RUSSIA

	2009	2011
INTERNET FREEDOM STATUS	Partly Free	Partly Free
Obstacles to Access	11	12
Limits on Content	16	17
Violations of User Rights	22	23
Total	49	52

POPULATION: 141.9 million
INTERNET PENETRATION: 33 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

After the elimination of independent television channels and the tightening of press regulations in 2000–01, the internet became Russia's last relatively uncensored platform for public debate and the expression of political opinions. However, even as access conditions have improved, internet freedom has corroded. In the last two years there have been several cases of technical blocking and numerous cases of content removal. The authorities have also increasingly engaged in harassment of bloggers. At least 25 cases of blogger harassment, including 11 arrests, were registered between January 2009 and May 2010, compared with seven in 2006–08. In addition, dozens of blogs have reportedly been attacked in recent years by a hacker team called the Hell Brigade.[1]

Since the internet was first launched in Russia in 1988, the country has made significant gains in the expansion of its information infrastructure. Most Russians access the internet from their homes (94 percent of users) and workplaces (48 percent), and use of cybercafes has consequently dropped off.[2] Internet access via mobile telephones and similar devices has gained popularity since 2006, and 9.4 million people report using this method.[3] Faster and more credible than conventional media, online outlets are becoming the main

[1] Vladimir Pribylovski, "Список взломанных бригадой хелла ЖЖ-блогов" [List of LiveJournal Blogs Hacked by Hell Brigade], LJ.Rossia.org, http://lj.rossia.org/users/anticompromat/769184.html (in Russian), accessed January 2011.
[2] Public Opinion Foundation, "Новый выпуск бюллетеня 'Интернет в России, Зима 2009/2010'" [New Issue of the Bulletin 'Internet in Russia, Winter 2009/2010'], news release, March 24, 2010, http://bd.fom.ru/report/cat/smi/smi_int/int240310_pressr (in Russian).
[3] Taylor Nelson Sofres (TNS), "Аудитория мобильного интернета приблизилась к 10 млн" [Mobile Internet Audience Has Reached 10 Million], RuMetrika, November 22, 2010, http://rumetrika.rambler.ru/review/0/4578 (in Russian).

information source for a growing number of Russians, and certain websites have larger audiences than television channels.

OBSTACLES TO ACCESS

Internet and mobile-phone penetration in Russia continue to grow, and the government largely supports the dissemination of these technologies, both directly and through state-controlled internet-service providers (ISPs) that offer relatively low broadband prices. The number of internet users jumped from 1.5 million in 1999 to 46.5 million in 2010,[4] and grew by more than 13 million in the last two years, though this still leaves Russia's penetration rate at 33 percent, lower than the rates in Central European countries. The level of infrastructure differs significantly from place to place, and gaps are evident between urban and rural areas as well as between different types of cities. The worst access conditions can be found in the North Caucasus and the industrial towns of Siberia and the Far East. In 2009, broadband penetration reached approximately 31 percent of internet users, or 15.7 million households, up from 8.3 million in 2008.[5] Unlimited-plan prices in the different federal districts vary from US$10 to US$69 a month.[6] By the end of 2008, the majority of schools were connected to the internet, but connection speeds are sometimes low. Libraries have been connected less extensively. Internet cafes are present in almost every city.

Mobile-phone penetration has grown rapidly in recent years, and there were 163 subscriptions per 100 inhabitants in 2009.[7] Third-generation (3G) mobile-phone infrastructure began developing relatively late due to resistance from military officials, who claimed that the technology might weaken national security.[8] Now approximately 21 percent of mobile subscribers, mostly in the largest cities, own 3G phones, and the 3G network is expanding rapidly.

