The internet in Russia: the cradle of civil society

Jadwiga Rogoża

In the last decade, along with economic and technological growth, Russia has seen a dynamic development of the internet. Today the net is an everyday tool of work, information and entertainment for 40% of Russians – the most educated, active and affluent part of the society. The spread of the internet (known in Russia as the Runet) has, in turn, brought about significant political and social consequences. With the political and social sphere in Russia strictly controlled by the government, most of this activity has moved to cyberspace. The internet has become an alternative to the state-controlled media, a site for the free exchange of views and a home to numerous social initiatives. In this way, it has become a school of citizenship for Russians, and a kind of 'test tube' that has spawned social and political activity. This activity went beyond cyberspace in the election period in 2011/2012, and turned into massive street protests.

The potential of the internet has also been used by the Russian government, both to shape public opinion (via loyal online media) and to monitor civil initiatives, especially opposition ones. The state has many instruments of technical control and supervision of the internet and its users' activity. This control was used in the election period 2011/2012, when selected sites were blocked and pressure exerted on independent websites. These actions were a warning sign from the government, aimed at discouraging internet users from any opposition activity. However, it does not seem feasible that any restriction of such activity can be effective. The scale of this activity is now enormous, and attempts to censor the net and resorting to repression against internet users on a wider scale would only fuel resentment towards the government.

1. The Runet: its scale

The access to the internet in Russia is nowadays widespread, and its significance in people's everyday lives enormous. In the last decade, the number of internet users has surged from 3.1 million users in 2000 to **52-54 million daily users** in early 2012 (nearly **40% of the population**)[1]. The reason behind this is the rapid economic growth that Russia has noted since 2000, and the dynamic development of information and telecommunication technologies, which has made internet devices more available, connections faster, and costs lower.

[1] For details, see ComScore and Internet World Stats.

Recent years have seen a rapid growth of wireless internet (via Wi-Fi and WiMax); today about a third of Russian users surf the net via wireless internet devices (smartphones, iPads etc.). The Russian internet comprises about 100,000 websites, 4,000 of which are officially registered at the Ministry of Communications as the 'internet media'. Nevertheless, the Russian-speaking internet is not limited to the .ru domain; it also includes the (less popular) .su domain (the acronym refers to the USSR), Russian-language websites in the post-Soviet states, and those registered on international domains (.com, .org and other). In June 2008, a Cyrillic domain (.рф) was created. Russia's most popular websites are **search engines and social networks**. The specific feature of the Runet is that its users **prefer their national equivalents** (the VKontakte social network and the Yandex search engine) to the global leaders such as Facebook and Google. The Runet's leading sites are the aforementioned Yandex and VKontakte, the Mail.ru portal, followed by Google.ru and Google.com, and the top ten is rounded off by the Livejournal.com blog service[2]. One of the most popular sites is YouTube, where Russians post their videos, including those concerning political and social affairs. The leading news websites are RIA Novosti, RBC.ru, Lenta.ru and Gazeta.ru[3]. Another website worth mentioning is the online infotainment television Dozhd (tvrain.ru), popular with the Russian middle class and available both on the internet (including smartphones) and on cable and satellite.

Most Russians use the internet for **entertainment, contacts and information**. In early 2011, the internet outstripped traditional paper press in terms of the number of people searching for information about Russia and the world[4]. Most of the Russian population (70%) still turns to television as their primary source of information, but this share is constantly decreasing in favour of the internet. Currently the net is the main source of information for a quarter of the Russian public – the most dynamic, educated and affluent part of society[5]. A trend observed among internet users and the Russian intellectual elite is their openly negative attitude towards television, a medium controlled by the government and offering low-quality commercial product. The representatives of the aforementioned groups openly declare that they do not watch television. Therefore, even though TV remains Russia's most popular medium, it does not shape the opinions and moods of the most active and educated part of society.

