

RUSSIA

	2011	2012
INTERNET FREEDOM STATUS	Partly Free	Partly Free
Obstacles to Access (0-25)	12	11
Limits on Content (0-35)	17	18
Violations of User Rights (0-40)	23	23
Total (0-100)	52	52

* 0=most free, 100=least free

POPULATION: 143 million
INTERNET PENETRATION 2011: 49 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

After independent television channels were eliminated and press regulations tightened from 2000-2001, the internet became Russia's last relatively uncensored platform for public debate and the expression of political opinions. In response, the government has tried various tactics to suppress citizens' right to free speech online over the years. In 2009-2010, many bloggers were harassed and opposition blogs were hacked. While these incidents still occurred in 2011, the tactics to restrict freedom of expression online have slightly changed, with the deployment of distributed denial-of-service (DDoS) attacks¹ and various smear campaigns² to discredit online activists becoming more common. Extralegal intimidation of social network activists and independent forum moderators³ has become another line of pressure over the online world through strategies such as informal meetings with the security services, calls from the Federal Security Service (FSB) to the parents of activists,⁴ or the sudden refusal of forum ad sponsors to buy advertisements.

The post-election events of December 2011 through March 2012 became an important period of awakening for the Russian digital civil society. Numerous demonstrations

¹ Hal Roberts, Bruce Etling, "Coordinated DDoS Attack During Russian Duma Elections," Internet and Democracy Blog, December 8, 2011, <http://blogs.law.harvard.edu/idblog/2011/12/08/coordinated-ddos-attack-during-russian-duma-elections/>.

² Alexey Sidorenko, "Russia: The Data Leak War and Other Pre-Election Surprises," Global Voices, October 29, 2011, <http://globalvoicesonline.org/2011/10/31/russia-the-data-leak-war-and-other-pre-election-surprises/>.

³ Alexey Sidorenko, "Russia: Digital Oppression Hits Web Forums as Election Approaches," Global Voices, November 22, 2011, <http://globalvoicesonline.org/2011/11/22/russia-digital-oppression-hits-web-forums-as-election-approaches/>.

⁴ "FSB officers and 'Extremism' center policemen threaten parents of a journalist," Grani.ru, January 20, 2011, <http://www.grani.ru/Politics/Russia/activism/m.194998.html> [in Russian].

organized through social-networking websites took place across the country, with the largest taking place in Moscow. Citizen and netizen activism ultimately led the government to concede a few demi-measures to pacify the protest movement, including the installation of electoral webcams (which despite poor quality, helped to identify more election fraud) and the liberalization of political party regulations.

OBSTACLES TO ACCESS

Internet and mobile phone penetration in Russia has continued to grow in 2011 and 2012,⁵ 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. In 2011, internet penetration in Russia stood at 49 percent, up from 18 percent in 2006 according to the International Telecommunication Union (ITU).⁶ Approximately 71 percent of those living in urban areas have access to broadband internet,⁷ and prices for unlimited broadband plans vary from US\$6 in Central Russia to US\$29.5 in the Far East.⁸

The level of infrastructure differs significantly across the country, and gaps are evident between urban and rural areas as well as between different types of cities. The rapid spread of mobile internet in recent years, however, has significantly improved connectivity in remote areas. Still, the worst access conditions can be found in the North Caucasus mountainous regions and the industrial towns of Siberia and the Far East. Access on Sakhalin Island at the Northern Pacific with nearly 500,000 inhabitants is particularly endangered: in May 2011, the fiber-optic cable connecting the island with the mainland was damaged, leaving inhabitants with an unreliable satellite connection as the only means to connect.⁹

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. Most Russians access the internet from their homes (94 percent of users) and workplaces (48 percent), while the use of cybercafes has significantly declined due to the growing penetration of WiFi

⁵ Public Opinion Foundation, "Интернет-аудитория растет быстрее, чем ожидалось" [Internet audience grows faster than expected], July 15, 2011, http://bd.fom.ru/report/cat/smi/smi_int/pressr_150611.

⁶ International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, <http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#>.

⁷ "TNS Gallup Zip Web Index," TNS Gallup, April 2012, <http://www.tns-global.ru/media/content/B7525726-B5E1-4C12-BE25-4C543F42F3EE/!Web%20Index%20Report%20201204.zip> [in Russian].

⁸ "Internet development in Russia's regions," Yandex Company, 2011, http://company.yandex.ru/researches/reports/internet_regions_2011.xml [in Russian].

