Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**318**
Land:	Rusland
Kilde:	Freedom House
Titel:	Freedom on the Net 2013 – Russia
Udgivet:	3. oktober 2013
Optaget på baggrundsmaterialet:	2. januar 2014

Freedom on the Net 2013 - Russia

Publisher	Freedom House
Publication Date	3 October 2013
Cite as	Freedom House, *Freedom on the Net 2013 - Russia*, 3 October 2013, available at: http://www.refworld.org/docid/52663adc2a.html [accessed 6 December 2013]
Disclaimer	This is not a UNHCR publication. UNHCR is not responsible for, nor does it necessarily endorse, its content. Any views expressed are solely those of the author or publisher and do not necessarily reflect those of UNHCR, the United Nations or its Member States.

2013 Scores

Freedom on the Net Status: **Partly Free**
Freedom on the Net Total: **54**
A Subtotal: Obstacles to Access: **10**
B Subtotal: Limits on Content: **19**
C Subtotal: Violations of User Rights: **25**

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	11	10
Limits on Content (0-35)	18	19
Violations of User Rights (0-40)	23	25
Total (0-100)	52	54

* 0=most free, 100=least free

POPULATION: 143.2 million
INTERNET PENETRATION 2012: 53 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

Key Developments: May 2012 – April 2013

- The number of websites classified as extremist material and blocked by the Ministry of Justice increased approximately 60 percent from January 2012 to February 2013 (see **Limits on Content**).
- In July 2012, the State Duma passed Federal Law #139-FZ which allows the government to create a list of websites that ISPs must block without any mechanism for judicial oversight. This law is intended to restrict access to sites with illegal content, such as child pornography, drug-related material, or extremist content; however, sites with legitimate content have also been blocked under this law (see **Limits on Content**).
- Internet use continued to be a significant tool for mobilization and communication among civil society and opposition groups (see **Limits on Content**).

- In July 2012, the Russian criminal code was amended to recriminalize defamation in traditional and online media (see **Violations of User Rights**).
- Cases of criminal prosecution for online activities increased from 38 in 2011 to 103 in 2012 (see **Violations of User Rights**).

Introduction

Since Vladimir Putin's return to the presidency in May 2012, issues related to internet freedom in Russia have continued to move toward the forefront of social and political concerns. Activists demonstrated the internet's wide-ranging potential for political mobilization and, in so doing, have attracted the close attention of the authorities. Increasingly, the internet is regarded by the Russian state as a realm that requires tighter regulation and restrictions.[1]

The number of active online users continues to grow, particularly in small towns and among older generations.[2] There was a notable increase in the number of websites on the three Russian top-level domains (.ru, .su and .pф), and by the end of 2012, a total of 5,156,504 domain names were registered by 25 accredited registrars.[3] At the same time, many website owners have begun to choose foreign jurisdictions to host their sites; last year showed a rapid growth in Russian demand for renting server equipment outside of the country.[4]

In July 2012, the government passed Federal Law #139-FZ, which allows for the creation of a "blacklist" of websites that internet service providers (ISPs) within Russia are required to block. The law is intended to block access to illegal or otherwise harmful material on the internet, such as child pornography, material related to drug abuse, and so forth. However, there is no judicial approval required to place a website on the blacklist, and many websites with legitimate content have also been blocked in the process. Critics warn that the law is difficult to implement without negatively impacting otherwise legal online activities, and that it could be used to directly censor online content.

The number of legal restrictions against online users also increased over the past year, including an increase in the number of criminal prosecutions against online users, and the recriminalization of defamation through legislation passed by the State Duma. Moreover, well-known bloggers like Aleksei Navalny and Rustem Adagamov,[5] as well as regular users and activists, were subjected to harassment and prosecution. For the first time, internet activists began to flee Russia, seeking asylum in other countries.[6]

Obstacles to Access

The internet penetration rate in Russia has continued to grow over the past few years.[7] In 2012, the internet penetration rate stood at 53 percent, up from 25 percent in 2007, according to the International Telecommunication Union (ITU).[8] Survey data from the Public Opinion Foundation indicates that the estimated number of people who use the internet on a daily basis increased from 44.3 million users (38 percent of the population) at the end of 2011 to 50.1 million users (43 percent of the population) at the end of 2012.[9] During this time period, the greatest growth in internet use occurred in villages and towns with less than 100,000 inhabitants.[10] The mobile phone penetration rate at the end of 2012 was 161 percent, with approximately 230 million mobile phone subscribers among the top seven Russian mobile service providers.[11]

