Cyber Security and Internet Protest

Author(s):
Giles, Keir; David, Maxine

Publication Date:
2013-07-30

Permanent Link:

https://doi.org/10.3929/ethz-a-009935869 →

No. 134 30 July 2013

russian analytical digest

www.css.ethz.ch/rad www.laender-analysen.de

CYBER SECURITY AND INTERNET PROTEST

German Association for East European Studies

Institute for European, Russian, and Eurasian Studies
The George Washington University

Research Centre for East European Studies
University of Bremen

Center for Security Studies
ETH Zurich

Institute of History
University of Zurich

ANALYSIS

Internet Use and Cyber Security in Russia

Keir Giles, London

Abstract

Intensive use of social media by an expanding population of Russian internet users gives rise to acute concern among the Russian security structures. This follows examples of facilitation of regime change by means of social media during the Arab Spring. At the same time, both the political impact of online activism, and the extent of measures taken by the authorities to mitigate it, have been exaggerated. Opinions on the nature and role of cyber security, and even on what to call it, vary widely within the Russian leadership, giving rise to confused policy. The release of a promised Cyber Security Strategy may bring some clarity.

Internet Use in Russia

The maxim that everything you read about Russia is both true and untrue at the same time is just as applicable to Russia's relationship with cyberspace as to other, more traditional domains. Contradictions abound not only between public policy on cyber security and actual practice, but also between the multiple public policies themselves. A perception in some quarters of draconian censorship and heavy-handed regulation needs to be placed in the perspective of the internet's relative liberality spilling over into other media; and focus on the internet as a dangerous political enabler for Russians needs to be set in the context of most users being primarily interested in its social and economic benefits.

Internet use in Russia continues to burgeon. A solid majority of Russian citizens are now internet users, and usage continues to spread rapidly beyond the original core of younger urban dwellers into other demographic groups. Importantly for Russian state security concerns, social media use is intensive, with 82% of internet users active on social media according to one 2012 poll, and usage "near-universal" among 18–24-year-olds according to another. Much-quoted figures from 2011 ranked Russians second in the world after Israel for time spent online in social networking.

The earlier perception that online media were far less significant than television and print is no longer valid. After a period of relative neglect, leading businessmen (including those with close ties to the current leadership) have acquired controlling stakes in key Russian internet resources over recent years. Equally, television executives have suggested that a recent increased flexibility and willingness to air controversial topics is an attempt to slow the trend of younger Russians abandoning television for the internet.

The Internet as Threat

Just as in other nations, the majority of Russians feel the effect of the internet in economic and social terms rather than as a political enabler. The intense attention given to the role of the internet in facilitating protests against election results in 2011–12 masked two important factors. First, in almost all cases where the internet is used to mobilise public opinion, even in cases of highly-publicised grass roots activism, the main benefits are improvement in very topical and local situations rather than mounting any kind of challenge to higher authority. Second, the internet gives a political voice to all factions, not just to activists for liberal democracy. Nonetheless, some sectors of the authorities are deeply concerned. In addition to frequent statements voicing alarm at the presence of material online which would be illegal in any country, a staple of commentary by the Russian security services regarding social media is the threat they pose to society as a whole.

The language used when describing the social media problem is often emotive. According to Leonid Reshetnikov, director of the Russian Institute of Strategic Studies (RISI) and a former SVR deputy director, the "conscious or unconscious destruction of all traditional ways of life is taking place" thanks to social media. As expressed by Maj-Gen Aleksey Moshkov of the Ministry of Internal Affairs in late 2011, "social networks, along with advantages, often bring a potential threat to the foundations of society". Naturally, foreign forces are alleged to be at work, as noted in commentary on social media by FSB First Deputy Director Sergei Smirnov in early 2012: "New technologies are used by Western secret services to create and maintain a level of continual tension in society with serious intentions extending even to regime change."

This alarm voiced by the security services is not a new concern that has arrived with the rise of social media, but a persistent narrative since the first public debates on the subject in the mid-1990s, when the internet as a whole was described by the FSB as a threat to Russian national security. A consistent argument since that time has been that Russian connection to the "world information space… is impossible without the comprehensive resolution of the problems of information security".

The view that political change in North Africa after the Arab Spring came about as a result of a Western information warfare and cyber conspiracy, which could now be implemented against Russia, fed into suspicion of foreign orchestration at the time of the election protests, and was subsequently vindicated by analysis of the role of social media in the Libyan civil war. These showed that social media can be used not only for the espionage, subversion, and circumvention of communications restrictions suspected by Russia's security services, but also for other instruments of regime change up to and including supplying targeting information for airstrikes. Assessment of Russian concerns over "misuse" of social media needs to be placed in the context of this perception of existential threat.

Security Responses

The most prominent visible trends in Russian cyber policy both domestically and internationally are bound up with attempts to mitigate this perceived threat.

Domestically, a number of largely short-lived initiatives such as the "Ring of Patriotic Resources" and the "School of Patriotic Bloggers" have recently given way to targeted investment in analysis of social media and both automated and human content influencers. In addition, some state-linked media are planning significant expansion into online operations, attracting existing journalistic talent from other outlets with offers of impressive salaries. The acquisition of key stakes in major websites by the Kremlin-friendly businesses noted above gives the authorities potential leverage over their content.