⁹ "Internet access in difficult because of the wind on Sakhalin fiber-optic cable," RIA Novosti, May 19, 2011, <http://dv.ria.ru/society/20110519/82009204.html> [in Russian].

and mobile internet.¹⁰ The internet is especially popular among youth, with 96 percent of individuals between 12 and 34 years old connected.¹¹ Applications such as the social-networking site Facebook, the Russian social-networking site VKontakte, the Twitter micro-blogging platform, and various international blog-hosting services are freely available.

Mobile phone penetration has also grown rapidly in recent years, standing at over 179 percent at the end of 2011.¹² 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.¹³ Now approximately 27 percent of mobile subscribers, mostly in the largest cities, own 3G and 4G/LTE phones, and the 3G and 4G/LTE networks are expanding rapidly. Internet access via mobile telephones and similar devices has gained popularity since 2006, and 27 million people report using this method.¹⁴

Five access providers—MTS (former Comstar), Vimpelcom, ER-Telecom, AKADO, and the state-owned Rossvyaz (previously branded as SvyazInvest)—controlled more than 71 percent of the broadband market as of November 2011.¹⁵ Regional branches of Rossvyaz/SvyazInvest, the fastest growing provider in the country, now account for 41 percent of subscribers, up from 36 percent in 2010. Similar to the federal level, regional dominance usually depends on political connections and tacit approval from regional authorities. Although this situation is not the direct result of legal obstacles, it nonetheless reflects an element of regional favoritism that is widespread in many parts of the Russian economy.

Three leading operators—MTS, Vimpelcom, and MegaFon—hold 83 percent of the mobile phone market.¹⁶ While formally independent, each of these firms has indirect ties to the government. According to independent analyst Vadim Gorshkov, MegaFon is connected to former minister of telecommunications Leonid Reyman, and MTS is linked to the former Moscow regional leadership. In March 2012, Dmitry Medvedev signed a presidential decree that authorized a merger between two government-controlled ISPs, RosTelecom and

¹⁰ 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].

¹¹ “TNS Gallup Zip Web Index,” TNS Gallup, April 2012.

¹² “Cellular Data 2011,” Advanced Communications and Media Report, December 2011, http://www.acm-consulting.com/data-downloads/cat_view/7-cellular/18-cellular-2011.html.

¹³ The frequency used by 3G had been restricted by the military as “strategic.”

¹⁴ J’Son and Partners, “Мобильный Интернет в России” [Mobile Internet in Russia], October 31, 2011, http://www.json.ru/files/mobile_internet_in_russia.pdf [in Russian].

¹⁵ Advanced Communications and Media, “Russian Residential Broadband Data 2Q2011,” data report, October, 21 2011, http://www.acm-consulting.com/data-downloads/doc_download/94-russian-residential-broadband-data-2q2011.html.

¹⁶ “Cellular Data 2011,” Advanced Communications and Media Report, November 2011, http://www.acm-consulting.com/data-downloads/cat_view/7-cellular/18-cellular-2011.html.

SvyazInvest.¹⁷ While the decision does not automatically increase government control over the industry, it does significantly change the concentration of internet service provision.

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 legal restrictions on opening cybercafes or starting ISP businesses, but unfair competition, widespread corruption, and other such obstacles are not unusual in Russia.

LIMITS ON CONTENT

Although attempts to establish a comprehensive, centralized filtering system in Russia have been abandoned, content is most frequently removed and blocked on the ISP level if it violates Russia's laws against "extremism." The procedure for identifying extremist materials is nontransparent, leaving room for politically-motivated content removal.¹⁸ Providers are punished for hosting or not blocking materials that are proscribed in a list on the the Ministry of Justice's website.¹⁹ The list is updated on a monthly basis and included 1,066 items as of January 2012 (compared to 748 items in January 2011).²⁰

Officially banned sites include Kavkazcenter.com (a radical terrorist and separatist website), Tawba.info (a site dedicated to Tatar), and radical leftist Limonka.nbp-info.ru, among others.²¹ In 2011, a Moscow prosecutor tried to add LiveJournal.com to the extremist list in response to a blog post created by user "nb_licantrop,"²² but the claim was never realized. Nonpolitical reasons for content removal have also been reported, with most involving child pornography and file-sharing services that violate copyright law.

¹⁷ "Medvedev ordered to reorganize Rostelekom by adding Svyazinvest within one year," *Gazeta.ru*, March 26, 2012, http://www.gazeta.ru/business/news/2012/03/26/n_2259933.shtml [in Russian].

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/>.