In early 2013, Prime Minister Dmitry Medvedev commissioned the Ministry of Communications and several other government bodies to develop a series of measures by April 1, 2013 that would reduce the cost of broadband internet access for households.[12] The average monthly cost of a broadband connection with a speed of 1 Mbps is $1.80.[13] Currently, however, it costs service providers RUB 12,000 (approximately US$365) to connect one household to a broadband network.[14] This cost may be one of the determining factors in the persisting gap in internet penetration between large cities and rural areas, and among different regions of the country. For instance, the penetration rate in the Northwestern Federal District reached 62 percent in 2012, whereas in the Volga and North Caucasus regions it did not exceed 49 percent.[15] In part, this gap in internet access is counteracted by the explosive growth of mobile internet access. By the end of 2012, there were approximately 22.5 million mobile internet subscribers, an increase of 88 percent from 2011.[16]

Internet access in schools also varies according to region, with many Russian schools still lacking an internet connection. According to a survey conducted by the National Training Foundation, 70 percent of schools in cities with more than 1 million inhabitants are connected to the internet, whereas in rural areas, less than 45 percent of schools have internet access.[17]

In May 2012, several Russian ISPs (VimpelCom, Megafon, Mobile TeleSystems and the state-controlled company Rostelecom) announced plans to develop an underwater fiber-optic cable connecting towns on the island of Sakhalin to the Far East regions of Kamchatka and Magadan.[18] The project, which would significantly lower prices of internet access on the island, is expected to take about two years to complete.[19] It should be noted, however, that there have been multiple failed attempts to construct an undersea cable to Sakhalin in the past.[20]

There are no specific legal restrictions on ICT connectivity or limitations on social media and communication apps. However, in September 2012, members of the State Duma issued a proposal that would outlaw the use of anonymizers and circumvention tools that enable users to send and receive encrypted data, access blocked websites, or make their online activities less conspicuous.[21] As of May 2013, this proposal had not been acted upon and the use of these tools is still legal, although in August 2013 the FSB director revived this debate by announcing that his agency would begin working with other Russian law enforcement and security bodies to draft such legislation.[22]

The broadband market in Russia is still highly concentrated. State-owned provider Rostelecom controls 39 percent of the broadband market, while the other five main providers (VimpelCom, ER-Telecom, Mobile TeleSystems, TransTelecom, and AKADO) together control approximately 40 percent.[23] The remaining 21 percent of the market is controlled by smaller ISPs. This data reflects the overall market distribution throughout the country; however, competition is much lower in small towns and regions where only a few service providers operate.[24] Similarly, the Russian mobile communications market is dominated by three leading companies – Mobile TeleSystems, VimpelCom, and Megafon – which together control 82 percent of the market.[25]

The ICT and media sector is regulated by the Federal Service for Supervision in the Sphere of Telecom, Information Technologies, and Mass Communications (Roskomnadzor) under the control of the Ministry of Communications and Mass Media and the Government of the Russian Federation. With the new internet blacklist law (Federal Law #139-FZ) going into effect in November 2012, Roskomnadzor now has the authority to determine if a website should be blocked based on whether or not the site contains material that is restricted by the law; these decisions do

not require prior court approval. As a result, Roskomnadzor has become a primary player in the field of controlling and filtering information on the internet. Concerning the technical aspects of access to the internet, the regulatory bodies generally operate fairly. However, their efforts to overcome the digital gap and open up the ICT market to greater competition have been insufficient.

Limits on Content

In 2012-2013, the Russian government ramped up its practice of restricting online content through the blocking of websites. In addition to a 60 percent increase in the number of websites placed on the federal list of extremist materials from January 2012 to February 2013, with the enactment of Federal Law #139-FZ in November 2012, the regulatory authority can now place websites deemed "harmful to the health and development of children" on an internal blacklist of sites that ISPs are required to block, without prior decisions or approval by a court.

Blocking access to information on entire websites, IP addresses, and particular webpages has become the most common means in Russia to restrict user activity on the internet. This control over online content expanded after Federal Law #139-FZ was passed on July 28, 2012. Commonly known as "the internet blacklist law," this law, for the first time in Russian history, legalised the blocking of access to websites without requiring a court ruling. Since the law took effect on November 1, 2012, websites on which experts find pornographic images of minors, information about suicide techniques, or information on preparing or taking drugs can be placed on a special register within two days, and access to these sites can be blocked on the basis of a decision by Roskomnadzor. In addition to the material targeted in the legislation, blocked websites have included Ri-online.ru (the website of *Ingushetia Online*, a local news site), a Jehovah's Witnesses site,[26] websites of Caucasian separatists, blogs on LiveJournal, and an analytical article by the public figure and academic Yuri Afanasyev.[27]

During the first four months of the enforcement of Federal Law #139-FZ (November 1, 2012-February 28, 2013), 309 domain names were banned and 197 IP addresses were blocked, causing approximately 4,000 blockings of those resources that shared IP addresses with banned sites.[28] In November 2012, during the first weeks of the implementation of the new law, dozens of websites were blocked for seemingly arbitrary reasons. Among those sites were popular resources such as Lurkmore.to (a wiki-based ironic online encyclopedia for internet subcultures), RuTracker.org (a popular torrent tracker), and Lib.rus.ec (an open library).