A number of new laws govern internet usage. Both a July 2013 law on protection of intellectual property online, and the July 2012 "internet blacklist" law setting up a "Single Register" of websites blocked because they are deemed threatening to minors, have been painted by activists and foreign media as state efforts to introduce internet censorship on ostensibly economic and moral grounds—including, potentially, censorship of social media outlets. But fears of sweeping powers to remove offending content from the internet, if not misplaced, are perhaps mistimed: these powers were already available to the Russian authorities through a number of legal and regulatory routes. Under the Federal Law "On Police" of 2011, ISPs can be instructed to shut down an internet resource on suspicion of providing "conditions which assist the commission of a crime or administrative violation", with no requirement for the police to seek a court order. And according to Russian domain name regulations, "the Registrar may terminate the domain name delegation on the basis of a decision in writing" by a senior law enforcement official—again, with no requirement for judicial oversight.

Despite allegations that the Single Register has been used to censor or stifle views critical of the government, the loudest criticism comes from those who note that it is a blunt instrument whose flawed implementation has serious unintended consequences—as, for instance, blocking YouTube because a zombie make-up instruction video is wrongly identified as promoting self-harm, or rendering Yandex unavailable for almost 30 minutes in late April 2013 due to its being accidentally added to the Register.

These criticisms are often directed at the Ministry of Communications, as the body with ultimate supervisory authority for the Register. The Ministry response, far from the hard line that critics of Russia often assume, is that it is asking the internet industry to self-regulate, and the Single Register is a mechanism for this—and furthermore, the Ministry should not be blamed as it is only implementing a Federal Law rather than its own regulations.

This passing the blame is symptomatic of a split not only between different departments in the Russian government and security structures, but even within individual ministries. Officials from bodies including the Ministry of Foreign Affairs, the Ministry of Internal Affairs, the Ministry of Communications, the Federal Security Service, the Security Council and the Presidential Administration (the latter two, voiced through their academic offshoots, the Institute of Information Security Issues and the Russian Institute for Strategic Studies respectively) make apparent policy statements on the role of the internet, and in particular on the limits to freedom of expression there, which are mutually contradictory. For this reason and others, commercial entities in Russia eagerly await the promised release of a new Cyber Security Strategy, which it is hoped will clarify at least some of the more controversial issues. Unusually and perhaps uniquely among Russian strategic documentation, this is being drafted by something approaching a true "multi-stakeholder" group, under the chairmanship of a Federation Council senator and including representatives of industry.

Internationally, Russia continues to promote its vision of global agreement on principles of information security. This long-running campaign saw a sudden intensification of effort in late 2011, producing both a Draft Convention on International Information Security and (jointly with China and others) an International Code of Conduct for Information Security introduced in the United Nations.

The provisions of these documents raise two points. First, they are at odds with Western principles in some of their key areas such as "national information space" (also described as network sovereignty), state management and governance of the internet, and the threat from hostile content as well as hostile code. Second, they are also dissonant with the everyday work of Russian commercial internet service providers and domain name authorities, who on a daily basis work to ensure the free and unobstructed flow of information across national borders simply because this is how the internet presently works in real life, as opposed to how some sections of Russia's security elite would wish it to work. Nevertheless, the extent of international support for Russia's initiatives needs to be considered seriously, not only from like-minded neighbours in the CSTO and SCO, but from a range of other states not normally thought of as major cyber actors but who share Russian and Chinese concerns over the destabilising potential of the internet.

Case In Point—VK

The line between well-intentioned regulation and official interference with the intent to suppress freedom of expression is sometimes indistinct. The case of VK (formerly VKontakte), with a leading position in Russian social media and a managing director with a history of resistance to pressure by the security services, is instructive. VK's daily visitor numbers approach the figures that watch state-owned Channel One TV. Following earlier closures of Russian file sharing websites in response to intellectual property protection initiatives, VK became recognised as a prime location for exchanging pirated music and films. But after the signing of the July 2013 anti-piracy law, VK mounted a brisk deletion campaign, ending its attraction to many users as a forum for free circulation of copyright material.

Since the new law renders the website owner liable for copyright breaches, this could be read as a straightforward business response to limit liability. But the speed and thoroughness of the response has also been interpreted as a response to mounting pressure on founder Pavel Durov, including not only the change in stakeholders in his company, but also apparently unconnected events such as a police raid on VK premises in April 2013 after Durov was accused of injuring a police officer while driving a car he supposedly does not possess. As with traditional media in earlier times, direct censorship of internet resources could be superfluous when other forms of messaging are available to the authorities to encourage compliance.

Conclusions

The announcement at the time of writing that Russian security structures were buying typewriters to avoid electronic interception is in fact nothing new. Despite causing excitement by being linked in the media to disclosures of the capability and reach of NSA and GCHQ, in reality it reflects a persistent and long-standing acute perception of the risks involved in online activity and the fact that the internet presents vulnerabilities as well as opportunities. Yet confusion over the nature of cyber security within the Russian leadership arises in part from the security services applying old information security principles to a new reality. The dissonance between this security approach, and that of the industry and ordinary users with an entirely different perception of cyberspace, finds expression in differences in the descriptive language used. This is demonstrated by an ongoing confrontation between the old concepts of "information security" as espoused by the security services and some sections of the Ministry of Foreign Affairs, and "cyber security", the term used by industry, users, and Foreign Minister Lavrov among others. In addition, it is clearly reflected in the inability of the Russian language to express some libertarian foreign concepts, leading to inelegant calques and barbaric direct borrowings such as *mul'tisteykkhol'derizm* for a multi-stakeholder approach.

Meanwhile, the nature of control of freedom of expression online in Russia is more subtle and nuanced than the heavy-handed censorship often described overseas, and it would be misleading to claim that the sole aim of recent legal initiatives is to suppress dissent. For the time being, most Russian internet users remain unconcerned at the prospect of interference with their online activity.