¹⁹ 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 Obligated to Filter Extremist Sites], *Regnum*, February 24, 2010, <http://www.regnum.ru/news/1256707.html>.

²⁰ Ministry of Justice, "Федеральный список экстремистских материалов" [Federal List of Extremist Materials], accessed April 1, 2012, <http://www.minjust.ru/ru/activity/nko/fedspisok/>.

²¹ These websites were included in the latest update of the Federal list of extremist materials.

²² The official letter from the Prosecutor's office proposing to block LiveJournal was published by LiveJournal blogger "nb-licantrop" on February 22, 2011 at: <http://nb-licantrop.livejournal.com/262567.html#cutid1>.

In addition, there were several reports in 2011 of “regional blocking,” the practice in which a website is blocked in selective areas of the country. Initiated by prosecutors in lawsuits and direct appeals to regional service providers, many of the regional blocks in 2011 were based on charges of extremism or vague claims that the sites or materials on them were otherwise harmful to society. Often, the web contents in question were not on the official list of extremist materials maintained by the Ministry of Justice. For example, some regional blocks were ordered for religious websites such as those of the Jehovah’s Witnesses in the republic of Mari El in September 2011 and in the region of Chuvashia in November 2011.²³

The practice of putting pressure on service providers and content producers by telephone has become increasingly common. Police and representatives of the prosecutor’s office often call the owners and shareholders of websites to remove unwanted material. Most providers do not wait for court orders to remove targeted materials, and such pressure encourages self-censorship. 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. For example, in May 2011, science fiction writer and blogger Leonid Kaganov had to change both the host and domain of his website due to allegations from the FSB of anti-Semitism and extremism and the subsequent extralegal pressure placed on the hosting providers to remove “extremist” content.²⁴ Kaganov, being a satirical blogger and poet, had mocked an anti-Semitic poem considered by Angarsk (a city in Siberia) as “extremist.”²⁵

On November 11, 2011, regulations governing the domains “.rf” and “.ru”²⁶ were updated to allow any law enforcement agency (such as the police, FSB, Federal Drug Control Services (FDCS), or prosecutor’s office) to seize a domain without a court order. Under these new regulations, the FDCS successfully seized the domain of Rylkov-fond.ru, a website of the Rylkov Foundation that had severely criticized the country’s drug trafficking situation, on February 3, 2012.²⁷ Later in February, the FSB seized the domain FSB21.ru on the same grounds.²⁸ On February 24, 2012, the largest domain registrar in Russia, Nic.ru,

²³ “В городах Чувашии заблокирован доступ к сайтам Свидетелей Иеговы” [Access to websites of Jehovah’s Witnesses blocked in town of Chuvashia], Sova Center, November 22, 2011, http://www.sova-center.ru/religion/news/harassment/non_state_discrimination/2011/11/d23076/.

²⁴ Alexey Sidorenko, “Russia: Famous Sci-Fi Writer’s Blog Removed for ‘Anti-Semitism,’” Global Voices, May 29, 2011, <http://globalvoicesonline.org/2011/05/29/russia-famous-sci-fi-writers-blog-removed-for-anti-semitism/>.

²⁵ Later, Kaganov received an official explanation from the FSB that it had ordered the provider, Zenon NSP, to remove only a particular page of “material that presents a threat to the security of Russian Federation” without telling the provider to remove the whole website. “A Letter from the FSB,” Leonid Kaganov’s blog, July 13, 2011, <http://leo.me/dnevnik/2011/07/13.html> [in Russian].

²⁶ Particularly Article 5, point 5.5, “Rules of the domain registration in .rf and .ru,” CCTLD.ru, <http://www.cctld.ru/ru/docs/rules.php> [in Russian].

²⁷ “ARF Open letter to Mr. Ivanov – head of Russian Federal Drug Control Services,” Andrei Rylkov Foundation, April 2, 2012, <http://en.rylkov-fond.org/blog/ost/rost/arf-open-letter-to-mr-ivanov-head-of-russian-federal-drug-control-services/>.