Applications like the social networking site Facebook, the Russian social networking site VKontakte, the Twitter microblogging platform, and various international blog-hosting services are freely available. The video-sharing site YouTube is currently accessible, although it has come under threat in some localities. For example, in July 2010, a court in Komsomolsk-on-Amur issued a decision instructing a local ISP to block YouTube, along

[4] *Интернет в России* [Internet in Russia] no. 31 (Autumn 2010), http://bd.fom.ru/pdf/Bulliten_31_osen_2010_short.pdf (in Russian).
[5] iKS-Consulting, "Общероссийские показатели ШПД активно растут" [Russia's Broadband Indices Grow Rapidly], RuMetrika, October 15, 2010, http://rumetrika.rambler.ru/review/0/4524 (in Russian).
[6] Alexey Sidorenko, "Russia: Mapping Broadband Internet Prices," Global Voices, March 14, 2010, http://globalvoicesonline.org/2010/03/14/russia-mapping-broadband-internet-prices/.
[7] International Telecommunication Union (ITU), "ICT Statistics 2009—Mobile Cellular Subscriptions," http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx, accessed February 14, 2010.
[8] The frequency used by 3G had been restricted by the military as "strategic."

with four other websites, because they hosted extremist content including copies of Adolf Hitler's *Mein Kampf* and skinhead videos. The ruling was later overturned after the provider filed an appeal.[9] Also in July, a court in Ingushetia ordered local providers to ban the entire blogging platform LiveJournal because it hosted a blog deemed to promote terrorism and extremism.[10]

Five access providers—Comstar, Vimpelcom, ER-Telecom, AKADO, and the state-owned SvyazInvest—controlled more than 67 percent of the broadband market as of February 2010.[11] Regional branches of SvyazInvest account for 36 percent of subscribers, up from 27.8 percent in 2008. As at the federal level, regional dominance usually depends on political connections and the tacit approval of regional authorities. Although this situation is not the direct result of legal or economic obstacles, it nonetheless reflects an element of corruption that is widespread in the telecommunications sector and other parts of the Russian economy.

Three leading operators—MTS, Vimpelcom, and MegaFon—hold 83 percent of the mobile-phone market.[12] While formally independent, each of these firms has indirect ties to the government. According to independent analyst Vadim Gorshkov, MegaFon is connected with former minister of telecommunications Leonid Reyman, and MTS is linked to the Moscow regional leadership. The information and communications technology (ICT) sector is regulated by the Federal Service for the Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor), whose director is appointed by the prime minister. Given Russia's closed political system and dominant executive branch, the appointment process is not transparent. There are no special restrictions on opening cybercafes or starting ISP businesses, but unfair competition and other such obstacles are not unusual in Russia.

LIMITS ON CONTENT

Although attempts to establish a comprehensive, centralized filtering system have been abandoned, several recent cases of blocking have been reported. In December 2009, a

[9] Alexey Sidorenko, "Russia: The First Case of YouTube Ban," Global Voices, July 30, 2010, http://globalvoicesonline.org/2010/07/30/russia-the-first-case-of-youtube-ban/.
[10] "В Ингушетии заблокировали весь ЖЖ из-за одного блога" [In Ingushetia Entire LiveJournal Blocked Because of One Blog], CNews, August 5, 2010, http://www.cnews.ru/news/line/index.shtml?2010/08/05/403880 (in Russian).
[11] Advanced Communications and Media, "Russian Residential Broadband Data, February 2010," news release, April 23, 2010, http://www.acm-consulting.com/news-and-data/data-downloads/cat_view/16-broadband.html?orderby=dmdate_published.
[12] J'son & Partners Consulting, "Информационный бюллетень: Сотовая Связь в России, Июнь 2009" [Information Bulletin: Mobile Communications in Russia, June 2009], http://www.json.ru/files/news/Cellular_Market_Watch_June_09_RUS.pdf (in Russian), accessed May 2010.

number of ISPs blocked access to the radical Islamist website Kavkaz Center.[13] At almost the same time, the wireless provider Yota blocked several opposition sites.[14] The practice of exerting pressure on service providers and content producers by telephone has become increasingly common. Police and representatives of the prosecutor's office call the owners and shareholders of websites, and anyone else in a position to remove unwanted material and ensure that the problem does not come up again. Such pressure encourages self-censorship, and most providers do not wait for court orders to remove targeted materials. As a result, there has been a massive exodus of opposition websites to foreign site-hosting providers, as well as a trend toward greater use of social networking sites.