About the Author
Keir Giles is an Associate Fellow of Chatham House and Director of the Conflict Studies Research Centre.

ANALYSIS

@Russia.com: Online & Offline Protest

Maxine David, Guildford

Abstract

As online activism in Russia has combined with offline activism in the form of street protests, questions have been asked about whether we are witnessing a societal awakening that will result in widespread political and social change. More questions remain, however, about how representative protest has been or whether it is restricted to the comfortable urban middle classes. In the meantime, the state response has been swift and repressive, instilling fear amongst ordinary Russians and demonstrating capacity to extinguish the reformist agenda. This article looks at online demographics in Russia and what they mean for offline protest and political reform.

In the years since the so-called Arab Spring, the role of social media in bringing about social and political change has been much considered. Questions have also been asked about the likelihood of Russia undergoing the same kind of transformation, symbolic of widespread disappointment in the West about the trajectory of Russia's political development. Such questions have become all the more salient since the autumn 2011 announcement of then Prime Minister Putin that he and President Medvedev would be switching places in the next electoral cycle. This was the catalyst for the well-organised and well-attended street protests that took place in December 2011 following parliamentary elections, in March 2012 following presidential elections and on the eve of Putin's (re)inauguration as President in May 2012. Crucial to organising and gaining momentum for all the protests were the tools provided by social media, particularly Twitter and the very popular Russian equivalent of Facebook, VK. But to what extent can social media really act as tools of change in Russia and how deeply does their usage penetrate into Russian society?

This article identifies the range of social media available to and in use by the protest movement in Russia, looking particularly at demographic data in order to determine the extent to which online activity is representative of the Russian population as a whole. Such an analysis is necessary if we are to understand the likelihood of protest leading to long-term change in the political and social life of Russia.

Theorising Online Activism

The internet's main contribution for social movements lies as a source of information, especially on less mainstream media issues. Additionally, it provides a forum through which protest can be organised and political views expressed. The communicative and mobilisation potential of the internet for social movements is undisputed. Equally referenced but more problematic is the identity-building capacity of the internet, important if protest is to be sustained and consistent. The internet now performs the same function as urbanising processes did in previous eras, bringing together seemingly unconnected groups of people into a single space, facilitating the building of an understanding of the extent of shared situations and concerns. There are limits to the internet's potential, however, it is not an effective tool for building trust or resolving conflict: vital functions if divisions between groups are to be overcome.

While the internet is often seen as ungoverned (and ungovernable), in fact, various societal groups—government, NGOs, researchers and private businesses[1]—compete to determine the types of rules and norms that will preside. Russia is currently negotiating this space, but operating under high levels of state interference and in an environment where the government has a deep interest in ensuring its domestic digital divide is maintained. In the battle to shape the governing rules and to establish a firm presence online, finance is an important variable for it is often the wealthier organisations that use online potential most effectively. Again, theoretical arguments about the importance of finances to effective use of the internet and social media are supported in the Russian case where it has been the relatively well-off, urbanised middle classes who have been the voice of online (and offline) protest to date. However, this is a fact that has not gone unnoticed and unmanipulated by Putin and his supporters.

Where online activities are designed to bring about political and social change, they must be supplemented by offline activism that brings groups together in person. This appears to be well understood by Russian activists. Protests in Moscow and St Petersburg and beyond were largely organised and advertised online but had their greatest impact in respect of the numbers they drew and their sustained (between December 2011 and May 2012) nature. As a result, images of enormous (uncharacter-

[1] Ernest J Wilson (2005) 'What Is Internet Governance and Where Does it Come From?, *Journal of Public Policy,* 25 (1) 29–50.

istically so for Russia) numbers were conveyed—often via social media—to the world for a number of months.[2]

The BBC News Correspondent in Moscow at the time, Daniel Sandford, referred to the December 2011 protests as being "in many ways a political reawakening" for Russia. The real questions, though, were *who* was awoken and what would the government do about it? This political reawakening, after all, actually had roots in the online world of blogs and tweets of government opponents, long prior to the December 2011 street protests. However, these opponents were, and are, not necessarily representative of Russia as a whole. Digital divides exist across borders certainly but also within them and they are not restricted to differences in wealth. Demographic data on use of social media reveals other cleavages too in respect of which parts of society are online or not, effectively suggesting the online world is a divided and elitist one.

Online Demographics

That there is a digital divide in Russia becomes very clear from even the most cursory review of relevant data. June 2012 figures for internet usage in Russia show a penetration of 47.7%.[3] This is low compared to European states such as Germany with 83% penetration and Poland with 64.9%. Overall, Russia accounts for just 13.1%[4] of internet usage in Europe, unimpressive considering relative population figures. It is worth remembering, however, that Russian use of the internet has undergone exponential growth in the twenty first century. In 2000, only 2.1% of the population were internet users, by 2007 that figure had risen to 20.8%, 32.3% in 2009, and it is now near the 50% mark.[5]

Within these figures, there are large societal divides. 2011 data shows that only 20% of VK users are women, the vast majority of users are between 25 and 44 (approximately 80%), approximately only 11% earn under $25,000 and 40%+ are educated above high school, with over 90% educated to high school level.[6] Educational divides can be overcome; there is much evidence to show that organisations can function as educators for the use of digital media but there is not an obvious way of overcoming the other aspects relating to lack of properly representative online activity without political will on the part of the government.

Further limits to a fully representative protest movement exist inasmuch as the internet may be most useful as a source for mobilising those who are *already* interested in politics and activism and has little utility in turning people *towards* that area of interest and activity. This is extremely significant in the context of a state like Russia where a civil society is in the early stages of emergence. It is for all these reasons that it is common to refer to a "digital divide", a divide which is as evident in Russian society as elsewhere. While it is true that this divide should not be seen as insurmountable, the chances of the divide being closed at all swiftly in the Russian case look slim.