> **Russia's most popular websites are search engines and social networks. However, Russian users prefer their national equivalents (VKontakte social network and Yandex search engine) to global leaders – Facebook and Google.**

2. An information alternative

The internet has long been a full-fledged mass medium, and its efficiency and pluralism make it an unrivalled source of information, especially when covering dynamic events and presenting diverse standpoints. Unlike traditional media (television, press, especially the high-circulation titles) which are controlled by the state, the internet allows for posting **unselected and politically uncensored** content. The Runet contains an **entire spectrum of ideological and political standpoints**: democratic, liberal, left-wing, leftist, anarchist, nationalist, pro-government, opposition and politically non-aligned. The leading online media (Gazeta.ru, Lenta.ru, RBC, Yandex and others), visited by millions of users daily, pursue an independent information policy. Russia's extensive **blogosphere**, apart from being a source of information and entertainment, is also a discussion forum and a tool for coordinating civic initiatives. The top Russian bloggers who specialise in social and political issues have tens to hundreds of thousands of readers. The Runet's most popular bloggers

2 See http://maxonline.3dn.ru/index/samye_populjarnye_sajty_runeta/0-15

3 See http://www.alexa.com/topsites/countries/R

4 Pew Research Center, see *Gazeta.ru*, 18 March 2011.

5 'Rossiyane zamenyayut televideniye internetom', http://news.softportal.com/nitem-11562.html

are Rustem Agadamov (drugoi.livejournal.com, 74,000 registered readers, and a larger number unregistered), Alexei Navalny (navalny.livejournal.com, 67,000 registered readers), and the internet activist and commentator Anton Nosik (dolboeb.livejournal.com, 38,000 registered readers). These numbers compare to or even exceed the circulation of many influential Russian newspapers (*Nezavisimaya Gazeta* has a daily print run of 40,000 copies, *Vedomosti* 75,000, and *Kommersant* 125,000).

One of the internet's features – the principle of interactivity – has **altered the relationship between the state and society in terms of information exchange**. Previously, society was a passive recipient of the information generated by the state and transmitted through the loyal media. The news were prepared by professional (and amenable) journalists; whatever did not appear on television, could not reach a wider audience and become national or even regional news. With the expansion of internet access and new technologies, especially mobile devices (smartphones), the Russian-language cyberspace has become a **fully-fledged news generator**. An increasing share of this news is provided by ordinary users, who become **witnesses** to interesting events and can easily make them public. Along with this process, the government is gradually **losing its monopoly on the creation of news and political messages** on the national scale. As a result, much information critical of the government is beginning to reach the public. The authors of these high-resonance reports include frustrated state officials or employees of the institutions of force, who uncover various faults and shortcomings in the state institutions. One of the most notorious 'whistleblowers' was a police captain, Alexei Dymovsky, who in 2009 in a series of videos posted on YouTube revealed the in corruption, nepotism, the ruthlessness of his superiors, lawbreaking by senior officials (tampering with statistics, drug trafficking) which were prevalent in the Interior Ministry. In this way, the internet has gradually become an alternative source of information and a **tool for social control** of the government's activities at all levels.

> The internet has become an alternative to the government-controlled media, and has undermined the state's monopoly on the creation of nationwide news and political messages.

The **decentralisation of the information process has strengthened social control of the government**, one example of which is the public's changing approach to law-breaking by the political and business elite. One of the most notorious problems in Russia is the road accidents caused by VIPs who drive cars equipped with special signs of privilege (such as the detachable flashing blue lights called *migalka* in Russian) and frequently violate traffic regulations. Formerly, such cases were rarely publicised or were hushed up (such as a little-known fact that in 1997, the then chauffeur of Vladimir Putin, who at the time was an official of the Presidential Administration, struck and fatally injured a child). In subsequent years, such news reached a rather narrow circle of internet users and readers of the opposition press (such as the accident caused in 2005 by the son of Deputy Prime Minister Sergey Ivanov, who knocked down and killed an elderly woman on a pedestrian crossing). Now the situation has changed completely. It is almost impossible to hush such accidents up – witnesses publicise them on the internet, the information reaches a wide audience and often causes an indignant public response. In cases of a gross violation of the law, internet users have been able to initiate an investigation and alter the course, and even the outcome, of the proceedings[6].