Regional blocking, whereby a website is blocked in some areas but remains available elsewhere in the country, is one of the methods used by the authorities to exert more control over the internet. Apart from the YouTube incidents mentioned above (see "Obstacles to Access"), a state-controlled local provider in August 2010 blocked the independent portal *Tulksiye Pryaniki*, which had published articles that were critical of the government. In another example of the phenomenon, a regional network provider in December 2010 temporarily blocked its users from accessing the environmentalist website Ecmo.ru, allegedly because the site initiated a petition to dismiss a local mayor. Regional blocking is arguably more efficient than nationwide blocking in that it attracts less attention and affects only the most relevant audiences.[15]

Content is often removed on the grounds that it violates Russia's laws against "extremism." Providers are punished for hosting materials that are proscribed in a list on the website of the Ministry of Justice.[16] The list is updated on a monthly basis and included 748 items as of January 2011.[17] The procedure for identifying extremist materials is nontransparent, leaving ample room for politically motivated content removal.[18] There have

[13] "Воронка стала достоянием общественности, а лживые сомнения были развеяны вторым взрывом" [The Shell Hole Went Public, and Fake Doubts Were Dispersed by a Second Blow], *Norvezhskiy Lesnoy* (blog), December 2, 2009, http://nl.livejournal.com/869414.html (in Russian).

[14] "Фильтры от Yota" [Filters from Yota], *Drugoi* (blog), December 5, 2009, http://drugoi.livejournal.com/3111589.html (in Russian). The sites blocked were Kasparov.ru, Rufront.ru, Rusolidarnost.ru, Nazbol.ru, Namarsh.ru, and Newtimes.ru. Later the provider explained that there was a technical problem, although journalists at the *Moscow Times* found evidence to the contrary. See Nikolaus von Twickel, "Internet Provider Says It Blocks Sites," *Moscow Times*, December 8, 2009, http://www.themoscowtimes.com/news/article/internet-provider-says-it-blocks-sites/391080.html.

[15] "It's Not the Kremlin," *Babbage* (blog), *Economist*, August 25, 2010, http://www.economist.com/blogs/babbage/2010/08/internet_censorship_russia.

[16] Two such cases occurred in the Kirov and Khanty-Mansiisk regions. See Alexey Sidorenko, "Russia: Hosting Providers Sued for Refusal to Block Web Sites," Global Voices, May 13, 2010, http://globalvoicesonline.org/2010/05/13/russia-hosting-providers-sued-for-refusal-to-block-web-sites/; "Провайдера обязали ограничить доступ к экстремистским сайтам" [Provider Obliged to Filter Extremist Sites], Regnum, February 24, 2010, http://www.regnum.ru/news/1256707.html (in Russian).

[17] Ministry of Justice, "Федеральный список экстремистских материалов" [Federal List of Extremist Materials], http://www.minjust.ru/ru/activity/nko/fedspisok/ (in Russian), accessed May 2010.

[18] As Dmitri Solovyev's case showed, the results may vary depending on the institution where the extremism check was performed. See Alexey Sidorenko, "Russia: Prosecution Against Opposition Blogger Stopped," Global Voices, January 28, 2010, http://globalvoicesonline.org/2010/01/28/russia-prosecution-against-opposition-blogger-stopped/.

been at least three cases of site closures, two of them temporary, on the grounds that the affected sites hosted extremist materials.[19] In February 2010, the major opposition portal Grani.ru was checked for extremism, but the authorities apparently found nothing incriminating.[20]

Nonpolitical reasons for content removal have also been reported, with most involving child pornography and file-sharing services that violate copyright law. In May 2010, eight hosting providers, which together control over 30 percent of the hosting market, signed a charter designed to fight child pornography.[21] The agreement places responsibility for content with the hosting providers, calls on them to install monitoring mechanisms, and urges closer cooperation with police.[22] In June, over 5,000 websites containing sexually explicit images of minors were identified by the Friendly RuNet foundation, which works with various government agencies and ISPs; the sites were subsequently shut down.[23] With respect to copyright violations, the file-sharing site iFolder.ru was blocked by police for several days during the year, but the most prominent recent episode was the early 2010 suspension of the domain of the largest Russian file-tracker, Torrents.ru, by regional registrar Ru-Center.[24]