Notwithstanding recent growth, and bearing in mind potential discrepancies in statistics, it is safe to say that half of the Russian population currently does not use the internet. Given the state monopoly of the press and television, the lack of connectedness of so many ordinary Russians creates enormous problems for any opposition movements that: seek to elicit wide-ranging support for political change; offer alternative sources of information; or try to counter mis-information and government propaganda. Even when considering the percentage of the population that *is* connected to the online world, the numbers who rely on the internet as their primary or even secondary source of reference for news is very low. Television remains, overwhelmingly, the most important source of information. 84% of those polled for Levada Centre's annual report for 2010–2011 cited either Russian state or private television channels as their first main source of news.[7] Only 6% first cited the internet. Figures for the internet rose to 11% when respondents were asked for their second reference but this still compares unfavourably to a combined second reference for state and private television of 46%.

The digital divide is highly significant in that it gives room for the government to argue the opposition movement in Russia is not representative of the population and therefore lacks legitimacy. This has carved out room for a harsh response.

Protest and the State's Response

The state response to street protest has been swift and repressive in nature. It has acted to deter protesters from mobilising by detaining large numbers of them and then undertaking judicial proceedings against small

[2] Numbers are notoriously difficult to verify but for the December 2011 protests, for instance, *theguardian* reported protest organisers as saying 120,000 participated, the police as saying 29,000 and Security sources 80,000. The BBC reported an estimate of 50,000, calling it the largest protest since the fall of the Soviet Union.

[3] Internet World Stats (2013a) *Internet Users in Europe.* http://www.internetworldstats.com/stats4.htm. Data collected from Nielsen Online, ITU, Facebook, GfK and "other reliable sources".

[4] ibid

[5] ibid

[6] Ignite Social Media (2012) http://www.ignitesocialmedia.com/social-media -stats/2012-social-network-analysis-report/.

[7] Levada Analytical Centre (2012) *Russian Public Opinion 2010–2011.* http://en.d7154.agava.net/sites/en.d7154.agava.net/files/Levada2011Eng.pdf.

(to date) numbers of protestors in a fashion reminiscent of the show trials of the soviet era. The recent conviction and then unexpected release on bail of opposition leader Alexei Navalny is only the most high profile case. Other well-known names against whom cases have been brought include Sergei Udaltsov and Leonid Razvozzhaev. A case more calculated to scare ordinary people into silence, however, is the Bolotnaya trial, brought in June 2013 against twelve ordinary protestors for their part in the May 2012 Bolotnaya Square protests. Legislation has also been pushed through the Duma that effectively criminalises protest.

The state has reverted to other methods familiar from soviet times, salami tactics to divide the different parts of society in an attempt to isolate and neutralise the opposition. These latter methods so far seem to have real potential for success. With the digital divide, and protests largely restricted to western Russia and its big metropolises, Putin has gone on the offensive, characterising opposing voices as belonging to an ungrateful middle class, hypocritical in their protest against their privileged lifestyle itself paid for by the conscientious working classes and by a government against whose policies they now protest.

The response to online protest has been more complex. Authoritarian states have largely elected until now to try and limit the penetration of external actors into their own states, including shutting down access to the internet at key moments in an attempt to close regions or even the entire country to outside communications.[8] Citizens of certain states are, however, more vulnerable than others to their state being able to "pull the plug" on their online activities. Most cited as a key factor here is the number of internet providers, and mechanisms for connecting to the outside. However, a far more important consideration in assessing the capacity of any state to adopt a wholesale closure of the internet is the number, diversity and security of physical paths.[9] In fact, Russia looks fairly resilient on both counts, which may explain the relatively sophisticated strategies that the state has undertaken to date to control internet usage. Rather than the heavy repression undertaken by its neighbour, China, it has opted largely for "second- and third-generation techniques such as legal and technical instruments and national information campaigns to shape the information environment and stifle dissent and opposition".[10] The latter have extended to somewhat mischievous tactics being employed: for instance, Navalny was in early 2012 a victim of a fake interview with Voice of America, during which he was quoted as making derogatory comments about opposition activists. Speculation has been rife that this was a state-sponsored fake, engineered by the FSB.

The internet can therefore be as effective a tool for the incumbent administration as for opposition activists. But it is not only the internet, more traditional forms of communication are also susceptible to attack. Open Democracy has speculated widely that the FSB and other pro-Kremlin groups have intercepted telephone calls and made illicit recordings of anyone suspected of being unfriendly to the Kremlin. Indeed, SORM (System for Operative Investigative Activities) gives a number of intelligence and law enforcements agencies in Russia a right to intercept information. Experiences include the tapping of Gennady Gudkov's, Deputy Chair of the Duma's Security Committee, telephone; Boris Nemtsov, transcripts of whose private conversations have appeared online; as well as those of diplomats from the UK and USA, the UK's Deputy Consul General in Ekaterinburg being forced to resign after footage of him with prostitutes was made public. It has been widely speculated that the FSB was responsible for the filming and circulation of such footage.

Concluding Remarks

The benefits of the internet and social media for social movements are clear and largely unarguable. They provide a platform for dissemination of information, for organising offline protests and can be used to build a sense of shared identity, the latter extremely important in divided societies. Social media and the internet play a vital role also in publicising any state activities that breach internationally agreed principles of what constitutes appropriate state behaviour. Coupled with offline activities, online activism can be an important step in the road to achieving desirable change, even transformation.

