International Journal of Communication 14(2020), 4224–4243 1932–8036/20200005

Internet Shutdowns and the Limits of Law

GIOVANNI DE GREGORIO[1]
University of Milano-Bicocca, Italy

NICOLE STREMLAU[2]
University of Oxford, UK

Internet shutdowns are on the rise. In the past few years, an escalation of this blunt censoring practice has affected different regions of the world, particularly Africa and Asia. Scholars and advocates have proposed no substantive solutions to effectively address Internet shutdowns, and analysis has largely been limited to examining the negative effects through data about their frequency, duration, and economic costs. This article attempts to move beyond the polarized debate between "keep it on" and "shut it off" to explore how there can be more transparency around decision-making processes behind Internet shutdowns. We also discuss the limits of law when it comes to the imposition and implementation of shutdowns. Shutdowns tend to be imposed somewhat arbitrarily with little process. Bringing back legal arguments into the exploration of the justifications around shutdowns may make the use of shutdowns less frequent and more limited, when they do occur.

Keywords: Internet shutdowns, human rights, freedom of expression, Internet access, information intervention, social media

Whether, when, and how to censor content on the Internet, and in what cases it might be justified, has increasingly become an area of contentious debate in an era of growing misinformation and hate speech online (Clark, 2017). Governments and corporations around the world have adopted massive forms of surveillance and are actively investing in and refining ways of monitoring data and information, including both human and machine-led techniques (Deibert, 2008; Warf, 2011). Within this broader array of tools for controlling content and access online, Internet shutdowns have increased in scale and scope, particularly in

Giovanni De Gregorio: g.degregorio@campus.unimib.it
Nicole Stremlau: nicole.stremlau@csls.ox.ac.uk
Date submitted: 2019–10–28

[1] This research is part of the ConflictNet project (The Politics and Practice of Social Media in Conflict). Further information can be found at https://pcmlp.socleg.ox.ac.uk/. It has been funded by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (Grant Agreement No. 716686, ConflictNET).
[2] Also with the University of Johannesburg, South Africa.

Asia and Africa. From India, that has had many localized Internet shutdowns (more than 100 in 2018; Bahree, 2018), to Cameroon, that brazenly blocked access in half of the country for more than 230 days between 2017 and 2018 (Dahir, 2018a), shutting down the Internet (either partially or entirely) appears to be used by governments when they want to act quickly, particularly to quell perceived or potential civil unrest, and might have limited capacity for other mechanisms of online control.

When Internet shutdowns occur, they are usually met with condemnation by free speech advocates and Internet freedom groups such as Access Now. Responses have, however, recently become more nuanced out of an increasing frustration with the slowness of social media companies to respond to online hate speech, and there is a growing debate around the responsibilities of these actors (De Gregorio, 2019; Suzor, 2019). The Christchurch Call, led by New Zealand Prime Minister Jacinda Ardern, and French President Emmanuel Macron, to "eliminate" (if such a thing is possible) terrorist and violent extremist content online in the wake of the March 2019 terrorist attack are two examples of the current situation.

Internet shutdowns also occur in consolidated democracies. For example, in 2019, British police shut down the public's access to the Internet on the London underground to tackle planned protests by climate protesters (Embury-Dennis, 2019). A similar tactic had been already implemented in the epitome of technological liberalism, San Francisco, in 2011, where mobile-Internet and phone services were shut down to control a protest in the subway (Kravets, 2011). And both the UK and U.S. have had extensive national debates about the relevance and applicability of what is often referred to as the "Internet kill switch," or a mechanism for shutting off the Internet entrusted to a single authority (Thompson, 2011).

Unlike the libertarian narrative around the Internet that developed around the end of the last century (Barlow, 1996; Johnson & Post, 1996) and still influences many perspectives on minimal regulation speech online, particularly in the U.S., the effective implementation of Internet shutdowns can be seen as one tool within the range of mechanisms with which the state can interfere with the digital environment (Goldsmith & Wu, 2006). When it comes to regulation, governments can impose their control over the Internet through various mechanisms, including law, social rules, and economic and network architecture (Lessig, 2006). States, especially authoritarian regimes, relied on the hierarchical physical infrastructure of the Internet not just to regulate it, but to block access and shut down the digital environment (Freyburg & Garbe, 2018).

The effects of Internet shutdowns by virtue of the role of the digital environment in today's society cannot be neglected. The Internet is not only relevant from a technical or economic perspective (OECD Digital Economy Outlook, 2017), but also for the exercise of democratic values such as assembly and freedom of expression and, therefore, as a crucial source of information and knowledge. Notwithstanding the traditional channels of information—TV and radio—that continue to play a fundamental role in the creation and dissemination of content, the Internet has evolved into an important forum for the approximately 50% of the global population that is online (Dahir, 2018b). Marginalization and exclusion from the Internet are still a major issue, particularly in many of the countries that are affected by largescale Internet shutdowns.

When states decide to block access to the Internet, they are interfering with important communications networks, no matter what justifications are in place. Many advocacy groups tie this to the interference of freedom of expression. This is an important argument and, as it is the most used one, will be central to this article. Nevertheless, we have to preface that Internet access per se is not recognized by the UN as a human right (Pollicino, 2019). Too often the area between access, human rights, and free expression is muddled. The movement around the "right to connect," or the "freedom to connect," essentially argues that Internet access is essential for people to enjoy their rights to freedom of expression. In 2016, the UN argued that "the same rights people have offline must also be protected online" and expressing concern with measures that "intentionally prevent or disrupt access to or dissemination of information online," (Human Rights Council, 2016, res. 32/13, para. 10) directly referring to Internet shutdowns. While recognizing this growing movement, we also urge caution and nuance. Indeed, Internet access has not (at least yet) been recognized as a human right, much in the same way that access to certain mediums (such as radio or newspapers) or platforms are also not differentiated as rights. The crucial aspect here is that technology may be "an enabler" of rights (Human Rights Council, 2018), a tool and mechanism for enabling freedom of expression, but like the telephone, access to it is not a human right.