In the period from July to December 2012, Google reported that there were 114 requests by the Russian authorities to remove content from various Google platforms, compared to 4 requests during the same period in 2011.[29] These included 111 requests issued by police or executive authorities and 3 court orders. Material related to suicide promotion and drug abuse accounted for the majority of the removal requests (56 requests and 51 requests, respectively), followed by 3 cases related to defamation, 3 related to privacy and security, and 1 related to hate speech. In response to these requests, Google removed content for violating their own product policies in more than half of the cases, and restricted content from local view in about one third of the cases.[30]

In September 2012, there were widespread demands from prosecutors' offices and from Roskomnadzor to block access to sites hosting fragments of the "Innocence of Muslims" video. According to Google's Transparency Report, the company decided to restrict in-country access to the video in eight countries, including Russia.[31] However, prior to this restriction, demands from

the General Prosecutor went out to ISPs across the country, instructing the service providers to block access to the content prior to any court decisions. Given the varying nature of each request, some ISPs opted to block the entire YouTube platform, rendering it temporarily inaccessible for users in certain regions, while other ISPs also blocked access to the social network Vkontakte for containing pages with links to the video.[32] In each case, the service providers complied with the request before the court identified the video as containing extremist material.

In late 2011, Roskomnadzor announced 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 the 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 Ministry of Justice, 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.[33]

The practice of identifying online materials as extremist, which was widespread and used to block websites after the adoption of anti-extremist legislation in 2002, expanded in 2012 when dozens of webpages were added to a federal list of extremist materials, operated by the Ministry of Justice. The federal list contains details of court decisions that identify any online information materials as extremist. As of February 2013, the list included 1,704 items, compared to 1,066 as of January 2012.[34] According to the law, anyone who disseminates these materials, either offline or online, may be administratively or criminally prosecuted and receive a penalty ranging from a fine of RUB 1,000 (approximately $30) to up to 5 years imprisonment, depending upon the legal treatment.

In total, no less than 608 decisions were made during 2012 to block access to websites, either through court judgments or by service providers, compared to 231 decisions in 2011.[35] This number does not include blockings made under the new "blacklist law." At the end of 2012, Roskomnadzor officials reported that 1206 entries were made on the Unified Register at the site Zapret-info.gov.ru, which means either that the information on these sites was deleted or that the website was blocked completely.[36]

At the end of 2011, new rules for the registration of domain names for the domains ".ru" and ".рф" were adopted by the Coordination Center for TLD RU/РФ.[37] These rules have given registrars the right to terminate the domain name delegation of a website based on a decision in writing by the head of an agency which exercises operational search actions, such as the police, the Federal Security Service, the drug police, or the customs agency. In accordance to these rules, in February 2012 the domain name registrar Masterhost discontinued its delegation of the Andrei Rylkov Foundation for Health and Social Justice's domain – Rylkov-fond.ru – based on a report by the head of the directorate of the Moscow branch of the Federal Service for Drug Control, which stated that "the office received information that the domain [...] contained materials that propagandised (advertised) the use of narcotics." In reality, the foundation's site contained official documents on replacement therapy from the World Health Organisation and the United Nations Office on Drugs and Crime.[38]

Some actions taken by local prosecutors and regional courts regarding the blocking of online content have been questionable. In August 2012, for example, the Perm City Court forced an ISP to block a free listings website, stating that a search for the phrase "buy marijuana in Perm" using the

Yandex search engine provided a link to that website. According to a representative from the company that ran the site, an advertisement for a smoking blend had indeed been placed on the site. However, the government bodies had not contacted the site owner, and instead went straight to court. Although the moderator subsequently deleted the advertisement, the ruling to force the service provider to block the site's IP address had already taken legal effect.

In October 2012, the Prosecutor's Office in the Orel region demanded that the court ban the website Orlec.ru, a local "free encyclopedia," based on the claim that the website hosted extremist material. The reason stated by the prosecutor – that the material "undermined the public image of local self-governments and the [Russian Federation] authorities in general" – indicates the political nature of the request.[39] Additionally, there were questions as to whether the material was actually planted on the website for the purpose of such an investigation. In the end, the court ruled that the particular material, which had already been removed, was extremist, but that the website itself was not.