6 An example from 2010 is the accident in Moscow caused by Anatoly Barkov, a vice-president of the Lukoil corporation.

3. A prosthesis to democracy

As the internet expanded, it became a home to the political and civic activity which was encountering difficulties in the 'real world' because of the government's control over the social and political sphere. This control made it difficult or even impossible to register a political party, establish an NGO, or obtain civil rights in court. In cyberspace, most of this 'unauthorised' activity has been conducted successfully. The internet has become not only a source of information, but also a **tool of social consolidation and coordination**. Online communities bound by common views and interests act as substitutes for political parties, and the blogosphere has become a public forum for exchanging information and opinions. Civil investigations have gained momentum, and political satire, which has been absent from the traditional media for years, flourishes in the internet. The net has become a bridgehead for the political opposition, which is reaching potential supporters via social networks and blogs, and also organising various actions, both virtual and conducted in the 'real world'.

In addition to activities related to politics, the internet is a site for various non-political initiatives, connected to charities, consumer protection, civil rights, culture and other issues. Many such initiatives have gained prominence and support on the national level and have motivated other citizens, who faced similar problems elsewhere. These initiatives, initiated and successfully completed thanks to the Runet, have proved **conducive to the development of attitudes characteristic of democratic societies**: the development of grass-roots initiatives, groups consolidating to defend common interests, and seeking to improve the people's legal awareness and education. This has helped overcome attitudes entrenched in Russian society – inaction, atomisation and low legal awareness – that had made the general public susceptible to the government's manipulation. Thus, the **internet has become a major counter-tool against the government's political and social strategy**, and this activity in cyberspace has become a forerunner and encouragement of such activity in the 'real world'.

> **Initiatives initiated and successfully carried out on the Runet have been conducive to the development of attitudes characteristic of democratic societies: the development of grass-roots initiatives, groups consolidating to defend common interests, and seeking to improve the people's legal awareness and education.**

One of the Runet's most remarkable phenomena in recent years has been the activity of the well-known blogger and lawyer Alexei Navalny, and especially the **RosPil** institution (rospil.info) which he founded. The aim of RosPil is to fight corruption: Navalny and the lawyers he has hired examine state tenders (also checking numerous reports sent by internet users) and initiate legal proceedings whenever these tenders raise suspicions of corruption. The whole documentation is published on their website. RosPil's activity is financed entirely by contributions from internet users; this has set a precedent in Russia, where attitudes of distrust and disbelief in the efficiency of collective action had predominated (for more cases of civil initiatives in the Runet, see the Appendix).

The internet (especially social networks and blogs) played a key role in the organisation of demonstrations at the end of 2011 and the beginning of 2012, which gathered tens of thousands of people in Moscow and other Russian cities in protests against electoral fraud. The evidence of electoral machinations and comments on the course and outcome of the elections were published on the internet, and the coordination of the rallies (including fundraising) was likewise conducted online. The leaders of electoral protests included activists who gained prominence thanks to their internet activity: Alexey Navalny, the aforementioned creator of RosPil and RosVybory and Petr Shkumatov, the founder of the Blue Bucket

Movement (see Appendix). This confirms once again that the **internet has become a school of civic activity** for the Russian people.

4. Cyber-propaganda: the government goes online

The internet has also been used for years by the government as an increasingly popular information tool. All state and local government offices have their own websites, while blogging and tweeting is becoming increasingly popular among government officials. The internet became 'trendy' in the state administration after Dmitry Medvedev took office as president. He encouraged officials to communicate with voters online by his own example; he has a video blog on the Kremlin website and a Twitter account. One of Medvedev's latest internet projects is a portal called 'Russia without fools' (rossiyabezdurakov.ru), which is an imitation of civic initiatives aimed at combating corruption and bureaucracy. Recently even Prime Minister Putin has referred to internet reports, even though he had earlier distanced himself from the net (rumour has it that the Prime Minister is not a computer user).

