.Y. Times (Aug. 9, 2022), *at* https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html.

[17] Giovanni de Gregorio & Nicole Stremlau, *Internet Shutdowns and the Limits of the Law*, 15 Int'l. J. Comm. 4224, 4237 (2020).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 13:46:05, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2025.10059

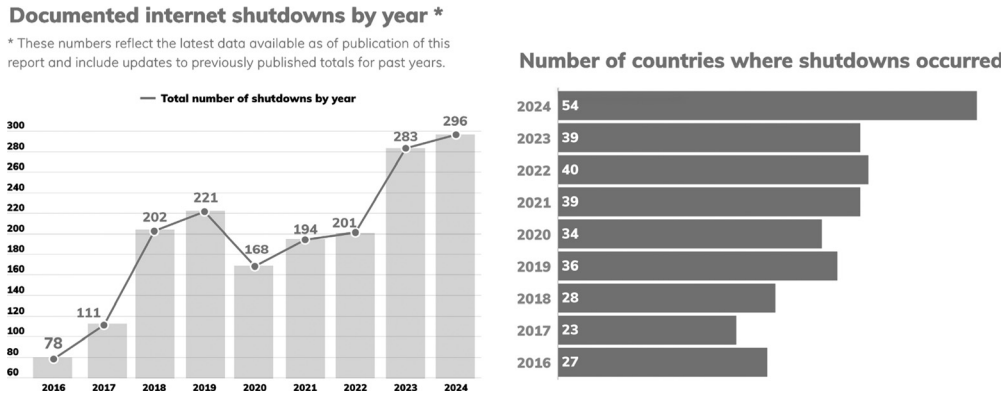


Figure 1. Illustration: "STOP" Records for the period ranging from 2016 to 2024 of total numbers of documented internet shutdowns globally.[18]

The concurrent application of IHRL and IHL generates an even further contested space within which to apply these rights.[19] That the core rules of IHL were drafted in a pre-digital era only compounds the uncertainty. Consider the Russian cyberattack on the Viasat satellite network: was the infrastructure a lawful military objective, given its dual civilian and military use? Does the widespread disruption to civilian connectivity constitute harm that IHL must recognize? And if so, can such harm ever be squared with the principles of distinction and proportionality, or the prohibition on collective punishment? These questions are routinely debated.

Taken together, the expanding use of internet shutdowns in both peacetime and armed conflict underscores the profound legal ambiguities that continue to surround the practice. What is at stake is the normalization of a digital future in which entire populations can be cast into silence at the flip of a switch—precisely when their access to information, and their ability to speak, is most urgently needed.

[18] Emboldened Offenders, Endangered Communities: Internet Shutdowns in 2024, #KeepItOn, 4 (Feb. 2025), *at* https://www.accessnow.org/wp-content/uploads/2025/02/KeepItOn-2024-Internet-Shutdowns-Annual-Report.pdf.

[19] *See generally* The Rights to Privacy and Data Protection in Times of Armed Conflict (Russell Buchan & Asaf Lubin eds., 2022).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 13:46:05, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/amp.2025.10059