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 editors 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. Additionally, as the blacklist law allows the government to quickly block access to websites that contain information considered to be prohibited, and the evaluation criteria for these decisions is unclear, users and administrators of web resources are forced to practice self-censorship in order to avoid responsibility.

Government attempts to influence the blogosphere and other online sources of information continued from 2012-2013. The Kremlin allegedly influences the blogosphere through media organizations as well as the progovernment youth movements Nashi ("Ours") and Molodaya Gvardiya ("Young Guard").[40] The emergence of competing propaganda websites has led to the creation of a vast amount of content that collectively dominates search results, among other effects.[41] Leaked e-mails allegedly belonging to 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.[42] 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.

There are few specific economic constraints that negatively impact the financial stability of online media. The most common sources of news and information – the federal TV channels – are owned or controlled by the government. In this way, access to opposition and independent sources of information depends on one's access to the internet. On July 23, 2012, amendments to the law "On advertising" entered into force, outlawing the advertisement of alcohol-based products on the internet.[43] This law has had a considerable financial impact on independent internet resources, as advertising is their main source of income.

During 2012 and 2013, the internet, particularly social networks like Twitter, Facebook, and Vkontakte, continued to be a significant tool for mobilization and communication between citizens and activists. In 2011, opposition activists in Moscow used Facebook to organize street protests in reaction to the December 2011 State Duma elections, although local platforms like Vkontakte are more popular tools for political mobilization in other regions.[44] Organizers of subsequent protests, such as those related to Putin's inauguration in May 2012 and the January 2013 "March Against Scoundrels" protesting the bill banning Americans' adoption of Russian children, have also made use of social-networking platforms to call attention to events. Additionally, crowdfunding websites such as RosUznik.org, which raises money for and coordinates the legal defenses of civil activists charged in the Bolotnaya Case, have emerged as a way for opposition activists to organize support efforts online.[45]

Violations of User Rights

During 2012 and early 2013, government pressure against online users continued to escalate through the use of lawsuits, administrative prosecutions, unlawful criminal prosecution using anti-extremist legislation, and charges for offending government officials. In July 2012, the State Duma introduced legislation that recriminalizes defamation for both online and offline speech. Additionally, the Russian government continues to employ surveillance methods that circumvent proper judicial oversight requirements and which threaten the civil liberties of online users.

Although the constitution grants the right to free speech, this right 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. Recently, police have been suppressing online expression through the use of 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." The phrase "social group" is particularly problematic as the criminal code does not clearly describe what a social group entails, and several extremism cases in 2012 involved broad definitions of the term "social groups" to include the United Russia political party and law enforcement officers.[46]

Despite claims that the State Duma is planning to adopt special legislation establishing criminal and civil liability for internet activities and offenses,[47] existing laws do not differentiate between online and offline activities. In the case of some crimes, such as defamation, slander, or extremism, use of the internet can be considered an aggravating factor.

In July 2012, the State Duma passed amendments to the criminal code that recriminalized defamation, after having just decriminalized it less than a year earlier. The revision of Article 128.1 of the code makes it easier to use this provision arbitrarily with the aim of pursuing those who criticize government policy. Revisions to Article 129 of the code officially make defamation a criminal offense, with applicable punishment including a fine of up to RUB 5 million (approximately $170,000). Previously, when prosecuted for defamation, one could typically expect a suspended sentence, especially as a first offender. Now the maximum possible fine allowed under the criminal law can be applied under section 5, Article 128.1, with no reduction in other negative legal consequences for the person convicted.

A draft law concerning the introduction of criminal liability for publicly insulting the feelings of religious believers was introduced in the State Duma in September 2012.[48] The law, which came

into effect on July 1, 2013, establishes fines up to RUB 300,000 (approximately $10,000) or 1 year imprisonment. Critics point out that the law is too vaguely worded and that key terms, such as "worship" or "religious traditions," are not properly defined, making it difficult to predict the ways in which the law will be implemented. It is also unclear in what ways online activities might be prosecuted under this new law.

