

Reporters Without Borders

<http://www.rsf.org/russie-concerted-cyber-attacks-and-18-06-2012,42795.html>

Europe/Ex-USSR - Russia

Net under attack

Concerted cyber-attacks and draconian bill reinforce threat to online freedom

18 June 2012

There are growing signs that the government is trying to tightening its control of the Internet while a new wave of Distributed Denial of Service attacks on independent news websites accompanied the latest major opposition demonstration, on 12 June.

The websites of the radio *Echo of Moscow*, the newspaper *Novaya Gazeta*, *Dozhd TV* and *Tayga Info* were all blocked by DDoS attacks as soon as the protest got under way. This kind of cyber-attack has become a regular event during opposition demonstrations since last December's parliamentary elections.

The authorities are trying to give a legal underpinning to attempts to reinforce online controls, citing the need to combat extremism and protect minors. Article 4 of a bill that parliamentarians from all four parties in the Duma submitted to the family commission on 7 June proposes a unified register of Internet domains and websites containing banned content. The commission has until 30 June to discuss and amend the bill before sending it to the Duma.

The proposed register would be created and run by an agency chosen by the government. According to the current version of the bill, content regarded as particularly harmful – including pornography, content promoting drug use, suicide or extremist ideas and content harmful to children – would be put on the blacklist immediately. Other content could be referred to the courts for a decision.

"While we understand this bill's aim, we are very disturbed by the methods it would use, especially the possibly of blocking access to websites without referring to the courts," Reporters Without Borders said. "We urge the Duma to reject the bill because we think it would endanger civil liberties and contravene the international conventions that Russia has signed."

Article 4 of the bill, which defines the circumstances in which a site would be added to the blacklist, is ambiguous. According to paragraphs 6 and 7, the owner of a site that has been added to the register because of "bad" content has 48 hours to remove the offending content, but paragraph 8 suggests that a site will not be added to the register until after this deadline has expired.

This contradiction makes it impossible to clearly identify the reason for which a site would be added to the register. Is it the presence of "bad" content that is decisive, or is it the owner's refusal to remove the offending content?

The bill is all the more disturbing for allowing hosting companies and Internet Service Providers to restrict access to a site when the owner refuses to remove content.

The bill would reinforce the pressure that Russia seems to want to put on ISPs, hosting companies and other technical intermediaries to block sites with "bad" content. On 27 March, St. Petersburg deputy prosecutor Igor Rezonov told local ISPs that, on the basis of nothing more than a written request from the prosecutor's office, they would be expected to block access to "websites such as online casinos and sites promoting extremism, drug use or paedophilia."

The reason given for this initiative was the difficulty of bringing legal actions against such websites as they are often located abroad. But the threat of prosecution for failure to cooperate forces ISPs to act as Internet police, a role for which they have no legitimacy, while the lack of any independent control increases the possibility of abuses and disproportionate censorship.

Furthermore, the definition of "extremism," a label often used to silence government critics, is too vague. The blocking of the Ruelect.com news website during last December's elections was a good illustration of this.

"The deputy prosecutor's initiative raised a number of questions to which we have obtained no answers, although we wrote to the prosecutor's office on 5 April," Reporters Without Borders said. "They are similar to the questions raised by the new bill. What criteria would be used to select the sites for blocking? What mechanisms would be used to safeguard against abuses? What sanctions are envisaged for ISPs that refuse to comply? And is a filtering system envisaged, with all the risks this entails for online freedom of expression?"

When a website has to be blocked, it should be done in a legally-prescribed and transparent manner on the basis of a court order. Any generalized filtering system should be ruled out. In a [May 2011 report](#), United Nations special rapporteur for freedom of opinion and expression Frank La Rue said the flow of information via the Internet should be restricted only "in few, exceptional, and limited circumstances prescribed by international human rights law."

La Rue's report added that: "Holding intermediaries liable for the content disseminated or created by their users severely undermines the enjoyment of the right to freedom of opinion and expression, because it leads to self-protective and over-broad private censorship, often without transparency and the due process of the law."

[Russia](#) is classified as a country "under surveillance" in the latest Reporters Without Borders report on "Enemies of the Internet," which was released in March.

You can download those documents on our website :

- , (JPEG - 49.2 kb)
-