²⁸ “FSB21 Blocked By FSB Order,” Openinform.ru, February 22, 2012, <http://openinform.ru/news/unfreedom/22.02.2012/26450/> [in Russian].

introduced stricter rules of third level domain cancellation, which now allow for the cancelation of a domain delegation if the site includes “calls to violence, extremist activity, calls to take over power, activity that contradicts with social interests, principles of humanity and morality, offends human dignity or religious feelings.”²⁹

Following the elections in December 2011, numerous groups on the popular Russian social-networking website Vkontakte were created to coordinate protests against the disputed election results. In response, the FSB contacted Pavel Durov, creator of Vkontakte, to demand the removal of seven groups. Durov refused and was later summoned to the prosecutor’s office, which he also ignored.³⁰ Despite Durov’s refusal to cooperate, a user in Bryansk reported that the FSB had forced the closure of the Bryansk group’s Vkontakte page by contacting one of the page administrators directly. The group in Nizhny Novgorod had its webpage hacked and event cancelled. In Tver, the police temporarily detained the group’s creators, Sergey Shilov and Sergey Osipov.³¹ In addition, in October 2011, a Twitter user named “@Vasily,” an anonymous military conscript and the author of the “Barracks Blog,” had his identity revealed by the military authorities and the contents of his micro-blog deleted.³²

Aside from the prosecutor’s office, which serves as the government body that monitors extremist materials, the Russian police have also acquired the power to remove online content. Beginning on March 1, 2011, the vaguely-worded new law “On Police” (Article 13, point 12) granted the police the right to order hosting companies to terminate the activity of webpages that infringe on Russian or international law or endanger individual or public security.³³ Previously, the police needed a court order to close a website. Claiming that the powers are intended to provide compliance with international copyright standards,³⁴ the new legal framework provides more freedom for the authorities to remove content on Russia-based hosting platforms. In February 2012, Interior Minister Nurgaliev announced that the police had closed 8,500 child pornography websites in 2011.³⁵ Nonetheless, critics

²⁹ Such as “.spb.ru” and particularly “.msk.ru,” where the independent radio station Echo Moskvy has its domain. “Changes in the Terms of Service,” Nic.ru, February 24, 2012, <http://nic.ru/news/2012/24.02.regl-ch.html> [in Russian].

³⁰ The full story see here: Gregory Asmolov, “Russia: Social Network In-Between Security Services and Free Market,” Global Voices, December 28, 2011, <http://globalvoicesonline.org/2011/12/28/russia-social-network-in-between-security-services-and-free-market/>.

³¹ “В Твери задержали организаторов группы “В контакте” “Против нечестных выборов,” TverNews, December 9, 2011, <http://www.tvernews.ru/news/27095.html> [in Russian].

³² “The author of “Barrack-blog” in danger,” RealArmy.org, October 26, 2011, <http://realarmy.livejournal.com/2281.html> [in Russian].

³³ “Article 13. Police Powers,” Codes and Laws of the Russian Federation, accessed September 11, 2012, <http://www.zakonrf.info/zakon-o-policii/13/> [in Russian].

³⁴ “Taras Podrez, Valery Weisburg, “Russia promised the United States to close pirate sites with the help of the law ‘On Police,’” Marker.ru, February 25, 2011, <http://marker.ru/news/3761> [in Russian].

³⁵ “Nurgaliev: Policemen had closed more than 8,5 thousand websites with child pornography within a year,” Fontanka.ru, February 10, 2012, <http://www.fontanka.ru/2012/02/10/086/> [in Russian].

have remained concerned that the law would not only be used for criminal activity but also to selectively shut down websites of political nature.

The Kremlin allegedly influences the blogosphere through media organizations as well as the pro-government youth movements, Nashi (“Ours”) and Molodaya Gvardiya (“Young Guard”).³⁶ 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.³⁷ Leaked emails allegedly belonging to the Nashi leaders revealed that the pro-Kremlin movement had been widely engaging in all kinds of digital activities, including paying commentators to post content, disseminating DDoS attacks, and hijacking blog ratings.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). Furthermore, minority languages are underrepresented in Russia’s blogosphere.

Paid online campaigns against opposition activists were widely used in 2011. In October, the newspaper *Novaya Gazeta* reported that the United Russia party was planning to invest nearly US\$320,000 in an effort to discredit Alexey Navalny, the prominent anti-corruption blogger and activist. The news report also wrote that the campaign might disseminate compromising footage of a Navalny look-alike involved in some illegal and/or immoral activities.³⁹ Several weeks later, the contents of different private mailboxes belonging to Navalny and his wife were published online at Navalnymail.kz.⁴⁰ Similarly, the private communications of Lilia Shibanova,⁴¹ an election monitoring activist, and Boris Nemtsov, an opposition politician,⁴² were published online.

³⁶ 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.

³⁷ 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>.

³⁸ Leaked mailboxes are published at this website: <http://slivmail.com/> [in Russian]. Email that contains the plan to paralyze Kommersant newspaper website published at: <http://rumol-leaks.livejournal.com/12040.html>.