The practice of criminal prosecution has expanded over the past year: in 2012 there were 103 cases of criminal prosecution against online users, compared to 38 cases in 2011.[49] The majority of these cases were related to incitement of hatred against national and social groups or calls for extremism published on social networks. A few charges for insulting government representatives and inciting riots have been registered as well. In April 2012, blogger Dmitry Shipilov was sentenced to 11 months of correctional labor for his brusque article addressed to the governor of the Kemerovo region, Aman Tuleev.[50] The Investigative Committee of the Russian Federation opened a criminal case in March 2012 against journalist and blogger Arkadiy Babchenko for writing a blog post encouraging an unauthorized protest, with references to using force against police authorities.[51] Additionally, on May 14, 2012, State Duma deputy Aleksandr Khinshtein sent a request to the General Prosecutor's Office to open a criminal case against users of Twitter and Facebook who called for participation in public protests in Moscow on May 6, 2012, though it appears that the General Prosecutor has not acted on the request.[52]

Various forms of administrative and legal pressure against online bloggers and activists continued in 2012-2013. In August 2012, Maksim Efimov, the chair of the Karelia Youth Human Rights Group, sought asylum in Estonia after prosecutors requested that he be committed to a psychiatric ward. In April 2012, Efimov was charged with insulting the feelings of Orthodox believers for his critical article entitled "Karelia is tired of priests," which described the close cooperation between the Karelian regional government and representatives of the Russian Orthodox Church.[53] Efimov has been granted political asylum in Estonia, while the criminal case against him remains under investigation by the Karelian Investigative Committee.[54]

In May 2012, a civil activist from Tuymen, Nikolay Lyambin, was arrested on suspicion of drug possession. Lyambin claims that the drugs were planted and relates his detention and prosecution to his activities online, as he was one of the creators of an opposition group on the social network Vkontakte.[55] In February 2013, Pavel Khotulev, who criticized regional standards of education in Tatarstan in his blog post, was sentenced to pay a fine of $3,300 for incitement of hatred against Tatars.[56]

Privacy and anonymity are key concerns for many online users in Russia. There are currently no restrictions on the use of circumvention tools or anonymizers, although such tools may be banned in the near future. Presently, identification is needed for signing a contract for internet access or cellular services. Additionally, owners of public Wi-Fi spots are required to use content filters to protect children from potentially accessing "harmful" information (Article 6.17 of the code of administrative offenses). This requirement may force owners to implement age checks for users. In October 2012, State Duma members from the Liberal Democratic Party of Russia revived the idea of forcing social network users to enter their passport details when registering on these websites.[57] However, later that month the State Duma decided that this proposal was unnecessary.[58]

The extent to which internet users in Russia are subject to extralegal surveillance of their online activities remains unclear; however, recent evidence suggests that the Russian government has

significantly increased its surveillance capabilities over the past few years. Since 2000, all ISPs have been required to install the "system for operational investigative measures,"[59] 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 and log data passing through a digital network.[60] ISPs that do not comply with SORM system requirements are promptly fined, and may have their license revoked if problems persist. Russian authorities are technically required to obtain a court order before accessing an individual's electronic communications data; however, the authorities are not required to show the warrant to ISPs or telecom providers, and FSB officers have direct access to operators' servers through local control centers.[61]

There is increasing evidence that Russian surveillance technology is being used for political purposes, including the targeting of opposition leaders. In a Supreme Court case in November 2012 involving Maxim Petlin, an opposition leader in the city of Yekaterinburg, the court upheld the government's right to eavesdrop on Petlin's phone conversations because he had taken part in so-called "extremist activities," namely antigovernment protests. Online surveillance represents somewhat less of a threat in the major cities of Moscow and Saint 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.

Extralegal intimidation is also used to limit users' abilities to interact and mobilize on the internet. For example, in the fall of 2012, Yuliya Bashinova, a journalist at the internet publication Grani.ru, was summoned for questioning by the Investigative Committee to explain why she had signed a petition on the website of Amnesty International in support of human rights defender Igor Kalyapin.[62] It has been reported that investigators have held talks with citizens who signed the petition in several Russian cities.

Despite the reduction in the severity of violence over the past year, implicit impunity for those who commit violence against bloggers, online journalists, and other online users is common. Information on investigations into crimes committed in previous years is usually not available to citizens. Between 2008 and 2011 there were three internet-related murders and one attempted murder, according to research conducted by the AGORA Association.[63] Only one of these resulted in a prosecution: according to the verdict, the murder of Magomed Evloev, the owner of the website Ingushetia.ru, was the result of a police officer's careless handling of a gun.[64] There has been no prosecution dealing with the attempted murder of journalist and blogger Oleg Kashin, and there were dozens of other assaults and beatings for which no individual has been brought to justice. Critics blame the Russian Federal Security Service for failing to provide the necessary operational support to solve such cases.[65]