But major problems exist for those seeking to bring about change in Russia. Most effective, perhaps, is the fear generated by the state clampdown on street protest and protestors, which deters dissenters from publicly showing their dissatisfaction. The appearance of only small numbers of protestors in turn legitimates state discourse which argues the vast majority of the population is content with the status quo. Even where more orthodox routes to change are followed by individuals, the state moves quickly to make an example of them, the case for the popular Mayor of Yaroslavl, Yevgeny Urlashov, who in July 2013 was arrested on corruption

[8] China 2009, Iran 2009 and 2012, Syria 2012 and 2013, to name but a few.

[9] Richard Chirgwin (2012) Internet shut-down easier than you think in some countries *The Register* http://www.theregister.co.uk/2012/12/04/kill_switch_analysis_renesys/.

[10] OpenNet Initiative (2010) *Russia* https://opennet.net/research/profiles/russia.

charges. Such arrests cannot fail to have their effect on ordinary people, forcing them to question their own vulnerability to arrest if even prominent activists and politicians are not immune. The second problem is one of disinterest. So far, the opposition has remained largely confined to the middle classes and there has been a failure to unite the majority of Russians behind a single cause. The digital divide (with little prospect for bridging this in the short term), coupled with a continued reliance on state-monopolised media for news means the galvanising benefits of social media are not felt nearly widely enough. Thus, fear, apathy and disinterest combine to work against the opposition's reforming agenda.

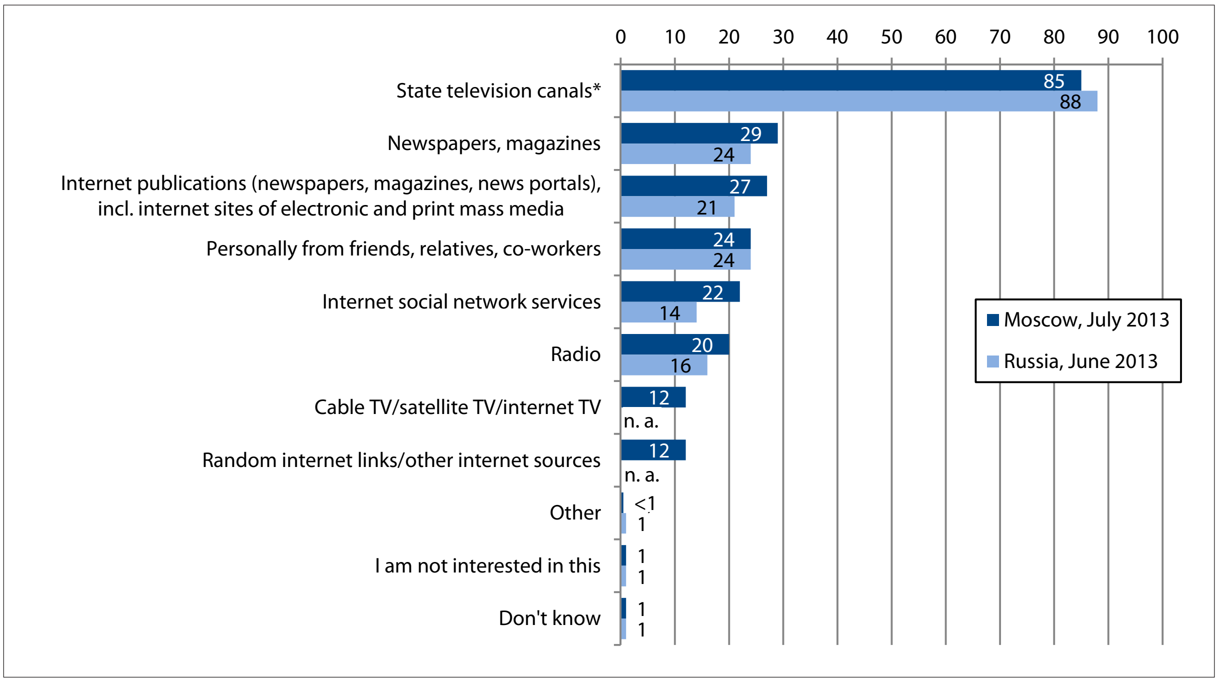
For reform-minded Russians, therefore, offline activism might not be the immediate answer. To date, the larger street protests have been successful in raising awareness externally of Russia's domestic problems. But they have also provided an opportunity for the Russian state to send a message about what happens to those who dare to protest openly. It is far less clear that the same tactics will work with online activism. Certainly, a range of remedies is available to the Russian authorities and they are using some of these. However, a sustained attempt to restrict services internally is particularly difficult, except for the big market leaders, which explains the 'accidental' Kremlin blocking of VK recently. But otherwise, monitoring and reacting to an increasing number of websites and other online sources will require the state to direct a good deal of its resources that way for a sustained period of time. In any case, in imposing restrictions, Russia leaves itself open to a good deal of attention and criticism from domestic and foreign critics. That it is sensitive to this issue is demonstrated by the rhetoric of justification employed, essentially a discourse of securitisation, which points to the need to provide a secure online environment to protect vulnerable groups in society and to counter terrorist and extremist threat. Apart from the threat to its legitimacy that such criticism brings, the government runs the risk of alienating the kind of market entrepreneurs that the country needs and which it has begun to attract. After the Navalny verdict, for instance, the Russian stock market suffered major losses. While such dips are often short-term, any pattern of losses inevitably affects the attitudes of investors and the market. Online activism may therefore continue to be the best tool available to reformers in Russia.

