Killing the Switch: Are Repressive Regimes Learning From Each Other?

In 2019 alone, <u>1706 days of Internet access</u> were blocked or otherwise disrupted by a total of 33 governments worldwide. And in 2020, we have witnessed an unprecedented amount of Internet shutdowns to curb unrest in response to <u>COVID-19</u>. In recent months, Internet shutdowns in <u>Kashmir</u>, <u>Belarus</u>, <u>Ethiopia</u>, <u>Bangladesh</u> and <u>Myanmar</u> have led to global outrages, particularly given the importance of <u>meaningful digital connectivity</u> for <u>fighting the coronavirus</u> and maintaining inalienable rights and freedoms.

Internet shutdowns are intentionally designed by repressive regimes to isolate, disconnect and silence individuals and communities, in a time when being (digitally) connected is more important than ever before. These shutdowns are an inexcusable infringement on human rights and a danger to hard-won political freedoms and civil liberties. What's more, government-mandated disruptions of Internet access have toxic, long-lasting consequences: they undermine citizen trust in technology, the reliability of online governance services, and disrupt economic activity (in fact, a study found that each day the Internet is blocked, it costs \$23.6m per 10m impacted; another report found that government-mandated shutdowns cost the global economy \$8b last year alone).

While network disruptions seek to curb unrest by mobilising digital isolation, they rely on globalised political learning. Increasingly, there is clear evidence that repressive regimes (both authoritarian and, worryingly, democratic) learn strategies and tactics for suppressing civil unrest from each other (see, for example, the research of Professors Koesel and Bunce on <u>Chinese and Russian diffusion-proofing against popular uprisings</u>). And in the age of politicised digital technologies, these crosscurrents of diffused and intentional learning have adapted to thrive in a new landscape of digital authoritarianism. In other words: <u>autocracy promotion has gone digital</u>. In fact, the very toolkit of authoritarian influence has been enabled by democracy's <u>"soft underbelly</u>": that is, the free market of information, which has been systematically exploited by malign authoritarian actors.

Internet shutdowns are a demonstrated and tangible threat to democracies worldwide. But the ecosystem of sharing digitally repressive tactics should be considered particularly menacing, especially given that political learning can be indirect and passive, and is often characterised as "diffusion" as opposed to overt autocracy promotion.

On a regional basis, there are signs that the governments of Myanmar, India and Bangladesh are learning from each other. Most directly, <u>Myanmar's Internet blackout</u> orchestrated across eight townships in Rakhine and Chin states was later <u>mimicked</u> <u>by Bangladesh</u> for the over one million Rohingya refugees living in border camps. Both governments cited security concerns over the <u>spread of "misinformation"</u>. In India, the digital siege of Kashmir and Jammu is eerily similar: considered security threats to the Modi government, regular (<u>a total of 394</u> since 2015, in the world's largest democracy) localised Internet shutdowns are implemented to silence dissent, isolate separatist movements and digitally incapacitate their ability to organise. Technology journalist Rohini Lakshané has called this occurrence and its toxic

consequences the <u>"long shadow of digital darkness"</u>. For aspiring autocrats, blackouts have demonstrated their effectiveness as a repressive tool: particularly when they are localised, simultaneously occur both online and offline, and curb (tele)communications among historically contested territories inhabited by historically targeted minorities.

And while Internet shutdowns are one of the most brazen strategies of digital repression, they are just one tool in the globalised and growing digital toolkit for repressive regimes. Beyond online censorship, misinformation and surveillance, several emerging trends should turn heads: as proposed by <u>a recent NED report</u>, with the increasing capacity of AI technologies, "authoritarian regimes stand ready to manipulate the development of global surveillance to serve their own interests".

Yet in adversity, there is hope. Faced with an Internet blackout orchestrated by the anti-democratic Lukashenko regime in Belarus, demonstrators have moved to the <u>encrypted messaging app Telegram</u> to spread the call to action; additionally, "you would see people in the elevator just leaving USB sticks with <u>VPN access</u> <u>files</u>" (enabling the Internet user to change their IP address). More importantly, prodemocracy demonstrators in Belarus are not the first to use these tactics: in recent, Iranian demonstrators have regularly used Telegram to <u>coordinate political action and</u> <u>disaster relief alike</u>, despite a 2018 ban. Repressive regimes can learn from each other: but in an increasingly networked world, so can their citizens, who are becoming demonstrably more adept at bypassing digital sieges.

Increasing digital connectivity and digitally sophisticated governance worldwide is undoubtedly a double-edged sword for democracy as we know it. Initiatives like Access Now's Shutdown Tracker Optimisation Project and the <u>#KeepItOn Coalition</u> and various NGOs (such as <u>Witness</u>) provide research, resources and practical support for pro-democracy activists worldwide faced with Internet shutdowns. Conferences like <u>RightsCon</u> have created safe, digital platforms for civil society to share strategies and coping mechanisms for navigating the maze of digital authoritarianism. As 2020 draws to a close, one observation is overwhelmingly clear: the fate of global democracy is progressively determined *by* and *in* digital spaces.