GlobalResearch
Center for Research on Globalization

Means of Control: Russia's Attempt to Hive Off the Internet

By Dr. Binoy Kampmark
Global Research, February 14, 2019

Region: Russia and FSU
Theme: Law and Justice, Media Disinformation, Police State & Civil Rights

Such measures were always going to come on the heels, and heavily so, of the utopians. Where there is Internet Utopia, Dystopia follows with dedicated cynicism. Where there are untrammelled means of searching, there will be efforts to erect signposts, usually of a warning nature. Like the librarian ever worried of her reader finding something inappropriate, material will be kept in a different section of the library, forever filed, concealed and kept from overly curious eyes. The library, however, will never close.

Like many of President Vladimir Putin's projects, tackling the internet has all the elements of the improbable, the boastful and the grand quixotic. It also has a certain Icarus, waxwing quality to it, and may end up melting when approaching its sunny objective. Be that as it may, the Russian Internet Isolation Bill is simply another one for the books, another project in authority's efforts to control, in the name of security, the way the world wide web works. It seeks to impose further restrictions on traffic and data, routing it through state-controlled points to be registered with Roskomnadzor, the federal communications regulator. To this will be added a national Domain Name System, enabling the internet to function even if severed from foreign links.

The obvious and sensible point here shared by all states with an interest in using, exploiting and controlling the internet is how best to preserve an information web function that is sovereign and resistant to attack. The Russian suggestion here is somewhat bolder than others: to hive off and keep RuNet (the state's internet infrastructure) safe from any cyber mauling. This would effectively link the Russian segment to a switch. Even after an attack, the internet within the country might still function in its provision of online services, minimising internal chaos.

Critics of this Russian venture would do well to note the differing tactics of states towards the internet. The functionaries in Moscow have never made any secret of the fact that control is the order of the day. Ditto China, which remains all focused on maintaining its Great Fire Wall, barrier to deemed ills. Other countries supposedly interested in freer flowing tributaries of information have the same suspicions and paranoias; they merely choose to manifest them in less heavy handed and, in some instances, underhanded ways.

As a June 2018 piece from those sinister chaps at Stratfor observes with some accuracy, all governments wish to exploit the internet. They are junkies for control. "Administrations even in liberal countries such as the United States have attempted to direct online discourse and to sway public opinion toward some outlets and away from others." Ever mindful of future solicitations for its services, Stratfor insists that four countries "merit special attention for their efforts to break Western hegemony on the internet and, by extension, to challenge

the free internet model." Delightfully slanted in selecting Iran, China, Turkey and Russia, the assessment ignores the obvious point: the free internet model is tat and show.

In the United States, where freedom of speech remains, at least in some form, relevant, the National Security Agency remains dedicated, not so much to controlling the net but conducting surveillance of it. If you can't beat it, spy on it. The point was made with amply devastating effect by whistleblower Edward Snowden: "I, sitting at my desk, could wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email."

The lower house of Russia's parliament, the State Duma, allowed passage of the bill on February 12 as the first of three votes. Amendments are bound to follow, but the work is formidable. A working group of industry figures established to implement the directives of the ensuing legislation insists that various tests and simulations will have to be done by telecommunication companies to test the effect of disconnection. Its head, Natalya Kaspersky, might well have praised the goals of the legislation, but she was frank enough about the draft law to suggest that implementing it "raises many questions".

Critics are, rightly, concerned that such bills have a rather nasty effect on how the Russian segment of the internet will work, which is precisely the point. The Russian Union of Industrialists and Entrepreneurs is suspicious that this is a grand act of self-harm. The Communists are sceptical. Vladimir Zhirinovksy of the Liberal Democratic Party of Russia will not back it.

The issues of cost and capabilities in creating the necessary equipment to implement such a regime of strategic isolation have also niggled legislators. As LDPR lawmaker Sergei Ivanov bitterly mused in debate,

> "Russia does not produce any IT hardware, only cables, which some people better hang themselves on."

Strange things tend to be suggested in the name of preservation.

The broader response by onlookers stretching from those in Freedomland to more autocratic outposts is to simply keep Russia in the cybernews. Cyberwarfare and cyber activities have lifted Russia into the permanent news cycle, and endless churning and turning in the domestic affairs of the United States and Europe. Spot the hack, spot the Russian. Lose an election, blame it on the Kremlin's hacking and electoral interference. If only it were that simple.

For all the fears, coupled with the boast and bark from the Kremlin, this controlling effort, given the constant evolution of networks, may well collapse. State regulators such as Roskomnadzor have already shown how they bungle when attempting to limit or stop various apps from working. Last year's effort to bar the encrypted communications app Telegram in 2018, for instance, disrupted associated IP addresses (15.8 million, in fact), precipitating havoc on Google and Amazon's cloud-hosting platforms. Networks will do that to you.

Notwithstanding that object lesson in what happens when swathes of the internet are blocked to target one undesirable gremlin, the utopians of government control are still in full

voice. German Klimenko, who had a rough time of it as Putin's grand wizard on internet affairs last year, may well be yet another name to add to that list, holding the belief that such complex interconnected systems can be protected by a merely "push" of a button without calamitous consequences.

In its ambition to control the internet, Russia is simply another state addicted to yet paranoid about the nature of the internet. All states, by definition, want control over the highways, the lanes and the alleys of a system that has its origins in survivability in catastrophic conflict. Paradoxically, it also has the means to inflict it. That way, a state's own infrastructure can be spared at some cost, allowing the censor of unwanted ideas to keep it company, rummaging through materials deemed appropriate for consumers. That's what you get for believing in utopia.

*

Note to readers: please click the share buttons below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. He is a frequent contributor to Global Research and Asia-Pacific Research. Email: bkampmark@gmail.com

---