³⁹ “Заказ на Навального. Политический детектив,” *Novaya Gazeta*, October 17, 2011, <http://www.novayagazeta.ru/politics/48964.html> [in Russian].

⁴⁰ Alexey Sidorenko, “Russia: The Data Leak War and Other Pre-Election Surprises,” *Global Voices*, October 31, 2011, <http://globalvoicesonline.org/2011/10/31/russia-the-data-leak-war-and-other-pre-election-surprises/>.

⁴¹ Alexey Sidorenko, “Russia: Creators of Election Violation Map Come Under Attack,” *Global Voices*, November 30, 2011, <http://globalvoicesonline.org/2011/11/30/russia-creators-of-election-violation-map-come-under-attack/>.

⁴² Anton Stepanov, “Life News publishes secret talks with the opposition Nemcova,” *Life News*, December 19, 2011, <http://lifenews.ru/news/77459> [in Russian].

Smaller smear campaigns were also implemented against less prominent bloggers such as Suren Gazaryan, a Krasnodar-based environmental activist, who discovered evidence that a campaign to discredit him had a budget amounting US\$15,000.⁴³ In November 2011, Yevgeniy Roizman, a Yekaterinburg-based anti-drug activist, stumbled upon a job posting for campaign against him at a headhunter agency. The employers were offering US\$8 for posting 100 short comments that bad-mouthed the activist.⁴⁴

Many social-networking sites and blogging platforms belong to 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 other sites elsewhere in the former Soviet Union. Mikhail Prokhorov, another billionaire oligarch, owns RosBusinessConsulting (RBC), whose hosting service is home to 19 percent of all Russian websites.⁴⁵ 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.⁴⁶

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. One such politicized decision was reported in 2011: in November, the editorial board of Gazeta.ru, an outlet controlled by the metals magnate Alisher Usmanov, was allegedly forced by one of its owners to remove a banner featuring a map of voting irregularities from the portal Kartanarusheniy.ru, even though Gazeta.ru was one of the co-creators of the map together with election observation association Golos. Roman Badanin, Gazeta.ru deputy chief editor responsible for the project, had to resign due to "disagreement with the owners."⁴⁷

The blog-hosting platforms LiveJournal, LiveInternet, Blogs.mail.ru, and Ya.ru together host the majority of all Russian-language blogs. LiveJournal has retained its leading position, though consistent DDoS attacks (in April, July, and December 2011; see "Violations of User

⁴³ Suren Ghazaryan, "As a journalist, Soloviev defended me from port terminals, and how much it cost budget," LiveJournal (blog), July 18, 2011, <http://gazaryan-suren.livejournal.com/12446.html> [in Russian].

⁴⁴ Yevgeny Roizman, "Администрации президента срочно требуются клеветники и мелкие пакостники. Оплата сдельная," LiveJournal (blog), November 2, 2011, <http://roizman.livejournal.com/1268886.html#cutid1>.

⁴⁵ RBC Information Systems, *Годовой отчет РБК за 2008 год* [RBC Annual Report 2008] (Moscow: RBC, 2009), <http://www.rbcinfosystems.ru/ir/2008.pdf>.

⁴⁶ 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, <http://www.fas.org/irp/dni/osc/runet.pdf>.

⁴⁷ "Замглавреда "Газеты.ру" уволился из-за проекта с "Голосом," Lenta.ru, November 30, 2011, <http://lenta.ru/news/2011/11/30/gazetaru/> [in Russian].

Rights”) together with rivalry from social networks such as Twitter, Facebook, and Google Plus have resulted in its decline in popularity.

Russia’s vibrant blogosphere includes over 52 million blogs and micro-blogs, up from 3.8 million in 2008.⁴⁸ Blog campaigns serve as the main platform for social mobilization and play an ever-increasing role in influencing government decisions. Directed against corrupt or unacceptably arrogant government officials, bloggers’ wrath has led to dismissals, boycott campaigns, and demonstrations. For example, following the parliamentary elections in December 2011, disagreement over the official results and evidence of vote-rigging collected by the crowd-sourced online portal Kartanarusheniy.ru, among others, led to a public protest that later transformed into an all-Russian movement for free elections and political reform. These post-election protests were coordinated through numerous Vkontakte event groups. A YouTube channel dedicated to documenting instances of electoral fraud also served as a major impetus for the post-election protests, garnering millions of hits.⁴⁹

The portal Kartanarusheniy.ru is one example of the growing number and popularity of online crowdsourcing tools in Russia, which have increased from two websites in 2009 to at least 14 crowdsourcing communities in 2011. The anti-corruption portal Rospil.info created by blogger and activist Alexey Navalny, is another good example of online crowd-funding, and the tool was able to fundraise nearly six million Roubles, the largest amount ever raised in Russian history. In December 2011, another online crowd-funding strategy (facilitated by e-money platform Yandex.money) was used to collect money to sponsor a pro-democracy demonstration at Sakharov prospect (a street in Moscow) that was attended by nearly 60,000 participants.