Russian-language cyberspace – including the blogosphere and social networks – is also home to pro-government activists, experts and commentators. Until recently, the main political coordinator of the pro-government activity online was Vladislav Surkov, the deputy head of the Presidential Administration (in December 2011 he was appointed deputy prime minister). One area of such activity is a 'youth platform' managed by Vasily Yakemenko, the coordinator of a pro-government youth organisation 'Nashi' (Our Folk), and head of the government agency for youth. This platform comprises a number of blogs by and profiles of members of youth organisations; one of the most active users therein is the 'Nashi' spokeswoman Kristina Potupchik (krispotupchik.livejournal.com). Another platform consists of pro-government infotainment websites created and coordinated by Konstantin Rykov, currently an MP and a member of the United Russia party (his most popular sites include dni.ru, vzglyad.ru and infox.ru). A similar role is played by the blogs run by popular journalists and other public figures known for their support for the government, such as the TV presenter Tina Kandelaki (tikandelaki.livejournal.com) and the journalist Vladimir Solovyov (vsoloviev.livejournal.com).

> **All state and local government offices have their own websites, while blogging and tweeting is becoming increasingly popular among government officials.**

The state's internet resource base also includes websites that are either directly controlled by the government or indirectly support it. The leading ones include the website of the *Komsomolskaya Pravda* daily and the state-owned news agency RIA Novosti[7]. Another is the popular multimedia portal LifeNews.Ru, which is controlled by Yuri Kovalchuk, an oligarch affiliated with Vladimir Putin. This tabloid-like portal specialises in leaks (publishing wiretapped conversations, etc.) that are aimed at discrediting the opposition. A similar role is played by online digests that compile articles and leaks which discredit many public figures. The best known ones are Compromat.ru, a compendium about Russian politicians and businessmen (there were repeated suggestions that the website was founded at the inspiration of the Federal Security Service) and Politrash (politrash-ru.livejournal.com).

[7] Data from ComScore, November 2011.

5. Big Brother watches over the internet

For years, the Russian government has perceived the internet as an important source of information, and recently also as a tool for coordinating political initiatives, including opposition activity. The government was concerned with the role the web played in the organisation of opposition protests in Moldova (2009) and North Africa (2010–2011). In December 2011, internet-coordinated protests broke out in Russia following the parliamentary elections. This led several high-ranking Russian officials to publicly express their **concern about the uncontrolled activity of internet users**, and to call for a 'reasonable regulation of the internet'[8]. The managements of internet portals and websites were subjected to various kinds of pressure. The Federal Security Service ordered the director of Russia's most popular social network VKontakte, Pavel Durov, to close the discussion groups that criticised the government and coordinated the organisation of protests. When Durov refused, he received a summons to an interrogation at the Prosecutor's Office. Before the presidential election this March, the government exerted pressure on the Dozhd online TV station and the Ekho Moskvy radio station (which runs a popular website with news and comments). As in most countries around the world, the Russian government has extensive legal and technical instruments for control over the internet. The internet activity is regulated by the **Civil Code** which covers intellectual property, among other issues. The **Penal Code** also covers the activity of internet users (especially Article 282, which prohibits incitement to hatred or hostility and degrading human dignity), as well as the **law on counteracting extremism**. On the basis of the aforementioned acts, the Ministry of Justice has created a list of materials (including websites) classified as extremist[9]. Under the law on counteracting extremism, sanctions against individuals have also been applied. In 2008, an internet user from Syktyvkar who had expressed controversial statements about policemen in his blog received a court sentence. The court ruled that he had incited hatred towards a particular social group (the police), and sentenced him to one year's probation.

The Ministry of Communications is the state body authorised to exercise **technical control over the connections** and monitor the internet. The ministry may revoke any internet service provider's license or demand that any website be closed. Roskomnadzor, an agency which monitors communications and is subordinate to the Ministry, is responsible for issuing licenses for internet service providers, and for monitoring the content of websites to check that they comply with the law. If a particular website is considered extremist, Roskomnadzor requests the operator to block it. The Federal Security Service, whose tasks include 'providing information security' (Articles 8 and 11.2 of the law on the FSS), also has extensive powers to monitor the activity of internet users. Since 2000, the Federal Security Service has operated the SORM-2 programme (a system of technical measures to conduct investigations), under which it can monitor internet and telephone connections without the sanction of the court; operators are obliged to provide access to lines of communication, otherwise their licenses may be revoked.