About the author

Dr Maxine David is Lecturer in European Politics at the University of Surrey. She is a foreign policy analyst with particular expertise in Russian, EU and UK external relations. Her most recent publication (co-edited with Jackie Gower and Hiski Haukkala) is *National Perspectives on Russia. European Foreign Policy in the Making?*, published in 2013 with Routledge.

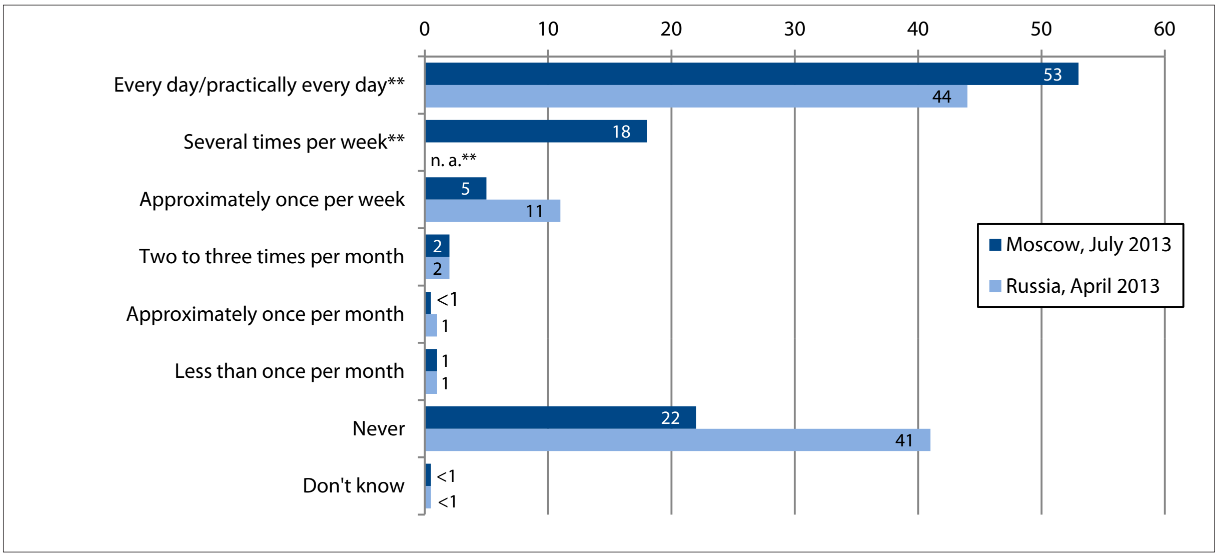
Internet Use And Attitudes Towards Illegal Downloading

Figure 1: What Are Your Sources for News in the City, Country, And the World? (%, several answers possible)



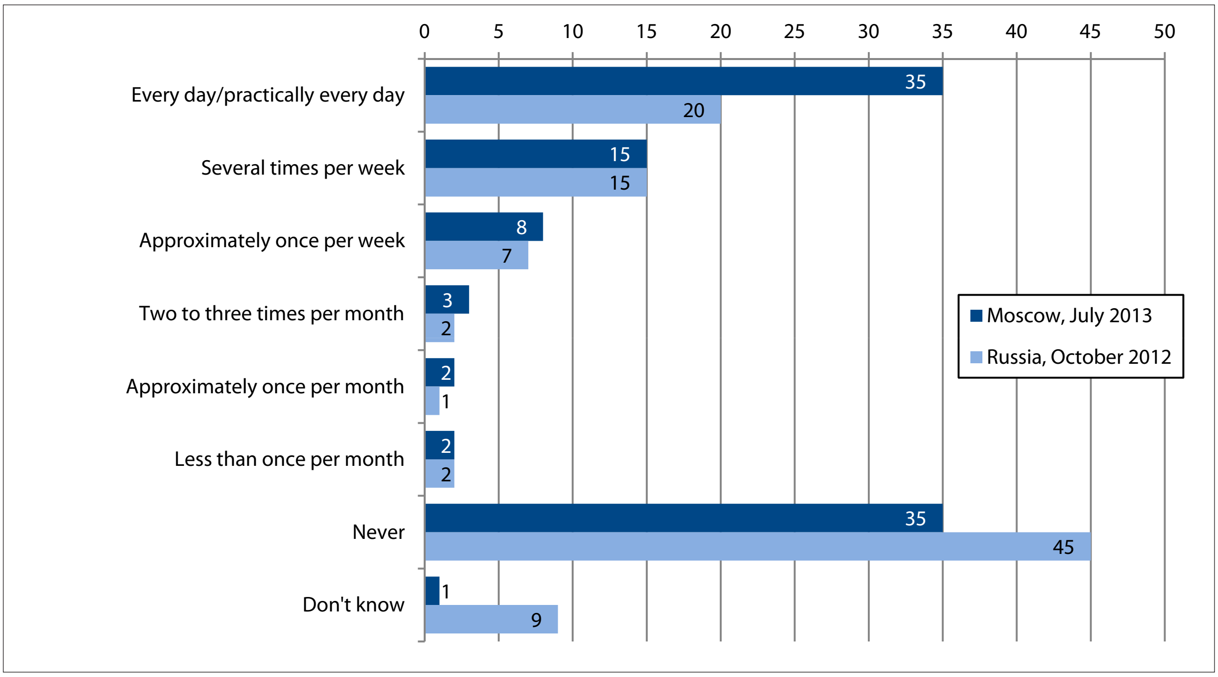
** In the June 2013 poll for all of Russia, this answer was "television" instead of "state television canals"*
Source: representative polls by Levada Center in Moscow and Russia 4–8 July 2013 and in June 2013, respectively, published on 15 July 2013 on http://www.levada.ru/15-07-2013/istochniki-informatsii-moskvichei