From 2012-2013, the threat of cyberattacks continued, including DDoS attacks on websites and hacking into the private accounts of users. The police and Investigative Committee have consistently failed to investigate these attacks, including dozens of cyberattacks on online media and opposition websites. During 2012, at least 47 episodes of DDoS attacks were registered,[66] but only 2 of them (against the official websites of the government and the prime minister) were investigated.[67] Most of the attacks occurred during important events such as the presidential election or mass protests. There were also significant attacks launched against independent media outlets. In May 2012, a botnet of 182,000 computers was used to attack the website of the television

channel Dozhd. On June 12, 2012, a single botnet made up of 133,000 computers attacked four online media outlets, including the websites of *Novaya Gazeta*, the radio station Echo of Moscow, Slon.ru, and the website for Dozhd.[68] In the past, similar cyberattacks on media outlets have been linked to leaders of the progovernment youth group Nashi.[69]

In January 2013, President Vladimir Putin signed Decree #31c "On the formation of a state system for detecting, preventing and mitigating the effects of computer attacks on the information resources of the Russian Federation." Under this decree, the FSB has been vested with the task of developing a method for preventing and investigating attacks by hackers on Russia's internet resources, and with promoting international cooperation in the fight against cybercrime; however, no further steps have been taken toward the prevention of cybercrime.

Notes

---

1 Elena Milashina, "Russia steps up crackdown on rights groups, Internet," Committee to Protect Journalists, March 26, 2013, http://www.cpj.org/blog/2013/03/russia-steps-up-crackdown-on-rights-groups-interne.php#more.

2 Anastasia Golitsyna, "Google ускоряет шаг" [Google Speeds Up], Vedomosti.ru, January 29, 2013, http://www.vedomosti.ru/newspaper/article/383941/google_uskoryaet_shag.

3 "Russian Domains" [in Russian], Statdom.ru, accessed July 30, 2013, http://statdom.ru/.

4 "Russian Customers Fill Up European Data-Centers" [in Russian], accessed July 30, 2013, http://www.deac.lv/?object_id=16936.

5 Alan Cullison, "Russia Investigates Allegations Against Opposition Blogger," *Wall Street Journal*, January 11, 2013, http://online.wsj.com/article/SB10001424127887324581504578236031175757590.html?KEYWORDS=Russia.

6 "Estonia Grants Political Asylum to Blogger Who Criticised Russian Orthodox Church," Agora Human Rights Association, October 19, 2012, http://agora.rightsinrussia.info/archive/news/efimov/asylum.

7 Public Opinion Foundation, "Интернет в России: динамика проникновения. Осень 2012" [Internet in Russia: Dynamics of Penetration. Fall 2012], December 18, 2012, http://runet.fom.ru/Proniknovenie-interneta/10738.

8 International Telecommunication Union (ITU), "Percentage of individuals using the Internet," 2007 & 2012, accessed July 13, 2013, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

9 Public Opinion Foundation, "Internet in Russia. Report highlights," accessed July 30, 2013, http://www.ewdn.com/wp-content/uploads/2013/03/FOM_Internet_Winter_2012_20131.pdf.

10 Public Opinion Foundation, "Internet Audience: Yesterday, Today, Tomorrow ... " [in Russian], November 29, 2012, http://runet.fom.ru/Proniknovenie-interneta/10714.

11 Advanced Communications & Media, "Cellular Data," accessed July 30, 2013, http://www.acm-consulting.com/data-downloads/cat_view/7-cellular.html.

12 "Medvedev Commanded to Decrease the cost of Internet access in Russia" [in Russian], RIA Novosti, January 21, 2013, http://ria.ru/economy/20130121/918943794.html.

13 Maria Petrova, "Broadband Access to the Internet Must Become Cheaper" [in Russian], Comnews.ru, January 22, 2013, http://www.comnews.ru/node/69851.

14 "В село проведут инновационную сеть," RBC Daily, January 22, 2013, http://www.rbcdaily.ru/media/562949985558334.

15 "Dynamics of Internet penetration in Federal Districts and settlements" [in Russian], December 18, 2012, http://runet.fom.ru/Proniknovenie-interneta/10738.

16 "Mobile Internet Market Review. Use of mobile internet through smartphones and tablet PCs," J'son and Partners Consulting Official Website, January 2013, http://bit.ly/15BZjTz.

17 Компьютерная оснащенность школ. РИАН ["Computer equipment in schools"], RIA Novosti, September 11, 2012, http://ria.ru/ratings/20120911/747679545.html.

18 "Стартовали проектно-изыскательские работы по строительству подводной ВОЛС «Сахалин-Магадан-Камчатка»" ["Ctartovali design work for the construction of underwater fiber-optic 'Sakhalin-Magadan-Kamchatka'"], Corporate website of Rostelecom, June 9, 2012, http://www.kamchatka.rt.ru/press/news/news877.