In this context, the primary concern of this article does not involve assessing if an Internet shutdown affects freedom of expression, but whether the limitations implemented by state actors can be justified and, if so, according to which legal conditions. Ultimately, we argue, Internet shutdowns do not appear to be abating, in line with an increasing trend censor speech for fighting cybercrime or disinformation. Therefore, there is a need for a new political and policy approach to stem their proliferation, possibly led by multilateral international organizations like the UN.

One way to address this question would be to take, as case studies, countries where Internet shutdowns have occurred. Most research has focused on Internet shutdowns from a domestic standpoint (Ayalew, 2019; Freyburg & Garbe, 2018; Rydzak, 2019; Wagner, 2018), without contextualizing this type of measure in an international framework; the latter of which has been addressed primarily by advocacy groups (Access Now, 2020). However, focusing on some national experiences provides incomplete insights about the potential range of approaches to justifying Internet shutdowns. It is also likely to obfuscate some of the underlying concerns or rationales that might be driving the recent increase in shutdowns. In other words, it is worth looking at not only the national legal framework but also international human rights law. Almost all countries are members of the UN and therefore bound by the principles of the UN Charter (United Nations, 1945a), as well as other international human rights covenants.

Focusing on international legal frameworks can provide insights into legal justifications for Internet shutdowns, including underlining how shutdowns may threaten freedom of expression, but also involve the sovereign right of states to close telecommunication services. If, on the one hand, Internet shutdowns raise challenges for the protection of human rights, on the other hand, state actors can also justify these practices by relying on legitimate reasons such as national security deriving from the principle of sovereignty or the responsibility to protect in the context of mass violence or genocide.

At the same time, existing domestic processes around Internet shutdowns highlight the limits of the law. Most Internet shutdowns are quickly implemented by politicians in response to concerns like exam

cheating, protests, or social unrest. They seldom engage in legal or policy processes to endorse or enable a shutdown. Lawyers and courts are not often involved until it comes to domestic actors contesting a shutdown, as was recently seen in the court challenge in Zimbabwe, when Zimbabwean Lawyers for Human Rights and the Media Institute for Southern Africa (MISA) successfully contested leading to a High Court ruling that the 2019 shutdown was illegal (Tobor, 2019). Thus, an overarching question we also address in this article is whether and to what extent international legal frameworks, and law more generally, can mitigate the rise of shutdowns.

So far, scholars and advocates have not proposed substantive solutions to deal with Internet shutdowns, other than urging governments to "keep it on" like Access Now, and limiting their analysis to examine the negative effects of this form of censorship and provide data about their frequency and duration. Going beyond the polarization of the debate between "keep it on" and "shut it off" is the first and most challenging aim of this article. We seek to both provide new perspectives, but also to start discussing how there can be more transparency and debate around decision-making processes behind Internet shutdowns. We recognize this is a contentious approach, and the very process of exploring the legal issues potentially justifying Internet shutdowns might normalize certain language or processes on which state could rely to censor the digital environment. This is not our intention. Our approach is more nuanced. The current polarized debate does not appear to be mitigating shutdowns and, when it comes to the imposition and implementation of shutdown, law has not always been relevant. Bringing back legal arguments into the exploration of the justification around shutdowns might actually make the use of shutdowns less frequent and more limited, when they do occur.

This article proceeds in three sections. We begin by examining the issue of Internet shutdowns underlining the primary human rights' concerns and the justifications used by states to block the digital environment. The second part analyzes the relationship among freedom of expression, national sovereignty, and Internet shutdowns. The third section questions the current international legal framework and proposes some initial steps to more effectively address some of the challenges posed by Internet shutdowns.

Justifications for Internet Shutdowns

Among the different forms of online censorship, Internet shutdowns are some of the most invasive and blunt. Unlike traditional forms of censorship like blocking Internet pages or certain content, these shutdowns are architectural and affect a preliminary condition in the information society: access to the Internet.

The core of most definitions is a recognition of the "intention" to shut down or "disrupt" the Internet (including the dissemination of information online) and the involvement of state actors (Human Rights Council, 2016). First, the intent of state actors to block access to the digital environment is crucial for understanding what is taking place. The intent around shutdowns is also what differentiates these practices from simple technical errors. In other words, Internet shutdowns do not involve technical problems to the national infrastructure potentially limiting access or connectivity, but rather the voluntary action of a state blocking the digital environment. Although online censorship usually targets content according to its purposes, morality or legality, an Internet shutdown blocks access more generally, with the result that all

Internet traffic (whether to a specific social media site or to the Internet as a whole) is treated in the same way, as unlawful or immoral content.

Second, at the core of these definitions is the direct involvement of state actors. This is essential from an international law standpoint because states are obligated to respect human rights. The traditional paradigm of protection of human rights applies vertically, meaning that the respect of human rights requires state actors to implement the necessary measures to protect and ensure the fulfilment of these rights and freedoms. This reflects the prevalence of the state over individuals, making state actors as the primary subject under international law (Smith, 2018). Moreover, human rights play a crucial role in limiting the power of state actors in relation to individuals vis-à-vis the state. In contrast, in the absence of any legal instruments adopted by state actors, private actors are not required to protect human rights (Carillo-Santarelli, 2017; Clapham, 2006).

Despite this international obligation, there is a clear lack of transparency and accountability of states when shutting down the Internet, including justification of the reasons or the procedures on which these restrictive measures are implemented. As mentioned earlier, there have been some efforts to map the reasons governments have provided, which are typically centered around questions of national security, including political mobilization or protest (Chutel, 2019; Howard, 2011; Micek, 2016; Wilson, 2019), whether through elections, public assemblies, or other sensitive events such as the visit of foreign state officials (Matfess, 2016; Olukotun, Micek, & Bjorksten, 2016). In some cases, governments have tried to marginalize specific groups that may, for example, be attempting to highlight human rights violations in some marginalized areas (Wagner, 2019). And Internet shutdowns have also been implemented for more benign seeming issues, such as before school exams to prevent cheating (Youssef, 2018).