Figure 2: Do You Use the Internet, And If Yes, How Often?* (%)



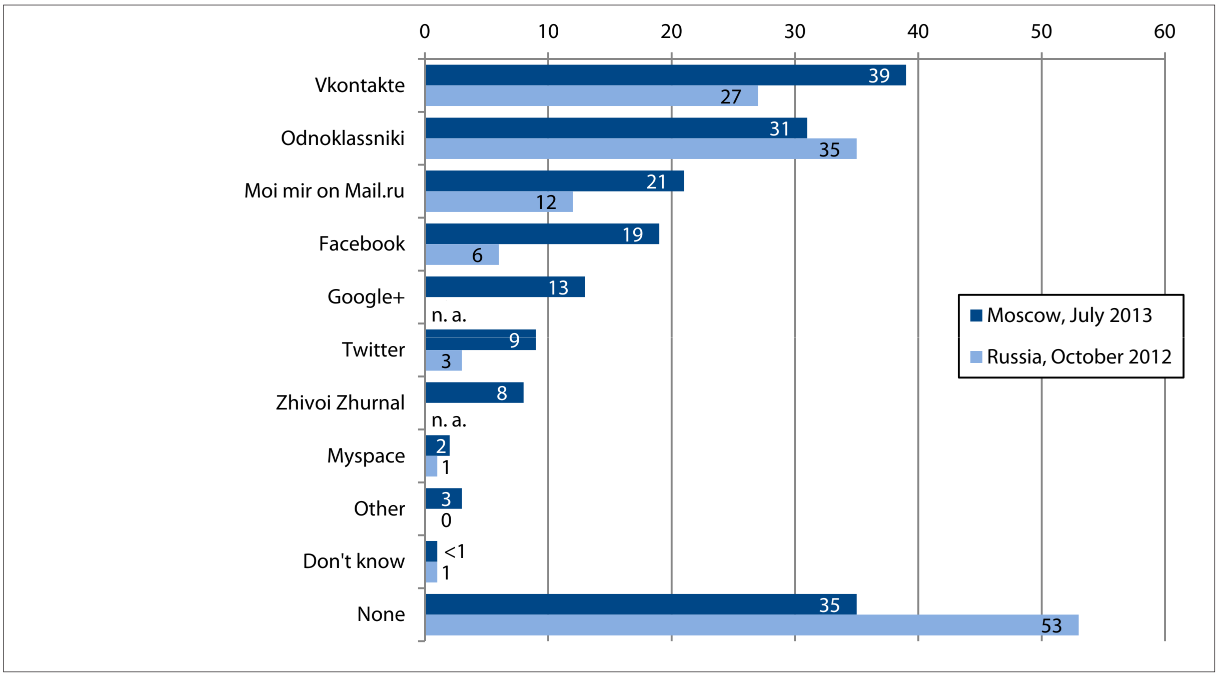
** *This question was formulated as follows in the April 2013 Russia poll: "Do you use the internet (apart from e-mail), and if yes, how often?"*
*** In the April 2013 Russia poll, the answers "every day/practically every day" and "several times per week" were combined into one answer*
Source: representative polls by Levada Center in Moscow and Russia 4–8 July 2013 and in April 2013, respectively, published on 15 July 2013 on http://www.levada.ru/15-07-2013/istochniki-informatsii-moskvichei

Figure 3: Do You Visit "Social Network Services" on the Internet? If Yes, How Often? (%)



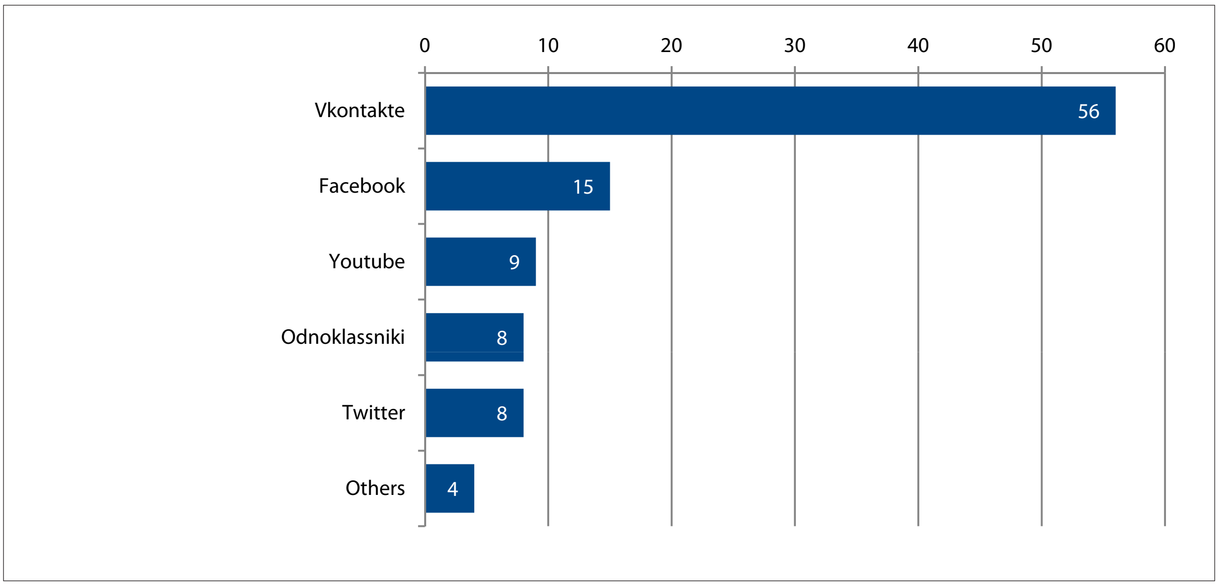
Source: representative polls by Levada Center in Moscow and Russia 4–8 July 2013 and in October 2012, respectively, published on 15 July 2013 on http://www.levada.ru/15-07-2013/istochniki-informatsii-moskvichei