19 "Russians to link eastern islands by cable," Global Telecom Business, May 16, 2012, http://www.globaltelecomsbusiness.com/article/3029654/Russians-to-link-eastern-islands-by-cable.html.

20 "The island of Sakhalin is still very far away," *The Economist*, April 5, 2010, http://www.economist.com/blogs/babbage/2010/04/broadband_prices_russia.

21 Dmitry Runkevich, Депутаты запретят анонимность в сети [The deputies shall ban anonymity on the Net], Izvesita.ru, September 21, 2012, http://izvestia.ru/news/535724.

22 "Russia's FSB mulls ban on 'Tor' online anonymity network," RT.com, August 16, 2013, http://rt.com/politics/russia-tor-anonymizer-ban-571/.

23 Advanced Communications & Media, "Russian Residential Broadband Data 2012," accessed July 30, 2013, http://www.acm-consulting.com/data-downloads/cat_view/16-broadband.html.

24 Интернет в глубинке: обзор стоимости ШПД в небольших городах [Internet in remote places: overview of broadband access cost in small towns], Telecomza.ru, April 17, 2013, http://telekomza.ru/2013/04/17/internet-v-glubinke-obzor-stoimosti-shpd-v-nebolshix-gorodax/.

25 Advanced Communications & Media, "Cellular Data 2012," accessed July 30, 2013, http://www.acm-consulting.com/data-downloads/cat_view/7-cellular/19-cellular-2012.html.

26 "Jehovah's Witnesses website identified as extremist" [in Russian], SecurityLab.ru, June 15, 2012, http://www.securitylab.ru/news/425840.php.

27 "Register of extremist materials was replenished with an article by Yuri Afanasyev" [in Russian], Agentura.yu, February 19, 2013, http://www.agentura.ru/news/28138.

28 "The Register Monitoring" [in Russian], February 27, 2013, http://rublacklist.net/4445/#more-4445.

29 "Russia," Google Transparency Report 2012, accessed July 30, 2013, http://www.google.com/transparencyreport/removals/government/RU/?hl=en_GB.

30 Ibid.

31 "Google Transparency Report: Russia," July-December, 2012, accessed July 30, 2012, http://www.google.com/transparencyreport/removals/government/RU/.

32 Maria Kravchenko, "Inappropriate Enforcement of Anti-Extremist Legislation in Russia in 2012," edited by Alexander Verhovsky, SOVA Center for Information and Analysis, June 26, 2013, http://www.sova-center.ru/en/misuse/reports-analyses/2013/06/d27382/#_Toc357760970.

33 "2012 Surveillance: Russia," Reporters Without Borders, March 12, 2012, http://bit.ly/VoO1HS.

34 "Federal list of extremist materials," Ministry of Justice official website, accessed July 30, 2013, http://minjust.ru/ru/extremist-materials?search.

35 AGORA Association, Доклад: Россия как глобальная угроза свободному Интернету [Report: Russia – a global threat to Internet freedom], http://eliberator.ru/news/detail.php?ID=21.

36 Twitter account of the Head of Russian Association for Electronic Communications (RAEC) Sergey Plugotarenko [in Russian], December 21, 2012, https://twitter.com/plugotarenko/status/282014753851854848/photo/1.

37 "The Terms and Conditions of Domain Names Registration in domains .RU and .Ð Ð¤," The Coordination Center for TLD RU, accessed July 30, 2013, http://cctld.ru/en/docs/rules.php.

38 "Rules Governing Registration of Domain Names Allow Law Enforcement to Arbitrarily Block Websites," Agora Human Rights Association, February 7, 2012, http://agora.rightsinrussia.info/archive/news/domains/andrei-rylkov.

39 Roman Zholud, "Labelling [sic] a web publication 'extremist,': how this is done in Oryol," Glasnost Defense Foundation Digest No. 586, Glasnost Defense Foundation, October 8, 2012, http://www.gdf.ru/digest/item/1/1016#ev1.

40 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.

41 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.

42 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.

43 Законопроект No.-81110-6 [Draft Bill #81110-6], Official State Duma website, accessed July 30, 2013, http://bit.ly/NlBpxl.

44 Tom Balmforth, "Russian Opposition 'Likes' Facebook," Radio Free Europe / Radio Liberty, May 18, 2012, http://www.rferl.org/content/russian-opposition-likes-facebook/24585388.html.

45 "Arrest extension validated for Moscow riot participants," Russian Legal Information Agency, August 8, 2012, http://rapsinews.com/judicial_news/20120806/264133072.html.