When governments do provide explanations of their actual or potential actions, which they often do not, democratic countries tend to justify Internet shutdowns as a necessary and temporary measure of protection to deal with emergencies, denying their intention to use Internet shutdowns as a general rule to pursue legitimate interests, such as national security. More authoritarian regimes often blame rogue domestic groups (often "terrorists") or foreign powers (including diaspora communities) for threating their internal stability (and sovereignty) through mobilizing protests or violence through the Internet (Vargas-Leon, 2016). Moreover, even if authoritarian regimes would rely on ad hoc ways to decide how to address Internet shutdowns, they rarely base their actions on evidence or data, and, as a result, they cannot justify their rationale. Also, they rarely proceed through legal or transparent steps when they implement a shutdown.

Despite the differences in various narratives for justifying shutdowns, one goal appears to be the "sabotaging of accountability" by relying on general justifications without a strong legal basis and proportionality assessment on which shutdown orders could be based (Glasius & Michaelsen, 2018). For example, in Cameroon, the government has shifted from total shutdowns at the beginning of 2017 to an extensive use of throttling. This change of approach suggests an attempt to replace the "kill switch" with a more subtle way of shutting down the Internet.

Although democratic states are usually inclined to provide a higher degree of transparency and accountability about the reasons behind Internet shutdowns, the general absence of government

transparency makes the entire situation extremely opaque because information about Internet shutdowns comes primarily from the same officials who have been responsible for the shutdown. As a result, understanding the true reasons and consequences of Internet shutdowns, and, in particular, how and to what extent human rights are affected, is not usually an easy task.

Furthermore, the indirect role of social media in Internet shutdowns is often glazed over. Social media play a crucial role in disseminating content, particularly objectionable content like hate, violence, and disinformation, to the extent of contributing to the escalation and promotion of violent conflicts around the world as in Myanmar (Stecklow, 2018). States cannot control the circulation of online content without regulating it because only social media govern the digital spaces where information flows online (Klonick, 2018). The only way states can intervene to face protests or the spread of hate and violence online in the absence of concerted cooperation from social media companies is by shutting down the entire network or specific websites.

It is notable how restrained many countries that have implemented Internet shutdowns have been toward blaming social media companies for their actions. The ire and frustration coming from countries such as New Zealand, Germany, or France toward Facebook or Twitter's inability to control hate speech or incitement to violence on their platforms has been far more pronounced. This may be because poorer countries and those that typically resort to Internet shutdowns have far less leverage over the large American companies.

However, this situation may also be because there is little evidence to suggest that such companies take their complaints seriously, and these countries have not developed a systematic way of engaging with the companies, including notifying them when content violates national laws. In Germany, for example, there were at least 2,900 content restrictions implemented by Facebook in 2018, including posts, comments, and pages/groups, the majority of which were implemented because they were "alleged to constitute 'incitement of hatred,' representation of illegal extremist organizations, and violations of the Youth Protection Law," including issues such as Holocaust denial (Facebook, 2018a). Countries such as Ethiopia and Cameroon, both of which have had Internet shutdowns and whose governments complain about extensive speech constituting "incitement of hatred" on social media platforms, have no instances of restricted content. Notably, Kenya had 13 items restricted between July and December 2017 that "were alleged to violate hate speech and election laws during the 2017 Kenyan Presidential elections" (Facebook, 2018b). Thirteen items are not significant given the scale of the concerns for election-associated violence. Although there has been a lengthy history of contested elections and associated violence, it was really the aftermath of the 2007 elections that elevated international concern for how hate speech (at the time it was primarily vernacular radio) was inflaming violence and tensions (Stremlau & Price, 2009). There has been growing pressure around Kenya's subsequent elections including the 2017 elections where Facebook was accused of spreading significant misinformation (with an estimated 9 of 10 Kenyans exposed to fake news). Facebook itself stepped up efforts of monitoring and publicizing information about fake news through ads in newspapers (Dahir, 2017). This effort has not been consistent across the continent, and can partly be attributed to both the international and domestic pressure on the company. Kenya has a large and active tech space, with a large international community, and much of the messaging on social media is in English, making it easier to track. Ethiopia, in contrast, has also struggled with hate speech online, but has not had

comparable attention from the company. There are many likely reasons for this, including the diversity of languages spoken in Ethiopia and the requirements this would place on monitors (Gagliardone, Stremlau, & Aynekulu 2019).

On the other side, companies such as Facebook have made "Internet disruptions" a key part of their transparency reporting, which they define as "intentional restrictions on connectivity that limit people's ability to access the Internet or specific websites and apps. Disruptions prevent people from sharing and communicating with their family and friends and create barriers for business" (Facebook, 2018a). On this list, countries such as Iran, Iraq, Libya, Chad, and Equatorial Guinea feature heavily.

Between Freedom of Expression and National Sovereignty

To understand how and to what extent the international legal framework can mitigate an Internet shutdown, it is helpful to review the relationship between freedom of expression and sovereignty. In 2015, human rights organizations and experts, including the Special Rapporteur on Freedom of Expression, issued a joint declaration arguing that kill switches can never be justified under human rights law.

However, the obligation for state actors to protect and facilitate the exercise of human rights requires contextualization in the circumstances of Internet shutdowns. Even if, at first glance, the vertical structure of international human right protection appears to prohibit interference like blocking access to the digital environment, the situation is more complex.

First, the international framework of human rights tolerates restrictions to free speech to protect other interests which, otherwise, would be overshadowed by the predominance of freedom of expression. To avoid such axiological risk, it is helpful to focus on whether and to what extent limitations to the right of free speech can be applied according to international law. The next subsection, however, does not take into consideration the different nuances in the protection of free speech, particularly at the regional level.

Second, despite the cross-border nature of the Internet, states maintain their right to exercise sovereign powers over their territory. Because the exercise of this authority entails interferences with human rights, such measure cannot be discretionary, but comply with principle of legality, necessity and proportionality. As a result, state actors can control the national "Internet switch" through telecommunication infrastructure and online intermediaries in their territory to protect public interests like security.

Therefore, when addressing Internet shutdowns, the concern is not only on how these practices might affect human rights but what degree of proportionality could ensure a fair balance between these different interests and, particularly, between the right to freedom of expression and other legitimate (or sovereign) interests.

International and Regional Frameworks for Freedom of Expression

At the international level, the UN framework is the starting point. The Universal Declaration of Human Rights (UDHR; United Nations, 1945b) provides the right "to seek, receive, and impart information

and ideas through any media and regardless of frontier" (United Nations, 1945b, Art. 19). While the UDHR is not a legally binding document, it can be considered customary international law by virtue of its role as a global standard in international human rights law (Hannum, 1996).