Russia's vibrant blogosphere includes over 7.4 million blogs, up from 3.8 million in 2008. Approximately 93 percent of Russian-language bloggers live inside the country,[25] and Moscow-based bloggers dominate the community.[26] President Dmitri Medvedev started a video blog in October 2007,[27] in January 2009 he established a LiveJournal blog,[28] and in June 2010 he opened a Twitter account.[29] Since then at least 39 regional governors have followed suit.[30] During the last year and a half, the role of the blogosphere grew significantly as it became not only the sole credible source of information—especially during disasters or

[19] The affected sites were Alleng.ru, 20marta.ru, and Stringer.ru.
[20] Alexey Sidorenko, "Russia: Media Portal Undergoes Check for Extremism," Global Voices, February 21, 2010, http://globalvoicesonline.org/2010/02/21/russia-media-portal-undergoes-check-for-extremism/.
[21] "Хостеры подписали декларацию против детской порнографии" [Hosters Signed Petition Against Child Pornography], CyberSecurity.ru, May 30, 2010, http://www.cybersecurity.ru/news/94903.html (in Russian).
[22] The text of the providers' joint declaration can be found at http://hostdeclaration.ru/ (in Russian), accessed May 2010.
[23] "За полгода в Рунете нашли пять тысяч сайтов с детской порнографией" [Within Half a Year, 5,000 Sites with Child Pornography Were Found on the Russian Internet], Lenta.ru, July 16, 2010, http://lenta.ru/news/2010/07/16/mvd/ (in Russian).
[24] Gregory Asmolov, "Russia: Closure of Torrents.ru Makes People Suspicious of .Ru Zone," Global Voices, February 26, 2010, http://globalvoicesonline.org/2010/02/26/torrents-sochi/.
[25] Yandex, *Блогосфера Рунета, Весна 2009* [Blogosphere of the Russian Internet, Spring 2009] (Moscow: Yandex, 2009), http://download.yandex.ru/company/yandex_on_blogosphere_spring_2009.pdf (in Russian).
[26] About 67 percent of the top bloggers reside in the capital. See "Территориальная ассиметрия русскоязычной блогосферы" [Territorial Asymmetry of the Russian-Language Blogosphere," *Blogosphere* (blog), November 29, 2009, http://habrahabr.ru/blogs/blogosphere/76734/ (in Russian).
[27] The Russian president's video blog is located at http://blog.kremlin.ru/.
[28] Dmitry Medvedev's LiveJournal blog is located at http://community.livejournal.com/blog_medvedev/.
[29] Yelena Osipova, "@MedvedevRussia, Are You Listening? A Story of 6 Months on Twitter," Global Voices, December 15, 2010, http://globalvoicesonline.org/2010/12/15/medvedevrussia-are-you-listening-a-story-of-6-months-on-twitter/.
[30] "Чиновники в сети" [Officials on the Net], *Vedomosti*, December 3, 2010, http://www.vedomosti.ru/special/governors-communications.shtml (in Russian).

extraordinary events like the Moscow subway bombings,[31] deadly fire in Perm,[32] and the summer 2010 wildfires[33]—but also the main platform for social mobilization. Several blog campaigns were quite successful,[34] although bloggers' actions came to nothing when attempting to address major cases involving senior officials.[35]

The blog-hosting platforms LiveJournal, LiveInternet, Blogs.mail.ru, and Ya.ru together host 76 percent of all active Russian-language blogs.[36] LiveJournal retains its leading position, although it is facing serious competition from its rivals. The Kremlin allegedly influences the blogosphere through media organizations as well as the progovernment youth movements Nashi (Ours) and Molodaya Gvardiya (Young Guard).[37] The emergence of competing propagandist websites has led to the creation of a vast amount of content that collectively dominates search results, among other effects.[38] Propagandist commentators simultaneously react to discussions of "taboo" topics, including the historical role of Soviet leader Joseph Stalin, political opposition, dissidents like Mikhail Khodorkovsky, murdered journalists, and cases of international conflict or rivalry (with countries such as Estonia, Georgia, and Ukraine, but also with the foreign policies of the United States and the European Union). Minority languages are underrepresented in Russia's blogosphere.

