Legal explainer: Internet and telecommunications shutdowns in the assessment of international crimes

An International Criminal Court decision and the way ahead

Published in February 2024

Acknowledgements

This report is an Access Now publication, written by Laura Winninger.

The author would like to thank the Access Now team members who provided support, including Aymen Zaghdoudi, Carolyn Tackett, Donna Wentworth, Giulio Coppi, Laura O'Brien, Marwa Fatafta, Natalia Krapiva, and Peter Micek.

Legal explainer: Internet and telecommunications shutdowns in the assessment of international crimes

Introduction

Intentionally disconnecting people from the outside world is a powerful method to increase their vulnerability to violence. Data shows that in areas of conflict and unrest, where connectivity becomes a lifeline, shutdowns or disruptions of internet and telecommunications services occur on a regular basis. As national and regional courts increasingly address the human rights implications of internet shutdowns, and discussions on atrocity crimes committed in Ukraine and Gaza unfold, the question arises as to what role shutdowns of internet and telecommunications services play in the assessment of international crimes.

Our analysis revealed that the case law on international criminal liability in connection with internet and telecommunications shutdowns is currently sparse. However, in 2011, the International Criminal Court's (ICC) Pre-Trial Chamber I considered disruptions of internet and telecommunications services to be evidence of a State policy in crimes against humanity.

This recognition of shutdowns' relevance in the assessment of crimes against humanity should encourage digital rights advocates to promote further progress in preventing and finding accountability for their use as tools to facilitate or conceal international crimes.

Shutdowns as evidence of a State or organizational policy in crimes against humanity

To qualify as a crime against humanity under Article 7 of the Rome Statute, an attack against civilians must, *inter alia,* be committed in "furtherance of a State or organizational policy to commit such attack."

The ICC has consistently kept the threshold for satisfying the so-called "policy element" relatively low. In practice, the policy requirement is met when an attack is directed, organized, or planned rather than occurring spontaneously or as "isolated acts of violence."[1] Besides, the policy does not need to be formalized,[2] since it can crystallize as actions are carried out by the perpetrators.[3]

Whether a State or organizational policy exists can generally "be inferred by discernment of, *inter alia*, repeated actions occurring according to the same sequence, or the existence of preparations or collective mobilization orchestrated and coordinated by [the relevant] State or organization."[4]

A key example of a tech-conscious analysis of the policy element occurred in the Situation in Libya, which the United Nations Security Council referred to the ICC, noting that the attacks against the civilian population during the Arab Spring protests "may amount to crimes against humanity."

[1] *Katanga and Ngudjolo Chui,* Pre-Trial Chamber I, 30 September 2008, § 396.
[2] *Bemba*, Pre-Trial Chamber II, 15 June 2009, § 81.
[3] *Katanga*,Trial Chamber II, 7 March 2014, § 1110.
[4] *Ibid.* at § 1109.

Following investigations, the ICC Prosecutor sought arrest warrants for *Muammar Mohammed Abu Minyar Gaddafi*, his son *Saif Al-Islam Gaddafi*, and *Abdullah Al-Senussi*, based on the claim that the accused had committed crimes against humanity (murder and persecution) through the Libyan State apparatus and security forces from 15 February 2011 onwards.

In the application for the issuance of the arrest warrants, the ICC Prosecutor explained that

> *"the total number of incidents and ensuing casualties remain undetermined due to the widespread cover-up carried out by the Security Forces for the purpose of hiding the evidence of past crimes and facilitating the commission of future ones. This cover-up has taken numerous forms: internet services and cell phone networks were disrupted [...]"*[5]

The ICC Pre-Trial Chamber I incorporated this explanation in its assessment of the policy element, as it held that "repeatedly blocking satellite transmission of [TV] channels [...] and disrupting internet and telecommunications services"[6] was relevant evidence to find that "there [were] reasonable grounds to believe" that a State policy existed.[7]

Shutdowns and evidence of international crimes in the digital age

The Pre-Trial Chamber I's decision legally substantiates civil society groups' support of legal action[8] regarding attacks on civilians through evidence of internet and telecommunications shutdowns.