Although the right to free speech is enshrined in one of the most important international bills of rights, it is subject to restrictions aimed to protect other interests. Thus, the UDHR establishes the criteria to assess the compatibility of limitations within the international human rights framework. The definition includes the principle of rule of law, legitimacy and proportionality requiring state actors to rely on legitimate legal basis and to ensure a fair balance among different interests. Article 30 completes this framework by establishing that no rights enshrined in the UDHR should be interpreted as implying the right to engage in any activity aimed at the destruction of other rights.

Furthermore, the International Covenant on Civil and Political Rights (ICCPR; United Nations, 1966) recognizes and protects freedom of expression. Like the UDHR, the ICCPR allows restrictions to free speech subject to certain conditions. Because the exercise of these rights requires "special duties and responsibilities," the right to free speech can be limited by implementing restrictive measures necessary "for respect of the rights or the reputations of others" or "for the protection of national security or of public order" (United Nations, 1966, Art. 19). Moreover, the ICCPR includes a provision aimed to avoid the abuse of rights like Article 30 UDHR (United Nations, 1966, Art. 5).

Other international covenants provide for restrictions to the right to freedom of expression, but they deal with specific issues that indirectly support justifications for Internet shutdowns, particularly related to the responsibility to protect those that may be victims of crimes like mass violence or genocide. (United Nations, 1965, Art. 4; United Nations, 1948, Art. 3).

At the regional level, the right to freedom of expression is enshrined in documents such as the European Convention on Human Rights (Council of Europe, 1950, Arts. 10, 17), and the American Convention on Human Rights (Organization of American States, 1969, Arts. 13, 19). Both instruments provide limitations to freedom of expression and share a similar approach to the right to free speech under international law.

Regional mechanisms are more restrictive in Africa and Asia. The African Charter, for example, guarantees every individual the right to receive information and express and disseminate his/her opinions within the law (African Union, 1981, Art. 9), and the African Commission on Human and Peoples' Rights (2016) has underlined the concerns about the emerging trend of African states in blocking or limiting access to telecommunication services such as the Internet, especially during elections (Res. 362, LIX). However, unlike the other international instruments analyzed above, this charter provides a general and broad limitation to freedom of expression. Despite the adoption of the Declaration of Principles on Freedom of Expression in Africa (African Commission on Human and Peoples' Rights, 2002) clarifying that limitations to free speech shall not be arbitrary and provided by law, serve a legitimate interest and be necessary and in a democratic society, the declaration includes claw-back clause that includes the interpretation of the broad term "law" allowing African states to overcome scrutiny of their actions by relying on their definition of national law. The African Commission on Human and People's Rights has, however, attempted to clarify that this provision constitutes a reference to international law. Therefore, any domestic restriction should comply with states' international

obligations. In particular, the Commission tried to avoid domestic interpretations that would have made the provision enshrined in the African Charter meaningless (Lohé Issa Konaté v. Burkina Faso, 2014).

As another point of comparison, the Arab Charter on Human Rights states the right to freedom of expression (Art. 30, Art. 32) but the Charter clarifies that individuals can exercise these rights and freedoms

> in conformity with the fundamental values of society and shall be subject only to such limitations as are required to ensure respect for the rights or reputation of others or the protection of national security, public order and public health or morals. (Art. 32[2])

These are further reinforced in the Arab Convention on the Suppression of Terrorism and the Arab Satellite Broadcasting Charter.

And while the ASEAN (2012) Declaration on Human Rights protects the right to free speech (Art. 21), it provides a broad limitation to the right to freedom of expression which has to be balanced with "duties to all other individuals, the community and the society where one lives" (para. 6). As a result, the Declaration does not exclude that the protection of human rights can be overcome by national duties, especially since "the realization of human rights must be considered in the regional and national context bearing in mind different political, economic, legal, social, cultural, historical and religious backgrounds" (para. 7). Therefore, according to these provisions, human rights are relativized since their protection differs according to the domestic environment and when it comes to limitations of fundamental rights there is no mention of proportionality (para. 8).

This broad picture of the international and regional human rights treaties re-emphasizes that, under international law, freedom of expression is not an absolute right and limitations to such a right can be tolerated. In other words, although the right to freedom of expression is enshrined in international, regional and national bill of rights, its scope of protection is subject to limitations applying according to certain safeguards which can be summarized in the principles of legality, legitimacy and proportionality. Therefore, the issue about justifications in the field of Internet shutdowns does not concern the block of the Internet per se but the assessment on its application in practice.

The principle of proportionality would be able to guide the assessment. While under international law, there could be situations justifying Internet shutdowns, the effects of blocking the Internet is not typically targeted, unlike other forms of digital censorship. Therefore, Internet shutdowns should likely be considered a remedy of last resort to be applied only when governments cannot rely on other means to safeguard a legitimate aim, such as to protect national infrastructure and services from an imminent cyber-attack which could cause human harm and destruction of national property. In other cases, a general shutdown performed to tackle the spread of hate and violence online potentially fueling conflict or genocide would not necessarily be justified since it might be possible to block access just to a single social media. The restriction of certain websites or tools rather than shutting down the entire network could be a more proportionate approach to pursue a legitimate aim established by the law.

Another criterion would require consideration of the safeguards in place within the framework of Internet shutdowns. This could include, for example, the application of a definite period or the explanation of the reasons to citizens about the shutdown, this could lead to a proportionate framework. Similar considerations could include relying on a system of judicial or independent administrative review that can scrutinize the proportionality of Governments' decisions, especially when the term of the blocking has not been defined ex-ante.

National Sovereignty and Self-Defense

An important question to consider is whether Internet shutdowns can be justified as an expression of sovereignty of states over their national telecommunication networks or based on the right to self-defense. Sovereignty can be both internal––the ability of state actors to exercise power and authority over their territory and population, or external––the ability to invoke independence vis-à-vis other external actors. Similar to the ban on the use of force, the principle of non-intervention derives from and supports, the idea of state sovereignty (Thomas, 1985). Article 2(1) establishes that the UN is based on the principle of the sovereign equality of all its Members and Article 2(7) bans any intervention on matters involving the domestic jurisdiction.