As social networking sites and blogging platforms have grown in importance, they have caught the attention of both the government and Kremlin-friendly business magnates, or "oligarchs." Metals magnate Alisher Usmanov owns 50 percent of SUP, the company that owns LiveJournal, as well as a 35 percent stake in Digital Sky Technologies, which owns the two most popular social networking sites in Russia and a number of others elsewhere in the

[31] Alexey Sidorenko, "Russia: Initial Coverage of the Moscow Subway Bombings," Global Voices, March 29, 2010, http://globalvoicesonline.org/2010/03/29/russia-initial-coverage-of-the-moscow-subway-bombings/.

[32] Gregory Asmolov, "Russia: Online Forum Beats Media in Covering Night Club Fire," Global Voices, December 5, 2009, http://globalvoicesonline.org/2009/12/05/russia-online-forum-beats-media-in-covering-night-club-fire/.

[33] One of the best citizen initiatives to map the wildfires and provide up-to-date information is the Russian Fires website, accessible at http://www.russian-fires.ru/.

[34] The positive outcomes included the punishment of a police officer who abused his authority, the rescue of a Russian tourist bitten by a snake in Indonesia, and the granting of a passport to opposition blogger Oleg Kozlovsky. See Alexey Sidorenko, "Russia: Blogger's Video Leads to Punishment of Policeman," Global Voices, March 9, 2010, http://globalvoicesonline.org/2010/03/09/russia-bloggers-video-leads-to-punishment-of-policeman/; Alexey Sidorenko, "Russia: Bloggers Saved Tourist's Life," Global Voices, February 4, 2010, http://globalvoicesonline.org/2010/02/04/russia-bloggers-saved-tourists-life/; Alexey Sidorenko, "Russia: Opposition Blogger Finally Gets Permission to Leave Country," Global Voices, January 29, 2010, http://globalvoicesonline.org/2010/01/29/russia-opposition-blogger-finally-gets-permission-to-leave-country/.

[35] For example, an online video in which police whistleblower Aleksey Dymovsky complained of widespread corruption led only to his own conviction for slander in March 2010, and bloggers' protests failed to persuade authorities to hold oil executive Anatoly Barkov accountable for a February 2010 automobile accident that killed two women.

[36] Yandex, *Блогосфера Рунета, Весна 2009*.

[37] The Kremlin-affiliated media organizations include the Foundation on Effective Politics, led by Gleb Pavlovsky; New Media Stars, led by Konstantin Rykov; and the Political Climate Center, led by Aleksey Chesnakov.

[38] Ksenia Veretennikova, "'Медведиахолдинг': Единая Россия решила формировать собственное медиапространство" ['Medvediaholding': United Russia Decided to Form Its Own Media Space], *Vremya*, August 21, 2008, http://www.vremya.ru/2008/152/4/210951.html (in Russian).

former Soviet Union. Mikhail Prokhorov, another billionaire oligarch, owns RosBusinessConsulting (RBC), whose hosting service is home to 19 percent of all Russian websites.[39] Vladimir Potanin owns Prof-Media, which in turn owns the search engine Rambler.ru, its news portal Lenta.ru, and other popular resources. Yuri Kovalchuk, a close friend of Prime Minister Vladimir Putin's who controls the media arm of state-owned energy giant Gazprom, recently bought RuTube, the Russian analogue of YouTube.[40] This oligarchic control over an important bloc of online media, social-networking applications, and blogging platforms has raised concerns about the Russian internet's vulnerability to political manipulation.