46 Maria Kravchenko, "Inappropriate Enforcement of Anti-Extremist Legislation in Russia in 2012," edited by Alexander Verhovsky, SOVA Center for Information and Analysis, June 26, 2013, http://bit.ly/18A40f8.

47 Vladimir Bogdanov, Анонимки на просвет [Anonymity on clearance], RG.ru, September 11, 2012, http://www.rg.ru/2012/09/11/anonim.html.

48 Законопроект No.-142303-6 [Draft Bill #142303-6], Official State Duma website, accessed July 30, 2013, http://asozd.duma.gov.ru/main.nsf/(SpravkaNew)?OpenAgent&RN=142303-6&02. See also "Analysis on Russia's New Blasphemy Law: 28 February 2013," The Institute on Religion and Public Policy, http://www.religionandpolicy.org/reports/the-institute-country-reports-and-legislative-analysis/europe-and-eurasia/russia/analysis-on-russia-s-new-blasphemy-law-2013/.

49 "Russia: a global threat to internet freedom," Agora Human Rights Association, February 4, 2013, http://agora.rightsinrussia.info/archive/reports/global-threat.

50 "Блогер получил 11 месяцев за оскорбление Тулеева" [Blogger received 11 months for insulting Tuleyev], Grani.ru, April 3, 2012, http://grani.ru/Internet/m.196855.html.

51 "Independent journalist sued for 'extremist' blog entry," Gazeta.ru, March 21, 2012, http://en.gazeta.ru/news/2012/03/21/a_4099301.shtml.

52 "Retweeted to General Prosecutor", Gazeta.ru, May 14, 2012, http://www.gazeta.ru/politics/2012/05/14_a_4583269.shtml.

53 Vyacheslav Kozlov, "Blogger faces up to 2 years in jail for critising Russian Orthodox church," Gazeta.ru, April 13, 2012, http://en.gazeta.ru/news/2012/04/13/a_4345165.shtml.

54 "Blogger who Criticized Orthodox Church Seeks Political Asylum in Estonia," Agora Human Rights Association, accessed July 30, 2013, http://agora.rightsinrussia.info/archive/news/efimov/estonia.

55 "New fraud criminal cases in Tymen" [in Russian], Golosa.info, May 18, 2012, http://www.golosa.info/lambin.

56 "Pavel Hotulev has been convicted" [in Russian], Evening-Kazan.ru, February 15, 2013, http://www.evening-kazan.ru/news/pavlu-hotulevu-vynesen-obvinitelnyy-prigovor.html.

57 "В Госдуме рассматривают возможность регистрации в соцсетях по паспорту" [State Duma considering registering social networks with passport], Kommersant-FM, October 11, 2012, http://www.kommersant.ru/doc/2041985.

58 "MPs oppose passport details for social networks," Russian Legal Information Agency, October 12, 2012, http://rapsinews.com/legislation_news/20121012/264976106.html.

59 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. 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.

60 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.

61 Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," *World Policy Journal*, Fall 2013, http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.

62 "Grani.ru journalist summoned to Investigative Committee" [in Russian], Grani.ru, September 6, 2012, http://grani.ru/Society/Law/m.206066.html.

63 Ibid.

64 Svetlana Bocharova, "The end at the "Oriental Fairytale" [in Russian], October 4, 2010, http://www.gazeta.ru/politics/2010/08/04_a_3404590.shtml.

65 "Advocate blames FSB of inactivity while investigation of attempted murder of Oleg Kashin" [in Russian], Openinform.ru, November 6, 2012, http://openinform.ru/news/pursuit/06.11.2012/27620/.

66 AGORA Association, Доклад: Россия как глобальная угроза свободному Интернету, [Report: Russia – a global threat to Internet freedom], http://eliberator.ru/news/detail.php?ID=21.

67 Второй красноярский хакер получил срок за атаки на сайт Путина в мае 2012 года [Second hacker from Krasnoyarsk sentenced to jail for cyber-attacks against Putin's website on May 2012], Gazeta.ru, March 29, 2013, http://www.gazeta.ru/social/news/2013/03/29/n_2823469.shtml.

68 Alexander Panasenko, Впервые сайты четырех российских СМИ атакованы одним ботнетом [For the first time fout websites of Russian media are under attack of one botnet], Anti-Malware.ru, June 14, 2012. http://www.anti-malware.ru/news/2012-06-14/9345.

69 "Mail Leaks Link Youth Tsars to Cyberattack," RIA Novosti, February 9, 2012, http://en.rian.ru/russia/20120209/171235899.html.