The principle of sovereignty has also been included in the Constitution of the International Telecommunication Union ("ITU"). ITU states have the right to block telecommunications services according to their national law when there is a danger for the security of the state or an infringement of its laws, public order or decency (Art. 34[2]). Although the Internet is not expressly mentioned, it can fall within the category of telecommunication according to the ITU definition (Annex). Nevertheless, the most important issue does not concern the definitions of which telecommunication technology can be interrupted, but the discretion of democratic or authoritarian states in legitimizing their actions based on this international framework or their national constitutions. Moreover, according to Article 35, ITU member states also have the right to suspend international telecommunication services, either generally or for certain kinds of correspondence (out-going, incoming or in transit) provided that such actions are immediately communicated to other member states through the Secretary-General.

When contextualizing national sovereignty within the framework of Internet shutdowns, these provisions offer states a legitimate way to block access to the digital environment as well as suspend digital services coming from other States. For example, the recent contribution of social media in escalating mass atrocities by disseminating hate and violent content could constitute a justification for states to shut down the digital environment. As previous discussed in this article, the lack of architectural control over the flow of content in social media' digital spaces forces Governments to rely on Internet shutdowns, no matter if they are in good or bad faith.

Another expression of the principle of sovereignty is the right to self-defense against the potential use of force consisting, for example, of cyber-attacks (Joyner & Lotrionte, 2001). In this case, Internet shutdowns could be implemented to avoid damages deriving from cyber-attacks or be provoked by the legitimate exercise of the right to self-defense from the external interference of other states.

Under international law, the UN Charter prohibits the use of force between states (n 18, Art. 2[4]). The founding relevance of this principle can also be understood by the general recognition of customary international law as supported by the International Court of Justice in the Nicaragua case (Nicaragua v. United States, 1986, ICJ 1). There are, however, two codified exceptions justifying the use of force- the use of force does not violate international law when the state exercises its right to self-defense (n 18, Art. 21), and the UN Security Council can authorize the use of force under Chapter VII (n 18, Art. 42).

Cyber-attacks on telecommunications infrastructure are a matter of national security since this can compromise not only infrastructure but also, potentially, interconnected services (Delerue, 2020; Moynihan 2019). Foreign governments can use information warfare and launch attacks without using traditional means such as military forces to destroy or sabotage energy, defense or telecommunications infrastructure that could affect security and primary services. While the notion of "armed attack" in Article 51 is different from the "use of force" in Article 2(4), since one of the purposes of the UN Charter is promote peace and stability, the definition of armed forces could be considered broadly due to the possibility of other states to conduct attacks in other countries without using military forces or other traditional armed means but just "digital attacks" (Kesan, & Hayes, 2012). Otherwise, state actors would be deprived of the opportunity to ensure security against external threats simply because they do not reflect the traditional notion of "armed attack." As observed, it would be possible to equate cyber-attacks to "armed attacks" when they threaten human beings or cause destruction of property (Dinstein, 2002). This should not, however, affect the requirement for state actors to respect the principles of necessity and proportionality of self-defense as well as the obligation to report to the Security Council (Iran v. United States of America, 2003, ICJ; Ochoa-Ruiz & Salamanca-Aguado, 2005).

It cannot, also, be excluded that Internet shutdowns could be triggered as pre-emptive measures when external threats are perceived as imminent. The doctrine of anticipatory self-defense has been used within international law for a long time and has augmented its credibility "both by contemporary practice and by deduction from the logic of modern weaponry" (Franck, 2003, p. 619). In other words, even if a strict interpretation of Article 51 of the UN Charter would initially render anticipatory self-defense unlawful, states could intervene against an imminent strike (Sofaer, 2003). According to this commonly quoted precedent, pre-emptive self-defense is justified whenever the perceived threat is imminent, or there is a "necessity that self-defense is instant, overwhelming, and leaving no choice of means and no moment for deliberation" (Kretzmer, 2013; Webster, 1983).

Therefore, not only the limitations to the right to freedom of expression but also both the principle of sovereignty and the right to self-defense could constitute justifications on which state actors can rely to limit access to the Internet performing practices of Internet shutdowns.

The Puzzle of Internet Shutdowns

While states have an obligation to respect human rights according to covenants and customary international law that protects the right to freedom of expression limiting the shutting down of the digital environment, states could also have legitimate interests to rely on shutdowns. Although there are different nuances of freedom of expression in regional human rights instruments and areas of the world, the UNDHR

and the ICCPR are the primary structures to take into account for the three step-test based on legality, legitimacy and proportionality of the actions public authorities may take. Together, they can have a role in mitigating the rise of Internet shutdowns.

Despite the potential relevance of these legal procedures, the law has limitations when applied to Internet shutdowns. It is complex to foresee how the scope of applicable regulation is interpreted and similar considerations apply when addressing legitimate interests which can be broadly interpreted to pursue political purposes. These concerns are particularly relevant when authoritarian countries are involved since the degree of transparency and accountability of their public processes can be more difficult to scrutinize. As a result, an unrelated legal basis can obscure political interests behind Internet shutdowns. Or, as we see more frequently, states simply do not engage with legal justifications when applying Internet shutdowns but rather make political actions.

Despite this framework, the limits of the law in relation to Internet shutdowns are not only about the boundaries of the three-step test but also concern the scrutiny of these practices. The failure of law concerning Internet shutdowns is also due to the lack of a common international enforcement mechanism that allows for both the transparent implementation of processes and procedures for when shutdowns might be justified as well as the scrutiny of when shutdowns might be applied inappropriately.