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.”

⁴⁸ Number of total indexed blogs and microblogs by Yandex blog search engine found at: <http://blogs.yandex.ru/>.

⁴⁹ Arch Puddington, “A Victory for the Net in Russia,” Freedom at Issue (blog), December 8, 2011, <http://www.freedomhouse.org/blog/victory-net-russia>.

In 2011, Russian officials went further and proposed—in partnership with China, Tajikistan, and Uzbekistan—an “International code of conduct for information security”⁵⁰ and later a United Nations convention “On ensuring international information security.”⁵¹ The latter document would make member countries pledge to combat sources that disseminate information “that incites terrorism, secessionism or extremism or undermines other countries’ political, economic and social stability, as well as their spiritual and cultural environment.” The document was not adopted internationally, although countries like Belarus have used its concepts to enact more restrictive reforms.⁵² In a positive development, the criminal code was amended at the end of 2011 to decriminalize libel, reducing it to an administrative infraction punishable by fines, effective on December 8, 2011.⁵³

There was less physical violence and legal harassment of bloggers in 2011 compared to 2010. In a positive development, Irek Murtazin, a prominent blogger and journalist who was imprisoned for libel against Tatarstan President Mintimir Shaimiev, was released on parole in January 2011, seven months before his official release.⁵⁴ Nevertheless, at least ten and as many as 38 cases of prosecutions against bloggers and internet activists were reported in 2011.⁵⁵ At the beginning of 2011, the police tried to prosecute several bloggers who had published a poster online that was reportedly disagreeable to Prime Minister Vladimir Putin.⁵⁶ The prosecution began in the Komi Republic against the user, “onchoys,” who was charged with “defamation against a representative of the government.” Similarly in April 2011, the FSB in Orel City filed a complaint to start a criminal case against Georgiy Sarkisyan for posting the same image online.⁵⁷ The proceedings in both cases, however, were eventually dropped.

⁵⁰ “China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations,” Ministry of Foreign Affairs of the People’s Republic of China, September 9, 2011, <http://www.fmprc.gov.cn/eng/zxxx/t858978.htm>.

⁵¹ “Convention on International Information Security,” Concept paper prepared for the International Meeting of High-Ranking Officials Responsible for Security Matters (Ekaterinburg, Russia: September 21022, 2011), <http://isocbg.files.wordpress.com/2011/09/russian-draft-un-cyber-convention-english.doc>.

⁵² Glyn Moody, “No, Belarus is not cut off from the internet, but new restrictions are still pretty bad,” Tech Dirt, January 3, 2012, <http://www.techdirt.com/articles/20120103/07193917260/no-belarus-is-not-cut-off-internet-new-restrictions-are-still-pretty-bad.shtml>.

⁵³ Anastasia Baraulya, “For the Criminal Code – Libel Is Not A Crime Anymore,” FederalInform.ru, February 15, 2012, <http://federalinform.ru/index.php/russia/rpeople/4426-2012-02-15-08-43-22> [in Russian].

⁵⁴ “Irek Murtazin: First Interview After Imprisonment,” Udikov.ru, February 1, 2011, <http://www.udikov.ru/2011/02/01/irek-murtazin-pervoe-intervyu-na-svobode/> [in Russian].

⁵⁵ “Threats to Internet Freedom in Russia (2011),” Agora Association, accessed April 1, 2012, http://openinform.ru/fs/j_photos/openinform_354.pdf; “Journal of Internet Unfreedom,” Agora Association, accessed April 1, 2012, http://openinform.ru/fs/j_photos/openinform_356.pdf [in Russian].

⁵⁶ The poster said, “Putin – pidoras.” “Pidoras” is a name for a male homosexual.

⁵⁷ “In defense of honor,” Kasparov.ru, April 6, 2011, <http://www.kasparov.ru/material.php?id=4D9C1F162C3DF> [in Russian].