VIOLATIONS OF USER RIGHTS

Although the constitution grants the right of free speech, this guarantee is routinely violated, and there are no special laws protecting online modes of expression. Online journalists do not possess the same rights as traditional journalists unless they register their websites as mass media. Recent police practice has been to target online expression using Article 282 of the criminal code, which restricts "extremism." The term is vaguely defined and includes xenophobia and incitement of hatred toward a "social group."

Since January 2009, police and the prosecutor's office have launched at least 25 criminal cases against bloggers and forum commentators. While some cases were against individuals who posted clearly extremist content, others appear to be more politically motivated. The most severe and widely known sentence was that of Irek Murtazin, a Tatarstan blogger and journalist who received almost two years in prison in November 2009 for defamation. Other important cases include the August 2009 arrest of five people affiliated with the website Ufa Gubernskaya for extremism, and the May 2010 arrest of blogger Alauddin Dudko, who had worked with Ingush opposition journalist Magomed Yevloyev before his murder in 2008. Dudko was accused of possessing drugs and explosives, but his colleagues argued that the real reason behind the arrest was his online activity.[41] Similarly, in Ulyanovsk region, environmentalist blogger and activist Aleksandr Bragin was

[39] RBC Information Systems, *Годовой отчет РБК за 2008 год* [RBC Annual Report 2008] (Moscow: RBC, 2009), http://www.rbcinfosystems.ru/ir/2008.pdf (in Russian).
[40] Open Source Center, "Kremlin Allies' Expanding Control of Runet Provokes Only Limited Opposition," Office of the U.S. Director of National Intelligence, February 28, 2010, available at http://www.fas.org/irp/dni/osc/runet.pdf.
[41] "В Москве по обвинению в хранении наркотиков и взрывчатки задержан известный блогер" [Popular Blogger Detained in Moscow on Charges of Possession of Narcotics and Explosives], EuIngush, May 20, 2010, http://euingush.com/index.php?newsid=1424 (in Russian).

recently accused of a hit-and-run accident; Bragin claims that he was framed by the authorities in response to his investigative reporting.[42]

Only one blogger, Dmitri Solovyev of Kemerevo, was able to defend his name in court, ultimately securing the government's recognition that the blog post in question was not extremist.[43] The issue of responsibility for anonymous comments has been raised as well. The administrator of the site Gorodirbit.ru lost a court case in March 2010 over an anonymous comment about local authorities and had to pay a fine.[44]

While traditional journalists and activists have faced a series of murders and severe beatings in recent years, physical attacks on Russian bloggers and online activists have so far been comparatively limited. However, one recent event drew significant attention. In November 2010, Oleg Kashin, a reporter for the newspaper *Kommersant* who was also well known as a blogger, was severely beaten near his home in Moscow. His coverage of protests and political youth movements had prompted vocal responses from pro-Kremlin groups in the past, but it was not known exactly who was responsible for the attack.

It is unclear to what extent internet users in Russia are subject to extralegal surveillance of their online activities. Since 2000, all ISPs have been obliged to install the "system for operational investigative measures,"[45] or SORM-2, which gives the Federal Security Service (FSB) and police access to internet traffic. The system is analogous to the Carnivore/DCS1000 software used by the U.S. Federal Bureau of Investigation (FBI), and operates as a packet-sniffer that can analyze and log data passing through a digital network.[46] However, no known cases of SORM-2 use have been reported, and the efficiency of the system has been seriously questioned. Legislation approved in April 2007 allows government services to intercept data traffic without a warrant. Online surveillance represents much less of a threat in the major cities of Moscow and St. Petersburg than in the regions, where almost every significant blog or forum is monitored by the local police and prosecutor's office. Most of the harassment suffered by critical bloggers and other online activists in Russia occurs in the regions.

---

[42] Mikhail Byeliy, "'Это наезд': Эколог, получавший многочисленные угрозы, стал участником странного ДТП" ['This Is a Shakedown': Environmentalist, Having Received Numerous Threats, Became Involved in a Strange Accident], *Noviye Izvestiya*, November 30, 2010, http://www.newizv.ru/news/2010-11-30/137219/ (in Russian).