Yet, while the acknowledgment of shutdowns' relevance in the ICC decision marks progress in the fight against impunity, it is insufficient to deter authorities from shutting down internet and telecommunications services during conflicts and civil unrest.

The consequences of a persistent use of shutdowns in high-risk scenarios are severe. Not only does the lack of connectivity in times of conflict rob individuals of crucial means to seek help, receive advance warnings of attacks, or access humanitarian aid, it also deprives people of the ability to document on-the-ground events and to share vital information online.

---

[5] "Prosecutor's Application Pursuant to Article 58 as to Muammar Mohammed Abu Minyar GADDAFI, Saif Al-Islam GADDAFI and Abdullah AL-SENUSSI," 16 May 2011, § 28.
[6] "Decision on the Prosecutor's Application Pursuant to Article 58 as to Muammar Mohammed Abu Minyar Gadaffi, Saif Al-Islam Gadaffi and Abdullah Al-Senussi," Pre-Trial Chamber I, 27 June 2011, § 30.
[7] *Ibid.* at § 31.
[8] In international courts and national courts, notably when the latter were provided with universal jurisdiction over international crimes and, thus, the ability to try persons for crimes committed outside their State's territory; for more context on universal jurisdiction and its limitations, see https://voelkerrechtsblog.org/one-court-at-a-time-challenges-of-universal-jurisdiction-and-enhancing-international-justice/.

This, in turn, may adversely impact efforts to hold perpetrators accountable for atrocities, given the growing reliance of courts, including the ICC, on internet-based evidence, such as social media posts,[9] in evaluating international crimes.

The way ahead?

In view of the above, the Pre-Trial Chamber I's decision in the Situation in Libya is only a starting point in addressing shutdowns of internet and telecommunications services in the context of international crimes.

Experts working in international criminal law are increasingly recognizing the importance of the digital dimension of international crimes. A case in point is the ICC Office of the Prosecutor's recent commitment to making cyber-enabled crimes a thematic focus in 2024, or the Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare, which examined, *inter alia*, the application of Article 7 of the Rome Statute to cyber operations.

However, due to the fact that shutdowns of internet and telecommunications services facilitate crimes by rendering connectivity-based technology useless (rather than by exploiting their functions), shutdowns are at risk of being overlooked in initiatives which explore how digital technology enables international crimes.

Against this backdrop, it is essential that legal and tech experts make a conscious effort to delve deeper into the role of shutdowns in the commission of international crimes and to work towards enhancing protections against their use as tools to facilitate or conceal atrocities.

Call to action

---

1. **We call on courts with jurisdiction over international crimes (i) to examine the precedent set by the ICC Pre-Trial Chamber I in the Situation in Libya, and (ii) to give due consideration to shutdowns and disruptions of internet and telecommunications services in evaluating the cases brought before them.**

---

2. **We call on digital rights advocates and civil society organizations to advocate for courts to include the prompt restoration of civilian telecommunications networks in provisional measures in relevant cases.**

---

[9] See, for example, *Al-Werfalli*, Pre-Trial Chamber I, 15 August 2017, § 3; for more context on the relevance of social media posts as evidence in the assessment international crimes, see https://theintercept.com/2017/11/02/war-crimes-youtube-facebook-syria-rohingya/.

3. **We call on legal practitioners and experts to conduct further research on the interrelation between interferences with digital rights and international crimes, notably the interrelation between shutdowns of internet and telecommunications services and attacks against civilians.**

---

4. **We call on tech and telecommunication companies (i) to consider the implications of shutdowns and disruptions of internet and telecommunications services during situations of violence, and (ii) to take action to ensure full transparency in cases of service interference, notably by establishing robust public reporting mechanisms and preserving relevant documentation, as appropriate in respect of international human rights laws and norms.**

---

5. **We call on UN Member States and their Delegations to consider the digital dimension of international crimes in general, and of crimes against humanity in particular, as the UN Security Council refers situations to the ICC, and the the UN General Assembly Sixth Committee resumes the discussion on the Draft Articles on Prevention and Punishment of Crimes Against Humanity in April 2024.**

For more information, visit www.accessnow.org.

Contact:
legal@accessnow.org

Access Now defends and extends the digital rights of people and communities at risk. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.