The government also has informal control over Russia's largest domain registration centre, the private company Ru-Center, which is owned by Mikhail Prokhorov, an oligarch affiliated with the Kremlin. This control has already been used in the pre-election period. Ru-Center announced it would block all domains with illegal content (including incitement to violence, extremism and subversion of state power). In February 2012, Ru-Center closed the website

> Since the internet-coordinated waves of protests in North Africa (2010–2011) and Russia (2011–2012), high-ranking Russian officials have expressed their concern about the uncontrolled activity of internet users.

[8] See the statements by Nikolai Patrushev, secretary of the Security Council, and Prosecutor General Yuri Chaika.

[9] The list of materials which are considered to be extremist: http://www.minjust.ru/nko/fedspisok

of the Helix centre, which specialised in election monitoring. The government can also block users who operate on foreign domains, with the assistance provided by the big global internet companies. First Twitter and then Google introduced the practice of blocking selected reports at the request of local authorities, whenever the latter consider that these reports violate the law of that particular state.

Apart from activities that are conform to Russian legislation, the opposition activists who operate in cyberspace face **actions that run counter to the law**, and which are interpreted as having been inspired by the government. The purpose of such actions is to **discipline or intimidate unruly internet users** by interfering with their websites and blogs, and signalling that their activity (including their private lives) is being monitored. One such form of pressure are **hacker attacks** that paralyse the opposition and independent websites. In recent years, the most common type of attack have been DDoS attacks (a distributed denial of service), with multiple computers trying to access a given website simultaneously. The culmination of such attacks occurred in the pre-election year of 2011; many websites associated with civic and opposition activity were blocked. The last large-scale attack took place on the **parliamentary election day,** 4th December 2011. The websites blocked included

> **Opposition activists who are active in cyberspace face actions that actually violate Russian law, and are aimed at disciplining or intimidating the unruly internet users.**

the site of the independent electoral observers Golos (which was planning to post up-to--date information on electoral violations), the popular Slon.ru website (which cooperated with Golos in publicising violations), the website run by Ekho Moskvy, the site of the New Times weekly, and finally, the Livejournal server, a home to Russian opposition and civil activists' blogs. Opposition bloggers also frequently face **trolling**, i.e. anonymous users posting controversial or incriminating comments, aimed at discrediting the authors of blogs or causing conflict among their readers.

Another practice aimed at users who support opposition initiatives on the internet is their **identification and disclosure of confidential information**. For example, personal details of people who financially supported Alexei Navalny's RosPil website via the Yandex-Payments portal were leaked in July 2011. Navalny later revealed that the Federal Security Service and the Ministry of Interior had requested Yandex for access to this data. Several months later, in October 2011, Navalny's mailbox was hacked and his e-mails of recent years were made public. Russia's most infamous hacker, nicknamed Hacker Hell, admitted to having broken into Navalny's mailbox; previously Hacker Hell had hacked the mailboxes of several other opposition bloggers and commentators, and was accused of acting on the orders of the Federal Security Service[10]. In recent months, wiretapped telephone conversations by opposition activists were posted on the net: a few days before a massive opposition rally (24 December 2011), the LifeNews portal associated with the government published telephone conversations by Boris Nemtsov, wherein he spoke critically about other opposition leaders. Video recordings from the opposition activists' homes were also posted on the net: in January 2012, a vulgar recording aimed at discrediting another opposition leader, Vladimir Ryzhkov, circulated on the web. It is worth stressing that only state investigating bodies (with court permission) are authorised to conduct wiretaps in Russia.

