Cyber Challenges to International Human Rights

Title: Blocking of Cyber-Enabled Communications by States: Ramifications for the Right to Freedom of Communication

Name: Deborah Housen-Couriel

Institution: Minerva Center for the Rule of Law under Extreme Conditions, University of Haifa; Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University; International Institute for Counter-Terrorism, IDC

Abstract:
Government blockage of public access to cyberspace by shutting down internet access, cellphone signals, and other cyber-enabled communications is increasing. A recent report by the Brookings Institute notes that "[t]here is a rising trend of governments disrupting the internet"[1] and analyzes 81 such instances. A well-known example of such governmental measures is the January 2011 shut-down by Egyptian authorities of internet and mobile phone services during the Tahrir Square uprising in order to block cyber-enabled communications among anti-government protesters;[2] and there are more recent instances of documented blockage of cyber-enabled communications in nearly twenty other countries.

Such blockages on the part of States, as well as the UN Security Council, are permissible under international law under certain circumstances.[3] The Tallinn Manual 2.0 identifies several such situations: for instance, Rule 62 of the Manual (entitled "Suspension or stoppage of cyber communications") recognizes the right of States to exercise their sovereign prerogative to suspend cyber communications on the basis of international telecommunications law.[4] Yet the Manual specifically notes that the exercise of such a prerogative is "…without prejudice to…human rights law."[5] In its Rules 34-38, the Manual expands upon the substance of some of these relevant international human rights norms, including freedom of expression.[6]

---

[1] DARREL WEST, *Internets shutdowns cost countries $2.4 billion last year*, THE BROOKINGS INSTITUTE (October 6, 2016), https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf) and Matt Kamen, *Governments shut down the internet more than 50 times in 2016*, WIRED (January 3, 2017), http://www.wired.co.uk/article/over-50-internet-shutdowns-2016.

[2] MATT RICHTEL, *Egypt Cuts off Most Internet and Cell Service*, NEW YORK TIMES (January 28, 2011), http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html). The shut-down, which extended over five days, also affected Egypt's international communications and thus the influx of opinions, ideas and communications into that country over the same period of time (NOAM COHEN, *Egyptians Were Unplugged, and Uncowed*, NEW YORK TIMES (February 20, 2011), http://www.nytimes.com/2011/02/21/business/media/21link.html).

[3] The Security Council may act under Chapter VII to completely or partially interrupt national communications. (UN Charter, Article 41).

[4] TALLINN MANUAL 291-294. The Rule is based on Articles 34 and 35 of the Constitution of the International Telecommunication Union (22 December 1992, 1825 UNTS 331). Government shutdowns of the internet may be permissible under domestic law, as, for example the more than thirty internet shutdowns in India during 2016 that were carried out under Section 144 of the Code of Criminal Procedure, used to mitigate danger in emergency situations. See *Are internet shutdowns becoming a dangerous new norm in India?*, SCROLL.IN (May 9, 2017), https://video.scroll.in/836953/watch-are-internet-shutdowns-becoming-a-dangerous-new-norm-in-india.

[5] TALLINN MANUAL 294 and 179-208 on "International human rights law". See also Steven Tully, *A Human Right to Access the Internet? Problems and Prospects*, HUMAN RIGHTS LAW REVIEW (2014) 14 (2): 175-195.

[6] The text states "…not only because it is a right in itself, but also because an ability to exercise the right is sometimes necessary for the enjoyment of other human rights." TALLINN MANUAL 187.

This *proviso* raises the challenge of a normative balancing between the right of a state to regulate (and indeed limit or block) communications within its territory, and the fundamental freedoms of communication and exchange of ideas enjoyed by individuals. New forms of human interaction in cyberspace enable, in an unprecedented way, the exercise of these fundamental freedoms as set out in Article 19 of the UDHR and similar provisions in regional human rights treaties.[7] How are these two conflicting prescriptive norms on the international plane to be optimally balanced in the context of cyber-enabled communications that continuously cross national regulatory boundaries?[8] The aim of the current research is to propose an array of balancing considerations in the context of international legal norms applicable when such blockages are being considered.[9]

*****

[7] "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." (Universal Declaration of Human Rights, GA Res. 217A (III), UN Doc. A/810 (10 December 1948)). Although established well before the advent of the internet and its spread to nearly half of the world's population at present (47% of the world's population is connected to the internet, according to the International Telecommunication Union (ITU, *Facts and Figures 2016*, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf) there is considerable support for the applicability in cyberspace of these provisions. See "International human rights law", and esp. Rule 34 "Applicability" in MICHAEL SCHMITT (ED.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 179-208, (2d ed. Cambridge University Press 2017) (herein TALLINN MANUAL). Nevertheless, as unprecedented as the dramatically enhanced scope of the exercise of these fundamental rights on the part of individuals and groups in cyberspace is, such is the unfamiliarity and complexity of the threat to these rights and liberties that has arisen as a result of the capacity of States to block internet access and other cyber-enabled communications. See, for instance, RONALD DEIBERT ET AL, ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS AND RULE IN CYBERSPACE (MIT Press 2010); and DANIEL JOYCE, *Internet Freedom and Human Rights*, Eur J Int Law (2015) 26 (2): 493-514.

[8] Pre-emptive blocking of communications is a particularly challenging issue, as in situations in which a State may claim that counter-terrorism measures include a localized or regional shut-down, without discriminating among users or gradations of danger to public safety and welfare.

[9] Examples include the Security Council and NATO.