If an Internet shutdown is not viewed to be compliant with international human rights law, it is necessary to question what remedies could be implemented to mitigate this situation. While Internet shutdowns are performed by public actors that are responsible for the protection and fulfilment of human rights, in theory, each individual would be entitled to claim a violation of their human rights against these practices. At the international level, the International Court of Justice adjudicates disputes between states (Art. 34), and, even if the Human Rights Committee may consider individuals complaints ("communications") vis-à-vis against states parties to the ICCPR and the Optional Protocol (No 1; Art.5), its decisions are not binding even if they contribute to interpreting the provisions established by the ICCPR. Some regional organizations do not have a competent body to scrutinize the behaviors of state actors. The *Arab Charter on Human Rights* (League of Arab States, 2004), for example, does not provide a complaint mechanism for individuals, but rather delegates to the committee the power to receive and review state reports and make recommendations. Even the Arab Court of Human Rights is competent only over human rights complaints submitted by states and non-governmental organizations. Moreover, the ASEAN system does not provide any redress mechanism against human rights violations. Even when there is a competent body to adjudicate these cases, the lack of ratification by some member states or the rules of procedures for each regional court can limit access to human rights' judicial protection, especially when the applicant has to first exhaust all domestic remedies (Council of Europe, 1950, n. 49, Art. 35; League of Arab States, 2004, n. 50, Art. 46[1]). Furthermore, there are not cases on Internet shutdowns from an international court clarifying whether and to what extent an Internet shutdown can be defined as legal. In this regard, without clear precedence, it is difficult to promote litigation strategies for reasons of procedural timeliness and the sensitivity of judges.

Given this fragmentation at the international level, it is important to look beyond the common framework of the triple step test. The doctrine of information intervention, according to which states or the international community intervene in the media environment of a target states to cease mass atrocities and

protect human rights, provides some alternative perspectives (Meltz, 1997; Price & Thompson, 2002). Under Chapter VII of the UN Charter, the Security Council has the power to decide what measures should be taken to maintain or restore international peace and security through the adoption of recommendations and binding decisions applying to all UN members (Oberg, 2005). Internet shutdowns do not always threaten the stability and peace of a region unless the prolonged block of the digital environment leads to an escalation of hate and violence in the country. In contrast, governments usually implement Internet shutdowns as part of an attempt to stem protests and violence, although it cannot be excluded that shutdowns can also exacerbate them.

Although there could be challenges in applying information interventions in the case of Internet shutdowns, the international community could decide to act outside the framework of Chapter VII, relying on humanitarian purposes or the responsibility to protect. This could be both for condemning a shutdown (which, depending on the nature and extent of the shutdown could be seen as leading to physical harm for people if they were unable to effectively access critical health and emergency services or other basic social services) or authorizing the use of a shutdown to protect communities from incitement to violence.

In this muddled context, it is important to move beyond the status quo by enabling mechanisms within the UN to better address local Internet shutdowns. As a first step, the UN Human Rights Committee could provide guidelines for governments about Internet shutdowns to increase the degree of transparency and accountability through proceduralization and to encourage a debate about navigating the complex priorities of enabling freedom of expression while maintaining responsibilities to protect. In other words, it is necessary to look at Internet shutdowns under the lens of liability for failure to protect human rights while also (and especially) focusing on fostering states' accountability through, for example, explanations and transparency of the procedures leading to Internet shutdowns.

From a short-term perspective, the issue of a report including guidelines on Internet shutdowns would be crucial. This document would disclose the procedures and conditions states should follow to comply with international law. Greater transparency and dialogue could also help to find alternative approaches to large-scale shutdowns. Within the framework of the UN, this could occur through roundtables where states implementing Internet shutdown practices share their views, data, and explain their need to rely on such restrictive measures. This would include engagement with social media companies about their responsibilities and abilities to address speech that is seen as causing the shutdowns such as incitement to violence. This approach would allow for mapping and monitoring the primary trends as well as provide guidelines and training about Internet shutdowns. Government officials would be more prepared when addressing Internet shutdowns by, for example, considering a wider array of tools to stem truly dangerous speech, providing motivation to the public, including the legal basis and the length of the shutdown.

A broader and longer-term approach should lead to an international instrument addressing Internet shutdowns, or Internet access more generally, where states would commit to avoid resorting to Internet shutdowns except in some narrow and listed exceptions that can be scrutinized by a competent UN body. The aim of this approach is to both introduce a proceduralization of shutdowns to increase the degree of transparency and accountability in public actors' conduct and to define roles and responsibilities for an international actor that can determine the legality of Internet shutdowns.

Conclusion

Determining whether, and under what circumstances, Internet shutdowns might be justified is challenging. Although we do not deny that Internet shutdowns constitute a highly intrusive form of censorship, there are reasons when these practices could be justified. This is not, in any way, to endorse or condone such actions, but we argue that in the context of a rising tide of incitement to violence on social media platforms (and an apparent inability of social media actors to curb such speech) there needs to be a more nuanced and transparent conversation about why some governments are taking the seemingly extreme actions they are, how they can be limited, or when they might be justified, and how concerns about widespread hate online can be better brought into debates around the protection of human rights (Allen & Stremlau, 2005). When it comes to limiting the justifications of Internet shutdowns on the basis that they affect human rights, states' justifications need to be assessed under the lens of the principles of legality, legitimacy and proportionality. However, this test is just a formal exercise without a mechanism of enforcement.

Domestic deterrents, such as arguments around potential economic costs, appear to have little impact (particularly if governments are weighing up the comparative economic costs of protests or unrest), and advocacy groups that focus on publicly shaming governments have not reduced the use of shutdowns. The polarized debate where (some) governments are grasping for ways to control flows of misinformation and hate speech, with legitimate concerns and frustration over the negligence and inability of social media companies to regulate such content on their platforms, and the overwhelming condemnation of Internet shutdowns by advocacy groups and the human rights community can make it difficult to have a nuanced conversation about when and under what circumstances shutdowns might be justified. The blanket condemnation can be counterproductive by restricting the space required to discuss when shutdowns might be proportional or what domestic processes should be in place to determine when and what type of shutdown to implement, for how long, and how such a shutdown would be monitored. Internet shutdowns have largely been ad hoc, without due process or oversight, which makes them more likely to be fall back tools used by governments that wish to censor material in their own political interests.

By failing to have a measured and transparent conversation about the policies and processes required when resorting to Internet shutdowns, and the compatibility with both domestic and international law, it seems likely that the frequency and erratic use of shutdowns will continue until those that most frequently employ widespread shutdowns, many of which are in Africa, find more nuanced and sophisticated tools for surveillance, censorship, and disinformation, and these tools no more likely to comply with human rights norms than shutdowns.