The **political inspiration** behind the hacker attacks and break-ins into the mailboxes of the opposition activists is often attributed to the former deputy head of Presidential Administration Vladislav Surkov[11]. Additional information that may confirm this opinion appeared in February 2012, when the internet correspondence of Kristina Potupchik (the activist of the pro-government youth movement 'Nashi') was made public. This time it was Potupchik herself who fell victim to the international hacker group Anonymous. The contents of her

[10] See http://www.anticompromat.org/gopniki/hellbio.html, http://dolboeb.livejournal.com/2256543.html

[11] See http://dolboeb.livejournal.com/2275327.html i http://www.anticompromat.org/raznoe/shevyakbio.html

mail as disclosed testified that she had coordinated hacker attacks on opposition websites and blogs at the request of Yakemenko and Surkov. Officially, the state does not respond either to hacker attacks or to allegations that such attacks are politically motivated. After scandals caused by attacks on the blogosphere in July 2011 (when the Livejournal server was blocked for several days), President Medvedev ordered the law enforcement bodies to investigate the case; however, the Interior Ministry concluded that there was no reason to initiate such proceedings.

6. Prospects

The Russian government has extensive technical tools to supervise internet activity, and to block those initiatives it considers troublesome. However, the main challenge for the government is the **massive scale of internet activity**. It is difficult to effectively monitor and block internet users who support the opposition when they number in the millions. In this situation the government is likely to **use selective repressions**, targeting the most active bloggers and popular online media. Their methods may include economic sanctions (penalties, blocking funding) and various forms of provocation (leaking personal information that could tarnish the reputation of a given person). However, the effectiveness of such actions may also be limited. The advanced development of the internet makes it possible to organise and finance independent activity online, be it the media or other civil projects. Nor have previous prosecutions of internet users proved to be a sufficient scare. The users have not wrapped up their political activity; on the contrary, cases of pressure from the state have been publicised, and the victims have been provided with support. Therefore, repressive actions on a larger scale could actually fuel social resentment and consolidate the public against the government.

> The main challenge for the government is the massive scale of internet activity.

The prospects of social and political developments in the coming years, including Vladimir Putin's return to the Kremlin, indicate the **worsening conflict** between the state, which will seek to regulate the political, social and information sphere, and the 'internet generation', who have developed attitudes that are contrary to the essence of Putin's system of rule – an acceptance of pluralism and free exchange of views, the know-how of organising grass-roots actions. The experience acquired online has already affected the political and social realities of Russia, an example of which was the recent mass political protests. Therefore, even if repression is used against 'indignant internet users' after Putin's return to the Kremlin, the government will hardly be able to curb or reverse the civil processes that have progressed thanks to the development of the internet.

> The 'internet generation' has developed attitudes that are contrary to the essence of Putin's system of rule – the acceptance of pluralism and the free exchange of views, active grass-roots actions.

APPENDIX

CIVIL INITIATIVES IN THE RUNET

RosYama (rosyama.ru), literally 'a dip in the [Russian] road' – a portal created by Alexey Navalny, aimed at documenting and improving the disastrous state of Russian roads. Internet users from all over Russia post pictures of pits and bumps, and the information is sent to the officials responsible for road infrastructure in the given region. Under the law, the state bodies are obliged to repair the damages within 37 days.

RosVybory (rosvybory.org), literally 'Russian elections' – another project by Alexey Navalny, created before the 2012 presidential elections. The portal coordinated the activity of independent election observers (registration, training, etc.).

Blue Bucket movement (sineevedro.ru) – another popular civic initiative that concerns roads. This website documents the violations of traffic regulations by Russian VIPs, which is an acute social problem, especially in Moscow. The name of the movement refers to the special signs of privilege that the elite's cars are equipped with (flashing blue lights, resembling a small bucket, called 'migalka' in Russian).

Pomogi.org (Help.org) – a charity portal that helps sick children. For the last seven years the website has collected 192.5 million roubles (about US$6.5 million) from contributions from internet users, and has financed over 1200 projects.

Russian Fires (russian-fires.ru) – a portal created in the summer of 2010, when Russia was ravaged by a wave of fires. The website coordinated assistance for the victims of fires, and was awarded the title of best social site in 2010.