In November 2011, the server of the Kostroma-based discussion board “Kostroma Jedis” (Jedi.net.ru) was physically confiscated by the police to be used as evidence in a defamation case against Kostroma governor, Igor Slyunyaev. Forum users who tried to gather to sign a petition were dispersed by the police.⁵⁸ They later created analogues of the discussion forum on a website hosted outside of Russia. In December 2011, the Moscow Election Committee called the authorities to start an investigation against popular Russian blogger Oleg Kozyrev for defamation, an effort which was viewed as an attempt by the authorities to punish bloggers for their reporting on electoral irregularities and fraud.⁵⁹

In June 2011, blogger Aleksey (Alaudin) Dudko—who was arrested in 2010—was sentenced to six years in a penal colony for the possession of drugs and weapons. Dudko denied the accusations and claimed his sentence was due to his blogging activity.⁶⁰ The same month, Yuri Yegorov, a blogger from Tatarstan and a former employee of the regional government, was sentenced to six months imprisonment and six months of probation for libel against the local ombudsman, Rashit Vagizov.⁶¹ His case was overturned by a local judge in March 2012 in response to the December 2011 decriminalization of libel.⁶² In November 2011, Vladimir Pronin, a blogger from the Moscow region who had been publishing online materials about corruption in the Odintsovo city police, was arrested for 13 days.⁶³ Only after wide coverage by the national media did the court recognize Pronin’s arrest as illegal and authorized his release.

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 required to install the “system for operational investigative measures,”⁶⁴ or SORM-2, which gives the 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

⁵⁸ Alexey Sidorenko, “Russia: Digital Oppression Hits Web Forums as Election Approaches,” Global Voices, November 22, 2011, <http://globalvoicesonline.org/2011/11/22/russia-digital-oppression-hits-web-forums-as-election-approaches/>.

⁵⁹ “Избирком ответил мне уголовным делом. Против меня,” Oleg-kozyrev.livejournal.com (blog), December 28, 2011, <http://oleg-kozyrev.livejournal.com/3926225.html> [in Russian].

⁶⁰ “The court in Moscow sentenced a blogger Alexei Deuko to six years in prison,” Karachaevo, June 10, 2011, <http://karachaevo-cherkesia.kavkaz-uzel.ru/articles/187049/> [in Russian].

⁶¹ “In Tatarstan, a globber was sentenced to six months for libel against the Ombudsman,” Openinform.ru, June 9, 2011, <http://openinform.ru/news/pursuit/09.06.2011/25035/> [in Russian].

⁶² “In Kazan, the blogger accused of libel against ombudsman, released from accusation,” OpenInform.ru, March 3, 2012, <http://openinform.ru/news/unfreedom/30.03.2012/26621/> [in Russian].

⁶³ “In suburban Odintsov unfolding saga involving bloggers to trial,” Novaya Gazeta (blog), November 1, 2011, <http://novayagazeta.livejournal.com/390785.html> [in Russian].

⁶⁴ Konstantin Nikashov, “СОМ 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, “СОМ-2 история, становление, перспективы” [SORM-2 History, Formation, Prospects], Protei, <http://www.sorm-li.ru/sorm2.html> [in Russian].

and log data passing through a digital network.⁶⁵ However, no known cases of SORM-2 use have been reported, and the efficiency of the system has been seriously questioned. Meanwhile, 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.

Roskomnadzor, the regulatory body overseeing information technology and mass communications, announced in late 2011 that it had installed online software to detect "extremist" material. Under the new system, websites flagged by the software are given three days to take down allegedly offending content. If a site does not comply, two additional warnings are sent followed by a complete shutdown. The test mode version of the software was to begin operating in December 2011, though its full deployment was indefinitely postponed as of mid-2012. The justice ministry, on the other hand, has invited bids to create its own internet monitoring system, apparently for the purposes of examining content related to the Russian government and justice systems and to any European Union statement concerning Russia.⁶⁶

In 2011, the FSB became keenly interested in services that use encryption, particularly Skype, Hotmail, and Gmail. In January 2011, the regional government in Sverdlovsk prohibited its employees from using Skype and Gmail.⁶⁷ In April 2011, a representative of the FSB said that any service using protocols that could not be hacked by the FSB should be banned from use,⁶⁸ but these calls were dismissed by the Ministry of Telecommunications and Political Leadership.⁶⁹

ICT providers are routinely asked to hand over user data to the authorities. In March 2011, the police requested from forum administrators the IP address of a graphic designer known as "Isabelle" after she had drawn a series of political posters, most of them mocking the ruling party United Russia, online at NevinkaOnline.ru.⁷⁰ In April 2011, donors to the

⁶⁵ B. S. Goldstein, Y. A. Kryukov, and V. I. Polyantsev, "Проблемы и Решения СОПМ-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].