[43] Alexey Sidorenko, "Russia: Prosecution Against Opposition Blogger Stopped," Global Voices, January 28, 2010, http://globalvoicesonline.org/2010/01/28/russia-prosecution-against-opposition-blogger-stopped/.

[44] Igor Lesovskikh, "Владелец сайта доплатит за комментарий" [Owner of Website Will Pay for Comment], *Kommersant*, March 3, 2010, http://www.kommersant.ru/doc.aspx?DocsID=1330650 (in Russian).

[45] Konstantin Nikashov, "СОРМ для IP-коммуникаций: требуется новая концепция" [SORM for IP-Communications: New Concept Needed], Iksmedia.ru, December 10, 2007, http://www.iksmedia.ru/topics/analytical/effort/261924.html?__pv=1 (in Russian). For more information on SORM, see V. S. Yelagin, "СОРМ-2 история, становление, перспективы" [SORM-2 History, Formation, Prospects], Protei, http://www.sorm-li.ru/sorm2.html (in Russian), accessed March 20, 2009.

[46] B. S. Goldstein, Y. A. Kryukov, and V. I. Polyantsev, "Проблемы и Решения СОРМ-2" [Problems and Solutions of SORM-2], *Vestnik Svyazi* no. 12 (2006), http://www.protei.ru/company/pdf/publications/2007/2007-003.pdf (in Russian).

In addition to official monitoring and prosecution, critical websites face censorship in the form of unexpected "technical difficulties." For example, the sites Sineevedro.ru, Navalny.ru, and Novayagazeta.ru have been unavailable due to "technical reasons" during important civic actions. Several newspaper websites have experienced denial-of-service (DoS) attacks,[47] typically in connection with articles that could seriously influence offline events. Hacker attacks on blogs that began in 2007 continued in 2009–10, with at least 16 blogs suffering attacks in the last two years.[48] As in previous years, the blogs were ravaged and defaced.

Cybercrime is a serious problem, and roughly 9 percent of all internet attacks worldwide between July and September 2010 were carried out from Russia.[49] A number of factors contribute to this growing threat. First, many personal computers in Russia are not protected by antivirus software, leaving them vulnerable to infection and integration into "botnets"—networks of computers that are controlled remotely for malicious purposes. Second, information and instruction on how to build and develop botnets is widely accessible. Finally, punishment of cybercriminals is rare, contributing to a culture of impunity. According to some sources, many hackers for hire are willing to carry out DoS attacks for as little as €200 (US$260) per day.[50] Russian law enforcement has not actively pursued cybercriminals due to corruption and a lack of technical skills, but also because most of the attacks originating in Russia are aimed at users abroad, including in Europe and the United States.

[47] These included *Kommersant* in March 2009, *Novaya Gazeta* in January 2010, and *Vedomosti* in February 2010. See "'КоммерсантЪ' подвергся DDoS атаке" ['Kommersant' Has Undergone DDoS Attack], Xakep.ru, March 16, 2009, http://www.xakep.ru/post/47483/default.asp (in Russian); Alexey Sidorenko, "Russia: Newspaper Web Site Hacked," Global Voices, January 26, 2010, http://globalvoicesonline.org/2010/01/26/russia-newspaper-web-site-hacked/; Alexey Sidorenko, "Russia: Another Newspaper Web Site Attacked," Global Voices, February 13, 2010, http://globalvoicesonline.org/2010/02/13/russia-another-newspaper-web-site-attacked/.

[48] Pribylovski, "Список взломанных бригадой хелла ЖЖ-блогов."

[49] Akamai, *State of the Internet: 3rd Quarter 2010 Report* (Cambridge, MA: Akamai, 2011), http://www.akamai.com/dl/whitepapers/Akamai_soti_apac_q310.pdf?curl=/dl/whitepapers/Akamai_soti_apac_q310.pdf&solcheck=1&.

[50] "В России DDoS-атака стоит от 200 евро в сутки" [In Russia DDoS Attack Costs 200 Euros Per Day]," iToday.ru, April 5, 2010, http://itoday.ru/news/35916.html (in Russian).