The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russian Internet Faces Tighter Kremlin Control

By Kevin Rothrock

September 30, 2014



The Kremlin is worried that the West might try to shut off Russia's access to the global Internet. According to a report by Vedomosti on Sept. 19, the Kremlin might soon deploy a new set of tactics in an effort to defend the country's "digital sovereignty."

Vedomosti's anonymous sources say the Kremlin may require Russian Internet service providers to install "equipment that would make it possible to sever Russia's access to the global Internet, in the event of an emergency." According to the newspaper, Russian ISPs might be ordered to kill access to websites hosted outside of Russia during "military actions" or "serious domestic protests."

Russian ISPs might be ordered
to kill access to websites amid
"serious domestic protests."

Moscow's fears of a foreign-engineered RuNet shutdown are in part a response to Edward Snowden's claim last month that the NSA accidentally caused a national Internet outage in Syria in 2012. In an interview with Wired magazine's James Bamford, Snowden said NSA hackers unintentionally crashed the Syrian web while trying to remotely install "an exploit in one of the core routers at a major Internet service provider."

Anastasia Golitsyna, the reporter who broke the Sept. 19 story in Vedomosti, told RuNet Echo that some officials in Moscow might worry about American Internet hegemony the way they fear Russian aviation's reliance on America's space-based positioning system, GPS. Just last month, for example, 12 planes flying over Moscow reported a sudden GPS outage, leading to some confusion in the air. There were no accidents or injuries, but some of Russia's more hawkish elements speculated that the U.S. cut GPS service over Moscow on purpose, to convey to the Kremlin the might of American technology.

Moscow also plans to push for control over the distribution system that connects domain names in Russia's ccTLDs (country code top-level domains) — ".ru," ".рф" and the discontinued ".su" — to the DNS (domain name system) of the global Internet, which forms the basis for Latin alphabet web addresses instead of forgettable IP addresses. In other words, web users can visit "www.runetecho.org" instead of the far less memorable "69.163.200.55."

The impetus behind Moscow's effort to wrest from the Internet Corporation for Assigned Names and Numbers (ICANN) greater control over DNS operations is nebulous. Russian officials have justified the move by demonizing ICANN as an American-controlled outfit, despite the organization's decentralized leadership structure and the U.S. government's plans to dial down its influence in the organization. Key functions of ICANN have fallen under the power of the U.S. Commerce Department since the administration of then-President Bill Clinton established the entity in the mid-1990s.

More involvement in the web's domain operations would grant the Kremlin some additional capacity to disrupt how the RuNet functions, but the shift would not "surrender control of the Internet to Russia," claims ICANN president Fadi Chehade. Harvard law professor Jonathan Zittrain agrees, saying the Internet works on a "consensus," of which "numbering and naming" is only a "tiny part."

Even as the U.S. disengages from its role in Internet domain administration, there are obstacles to putting the RuNet's DNS in the hands of the Kremlin. According to a report by Kommersant, ICANN will not surrender control of the older and more popular ".ru" domain without broad agreement among Russia's Internet society and human rights authorities. Transferring ".ru" DNS maintenance to the Russian federal government would require "consensus across all [Russian] Internet society," an anonymous ICANN source told Kommersant.

If we dismiss Russia's talk about DNS sovereignty as patriotic bluster, we're left with the Security Council's plan to install special equipment at the ISP level, creating the so-called "Internet kill switch." Ostensibly, this tool would protect the RuNet from malicious attacks like the one that Snowden asserts brought down Syria's Internet two years ago. A RuNet ready for total autonomy would also be better protected against theoretical "Internet sanctions" against Russia, which President Vladimir Putin's press spokesman has intimated are

a possibility, given the West's sudden "unpredictability."

The idea that the U.S. would disconnect Russia from the Internet, however, is antithetical to Moscow's own apparent understanding of U.S. foreign policy. Indeed, Russian officials themselves have accused the West of using the Internet to orchestrate the Arab Spring. In February 2011, for instance, Igor Sechin accused Google of "manipulating the energies of the [Egyptian] people." Even in Syria, if Snowden is telling the truth, crashing the web was unintentional.

The justifications for preparing a "self-sufficient RuNet" are weak. The tools necessary for such a feat, moreover, would empower the Russian government to restrict the country's most vital communication network in an instant, presumably to interfere with mass protests, like the kind that swept Moscow in 2011 and 2012, or the demonstrations that recently brought about regime change in Ukraine, the Middle East and North Africa.

However, given the crackdown on Internet openness and online speech in Russia over the past two years, putting an "Internet kill switch" in the hands of the Kremlin should give RuNet users plenty to worry about.

Kevin Rothrock is project editor of RuNet Echo. A version of this story was originally published on GlobalVoicesOnline.org.

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2014/09/30/russian-internet-faces-tighter-kremlin-control-a39927