⁶⁶ "2012 Surveillance: Russia," Reporters Without Borders, March 12, 2012, http://en.rsf.org/russia-russia-12-03-2012_42075.html.

⁶⁷ Ashley Cleek, "Russia: Why Skype Worries the FSB?" Global Voices, January 22, 2011, <http://globalvoicesonline.org/2011/01/22/russia-why-skype-worries-the-fsb/>.

⁶⁸ "FSB wants to ban Skype and Gmail, as no control over communication and correspondence on these resources," *Gazeta.ru*, April 8, 2011, http://www.gazeta.ru/news/lastnews/2011/04/08/n_1784533.shtml [in Russian].

⁶⁹ Marina Litvinovich, Sian Sinnott, "Russia: Bloggers Stop FSB Initiative to Ban Skype," Global Voices, April 18, 2011, <http://globalvoicesonline.org/2011/04/18/russia-bloggers-prevent-fsb-from-banning-skype/>.

⁷⁰ "In the Stavropol region, the struggle between Russia and United Internet users," LiveJournal (blog), March 12, 2011, <http://mredisonic.livejournal.com/7525.html> [in Russian].

Russian anti-corruption website Rospil.info received calls and emails from unknown people (allegedly members of the pro-Kremlin youth movements) asking about their donations. Previously all donors had sponsored money via the aforementioned crowd-funding site Yandex.Money. In May 2011, Yandex.Money confirmed it had released Rospil.info donors' financial and personal information to the FSB.⁷¹ In November 2011, the Russian Drug Control Service approached Habrahabr.ru, a popular IT-portal, and demanded⁷² personal data of the Belarus-based staff writer Anatoly Alizar on the grounds of alleged drug propaganda.⁷³ In this instance, the portal refused to provide the data.

Extralegal intimidation of social network activists and independent forum moderators has become another line of pressure over the online world through strategies such as informal meetings with the security services, calls from the FSB to the parents of activists, or the sudden refusal of forum ad sponsors to buy advertisements. For example, in an attempt to intimidate activists during the post-election period in December 2011, the FSB called the parents of Ilya Klishin for questioning after Klishin had organized a rally to be held on December 10th in Moscow through the Facebook page, "For Fair Elections."⁷⁴

In addition to official monitoring and prosecution, critical websites face censorship in the form of unexpected "technical difficulties." Over the past year, DDoS attacks have become an increasing problem for the Russian media sphere. Still, the police generally refuse to investigate the attacks.⁷⁵ LiveJournal, the most popular blogging platform in Russia, was attacked three times during the year. During the parliamentary election in December 2011, 22 websites became dysfunctional due to a powerful attack dubbed as the election "DDoS-alyse."⁷⁶

More generally, cybercrime is a serious problem, as a significant number of cyberattacks were carried out from Russia and against Russian cyber actors. A number of factors contribute to this 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,

⁷¹ Ashley Cleek, "Russia: Anti-Corruption Donor Details Leaked," Global Voices, May 4, 2011, <http://globalvoicesonline.org/2011/05/04/russia-anti-corruption-donor-details-leaked/>.

⁷² Dura Lex, "Federal Drug Control Service aims Alizar," Habrahabr.ru, October 14, 2011, http://habrahabr.ru/blogs/Dura_Lex/132109/ [in Russian].

⁷³ In his post, Alizar speculated on Steve Jobs' ingenuity, marijuana and LSD, and the governments' policies towards light drugs, citing such widely recognized media outlets as *Time Magazine*, the *New York Times*, etc.

⁷⁴ "FSB officers and 'Extremism' center policemen threaten parents of a journalist," Grani.ru, January 20, 2011, <http://www.grani.ru/Politics/Russia/activism/m.194998.html> [in Russian].

⁷⁵ "«Живой журнал» остался без дела," Gazeta.ru, August 22, 2011, <http://www.gazeta.ru/business/2011/08/19/3739473.shtml> [in Russian].

⁷⁶ Alexey Sidorenko, "Russia: Election Day DDoS-alyse," Global Voices, December 5, 2011, <http://globalvoicesonline.org/2011/12/05/russia-election-day-ddos-alyse/>.

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 DDoS attacks for as little as €200 (US\$260) per day.⁷⁷

⁷⁷ “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].