References

Access Now. (2020). The state of Internet shutdowns around the world the 2019 #KEEPITON Report. *Access Now.* Retrieved from https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf

African Union. (1981). *African Charter on Human and Peoples' Rights.* Retrieved from https://au.int/en/treaties/african-charter-human-and-peoples-rights

African Commission on Human and Peoples' Rights. (2002). *Declaration of Principles on Freedom of Expression in Africa*. Retrieved from http://hrlibrary.umn.edu/achpr/expressionfreedomdec.html

African Commission on Human and Peoples' Rights. (2016). *Resolution on the Right to Freedom of Information and Expression on the Internet in Africa, ACHPR/Res. 362(LIX)*. Retrieved from https://www.achpr.org/sessions/resolutions?id=374

Allen, T., & Stremlau N. (2005). Media policy, peace and state reconstruction. Crisis States Research Centre discussion papers, 8. London, UK: London School of Economics and Political Science, Retrieved from http://eprints.lse.ac.uk/28347/

ASEAN. (2012). *ASEAN human rights declaration*. Retrieved from https://asean.org/asean-human-rights-declaration/

Ayalew, J. E. (2019). The Internet shutdown muzzle(s) freedom of expression in Ethiopia: Competing narratives. *Information & Communications Technology Law*, *28*(2), 208–224.

Bahree, M. (2018, November 13). India leads the world in the number of Internet shutdowns: Report. *Forbes*. Retrieved from https://www.forbes.com/sites/meghabahree/2018/11/12/india-leads-the-world-in-the-number-of-internet-shutdowns-report/

Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. Retrieved from https://www.eff.org/cyberspace-independence

Carillo-Santarelli, N. (2017). *Direct international human rights obligations of non-state actors: A legal and ethical necessity*. Tilburg, North Brabant, The Netherlands: Wolf Legal Publishers.

Chutel, L. (2019, January 15). Zimbabwe's government shut down the Internet after fuel price protests turned deadly. *Quartz Africa*. Retrieved from https://qz.com/africa/1524405/zimbabwe-protest-internet-shut-down-military-deployed-5-dead/

Clapham, A. (2006). *Human rights obligations of non-state actors*. Oxford, UK: Oxford University Press.

Clark, J. (2017). *The shifting landscape of global Internet censorship*. Retrieved from https://dash.harvard.edu/handle/1/33084425

Council of Europe. (1950). *European Convention on Human Rights*. Retrieved from http://www.hri.org/docs/ECHR50.html

Dahir, A. L. (2017, August 2). Facebook has joined the battle to combat fake news in Kenya. *Quartz Africa*. Retrieved from https://qz.com/africa/1044573/facebook-and-whatsapp-introduce-fake-news-tool-ahead-of-kenya-elections/

Dahir, A. L. (2018a, November 19). Africa Internet shutdowns grow longer in Cameroon, Chad, Ethiopia. *Quartz Africa*. Retrieved from https://qz.com/africa/1468491/africa-internet-shutdowns-grow-longer-in-cameroon-chad-ethiopia/

Dahir, A. L. (2018b). Half the world is now connected to the Internet—Driven by a record number of Africans. *Quartz Africa*. Retrieved from https://qz.com/africa/1490997/more-than-half-of-worlds-population-using-the-internet-in-2018/

De Gregorio, G. (2019). From constitutional freedoms to the power of the platforms: Protecting fundamental rights in the algorithmic society. *European Journal of Legal Studies*, *11*(2), 65–103.

Deibert, R. (2008). *Access denied: The practice and policy of global Internet filtering*. Cambridge, MA: MIT Press.

Delerue F. (2020). *Cyber operations and international law*. Cambridge, UK: Cambridge University Press.

Dinstein, Y. (2002). Computer network attacks and self-defense. *International Law Studies*, *76*, 99–120.

Embury-Dennis, T. (2019, April 17). Extinction rebellion: London tube WiFi shut down by police in attempt to disrupt climate change protesters. *Independent.* Retrieved from https://www.independent.co.uk/news/uk/home-news/london-tube-wifi-down-internet-not-working-underground-protest-extinction-rebellion-a8873681.html

Facebook. (2018a). *Internet disruptions*. Retrieved from https://transparency.facebook.com/internet-disruptions

Facebook. (2018b). *Kenya: Country overview*. Retrieved from https://transparency.facebook.com/content-restrictions/country/KE

Franck, T. (2003). What happens now? The United Nations after Iraq. *American Journal of International Law*, *97*, 607–620.

Freyburg, T., & Garbe, L. (2018). Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa. *International Journal of Communication*, *12*, 3896–3916.

Gagliardone, I., Stremlau, N., & Aynekulu, G. (2019). A tale of two publics? Online politics in Ethiopia's elections. *Journal of Eastern African Studies, 13*, 192–213.

Glasius, M., & Michaelsen, M. (2018). Prologue: Illiberal and authoritarian practices in the digital sphere. *International Journal of Communication*, *12*, 3795–3813.

Goldsmith, J., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. Oxford, UK: Oxford University Press.

Hannum, H. (1996). The status of the Universal Declaration of Human Rights in national and international law. *Georgia Journal of International and Comparative Law*, *25*(1/2), 287–397.

Moynihan H. (2019). The application of international law to state cyberattacks sovereignty and non-intervention. *Chatham House*. Retrieved from https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf

Howard, P. (2011). When do states disconnect their digital networks? Regime responses to the political uses of social media. *The Communication Review*, *14*(3), 216–232.

Human Rights Council. (2016). *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development*. Geneva, Switzerland: Author.

Human Rights Council. (2018). *The promotion, protection and enjoyment of human rights on the Internet.* Geneva, Switzerland: Author.

Johnson, D. R., & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, *48*(5), 1367–1402.

Joyner, C. C., & Lotrionte, C. (2001). Information warfare as international coercion: Elements of a legal framework. *European Journal of International* Law, *12*(5), 825–865.

Kesan, J. P., & Hayes, C. M. (2012). Mitigative counterstriking: Self-defense and deterrence in cyberspace. *Harvard Journal of Law & Technology*, *25*(2), 431–541.

Klonick, K. (2018). The new governors: The people, rules, and processes governing online speech. *Harvard Law Review*, *131*(6), 1598–1670. Retrieved from https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670_Online.pdf

Kravets, A. (2011, May 15). *San Francisco subway shuts cell service to foil protest: Legal debate ignites*. Retrieved from https://www.wired.com/2011/08/subway-internet-shuttering/

Kretzmer, D. (2013). The inherent right to self-defence and proportionality in jus ad bellum. *European Journal of International Law*, *24*(1), 235–282. doi:10.1093/ejil/chs087

League of Arab States. (2004). *Arab Charter on Human Rights*. Retrieved from http://hrlibrary.umn.edu/instree/loas2005.html

Lessig, L. (2006). *Code 2.0: Code and other laws of cyberspace*. New York, NY: Basic Books.

Lohé Issa Konaté v. Burkina Faso, Application 004/2013 (ACtHPR, 2014).

Matfess, H. (2016, June 1). More African countries are blocking Internet access during election. *Quartz Africa*. Retrieved from https://qz.com/africa/696552/more-african-countries-are-blocking-internet-access-during-elections/

Meltz, J. F. (1997). Information intervention: When switching channels isn't enough. *Foreign Policy*, *76*(6), 15–20.

Micek, P. (2016, June 24). Internet disrupted in Bahrain around protests as wrestling match sparks shutdown in India. *Access Now*. Retrieved from https://www.accessnow.org/internet-disrupted-bahrain-around-protests-wrestling-match-sparks-shutdown-india/

Oberg, M. D. (2005). The legal effects of resolutions of the UN Security Council and General Assembly in the Jurisprudence of the ICJ. *European Journal of International Law*, *16*(5), 879–906.

Ochoa-Ruiz, N., & Salamanca-Aguado, E. (2005). Exploring the limits of international law relating to the use of force in self-defence. *European Journal of International Law*, *16*, 499–524.

OECD digital economy outlook 2017. (2017). Retrieved from https://www.oecd.org/sti/ieconomy/oecd-digital-economy-outlook-2017-9789264276284-en.htm

Olukotun, D., Micek, P., & Bjorksten, G. (2016, May 23). Vietnam blocks Facebook and cracks down on human rights activists during Obama visit. *Access Now*. Retrieved from https://www.accessnow.org/vietnam-blocks-facebook-human-rights-obama/

Organization of American States. (1969). *American Convention on Human Rights.* Retrieved from https://www.cidh.oas.org/basicos/english/basic3.american+convention.htm

Pollicino, O. (2019). The right to Internet access: Quid iuris? In A. Von Arnauld, K. Von Der Decken, & M. Susi (Eds.), *The Cambridge handbook of new human rights* (pp. 1–14). Cambridge, UK: Cambridge University Press.

Price, M. E., & Thompson, M. (2002). *Forging peace. Intervention, human rights and the management of media space*. Edinburgh, UK: Edinburgh University Press.

Rydzak, J. (2019). *Of blackouts and bandhs: The strategy and structure of disconnected protest in India*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413

Smith, R. K. M. (2018). *International human rights law*. Oxford, UK: Oxford University Press.

Sofaer, A. D. (2003). On the necessity of pre-emption. *European Journal of International Law*, *14*, 209–226.

Stecklow, S. (2018, August 15). Why Facebook is losing the war on hate speech in Myanmar. *Reuters*. Retrieved from https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/

Stremlau, N., & Price, M. (2009). *Media, elections and political violence in Eastern Africa: Towards a comparative framework*. Retrieved from https://repository.upenn.edu/cgi/viewcontent.cgi ?article=1006

Suzor, N. (2019). *Lawless: The secret rules that govern our digital lives*. Cambridge, UK: Cambridge University Press.

Thomas, C. (1985). *New states, sovereignty, and intervention*. London, UK: Palgrave Macmillan.

Thompson, K. K. (2011). Not like an Egyptian: Cybersecurity and the Internet kill switch debate. *Texas Law Review*, *90*, 465–495.

Tobor, A. (2019, January 21). *Zimbabwe's high court rules that Internet shutdown was illegal*. Retrieved from https://www.iafrikan.com/2019/01/21/zimbabwes-high-court-rules-that-internet-shutdown-was-illegal/

United Nations. (1945a). *Charter of the United Nations*. Retrieved from https://www.un.org/en/charter-united-nations/

United Nations. (1945b). *Universal declaration of human rights*. Retrieved from https://www.un.org/en/universal-declaration-human-rights/

United Nations. (1948). *UN convention on the prevention and punishment of the crime of genocide.* Retrieved from https://www.un.org/en/genocideprevention/genocide-convention.shtml

United Nations. (1965). *International convention on the elimination of all forms of racial discrimination.* Retrieved from https://www.ohchr.org/en/professionalinterest/pages/cerd.aspx

United Nations. (1966). *International covenant on civil and political rights*. Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Vargas-Leon P. (2016). Tracking Internet shutdown practices: Democracies and hybrid regimes. In F. Musiani, D. L. Cogburn, L. De Nardis, & N. S. Levinson (Eds.), *The turn to infrastructure in Internet governance: Information technology and global governance* (pp. 167–188). New York, NY: Palgrave Macmillan.

Wagner, B. (2018). Understanding Internet shutdowns: A case study from Pakistan. *International Journal of Communication*, *12*, 3917–3938.

Warf, B. (2011). Geographies of global Internet censorship. *GeoJournal*, *76*(1), 1–23.

Webster, D. (1983). Letter to Henry Stephen Fox. In Avalon Project—British-American Diplomacy: The Caroline Case. (1841). *British and Foreign State Papers, 29*, pp. 1137–1138. Retrieved from https://avalon.law.yale.edu/19th_century/br-1842d.asp

Wilson, T. (2019, June 11). Sudan Internet blackout forces battered protesters to rethink. *Financial Times*. Retrieved from https://www.ft.com/content/b1848126-8c0f-11e9-a1c1-51bf8f989972

Youssef, N. (2018, June 21). Algeria's answer to cheating on school exams: Turn off the Internet. *The New York Times*. Retrieved from https://www.nytimes.com/2018/06/21/world/africa/algeria-exams-cheating-internet.html