Figure 4: Which "Social Network Services" Do You Visit? (%)



Source: representative polls by Levada Center in Moscow and Russia 4–8 July 2013 and in October 2012, respectively, published on 15 July 2013 on http://www.levada.ru/15-07-2013/istochniki-informatsii-moskvichei

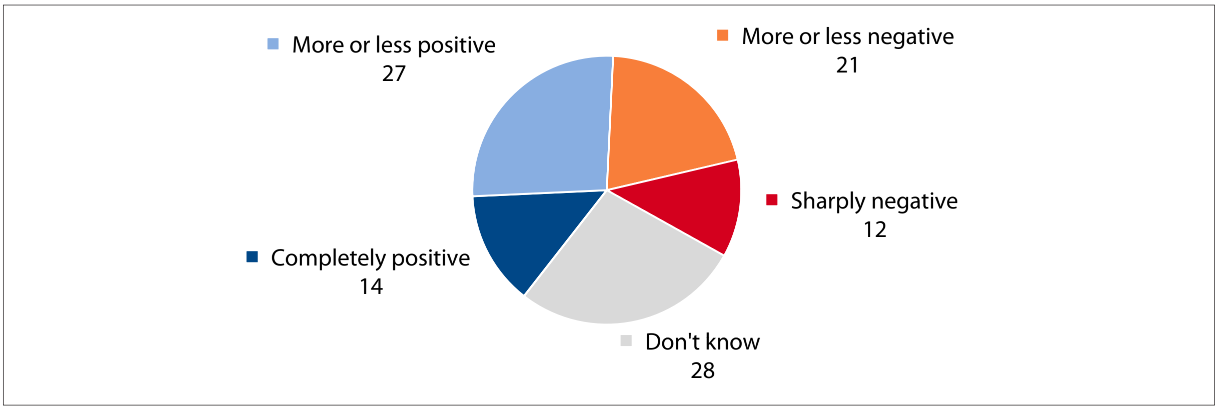
Figure 5: Distribution of Actual Visits to Social Media Sites (June 2012–June 2013) (%)



Note: Whereas the public opinion poll documented above shows how many people use specific social media at all, the statistics used for this figure measure how often specific sites have actually been visited. That means the opinion poll counts users (independently of how often they visit the respective site), while the statistics count visits (many of which may come from the same person).

Source: data taken from http://gs.statcounter.com/#social_media-RU-monthly-201206-201306-bar. *Statistics for Russia are based on coverage of more than one hundred million page views per month, see* http://gs.statcounter.com/sample-size/StatCounterGlobalStatsAug12_SampleSizeCountry-Breakdown.csv

Figure 6: What Is Your Attitude Towards the Law Penalizing Illegal Downloading of Copyrighted Materials: Films, Books, And Music? (%)



Source: representative polls by Levada Center 23–27 May 2013, published on 18 June 2013 on http://www.levada.ru./18-06-2013/otnoshenie-k-zakonu-o-zashchite-avtorskikh-prav

ABOUT THE RUSSIAN ANALYTICAL DIGEST

The Russian Analytical Digest is a bi-weekly internet publication jointly produced by the Research Centre for East European Studies [Forschungsstelle Osteuropa] at the University of Bremen (www.forschungsstelle.uni-bremen.de), the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology Zurich (ETH Zurich), the Resource Security Institute, the Institute of History at the University of Zurich (http://www.hist.uzh.ch/) and the Institute for European, Russian and Eurasian Studies at The George Washington University. It is supported by the German Association for East European Studies (DGO). The Digest draws on contributions to the German-language Russland-Analysen (www.laender-analysen.de/russland), the CSS analytical network on Russia and Eurasia (www.css.ethz.ch/rad), and the Russian Regional Report. The Russian Analytical Digest covers political, economic, and social developments in Russia and its regions, and looks at Russia's role in international relations.

To subscribe or unsubscribe to the Russian Analytical Digest, please visit our web page at www.css.ethz.ch/rad

Research Centre for East European Studies at the University of Bremen
Founded in 1982, the Research Centre for East European Studies (Forschungsstelle Osteuropa) at the University of Bremen is dedicated to the interdisciplinary analysis of socialist and post-socialist developments in the countries of Central and Eastern Europe. The major focus is on the role of dissent, opposition and civil society in their historic, political, sociological and cultural dimensions.
With a unique archive on dissident culture under socialism and with an extensive collection of publications on Central and Eastern Europe, the Research Centre regularly hosts visiting scholars from all over the world.
One of the core missions of the institute is the dissemination of academic knowledge to the interested public. This includes regular e-mail newsletters covering current developments in Central and Eastern Europe.

The Center for Security Studies (CSS) at ETH Zurich
The Center for Security Studies (CSS) at ETH Zurich is a Swiss academic center of competence that specializes in research, teaching, and information services in the fields of international and Swiss security studies. The CSS also acts as a consultant to various political bodies and the general public. The CSS is engaged in research projects with a number of Swiss and international partners. The Center's research focus is on new risks, European and transatlantic security, strategy and doctrine, area studies, state failure and state building, and Swiss foreign and security policy.
In its teaching capacity, the CSS contributes to the ETH Zurich-based Bachelor of Arts (BA) in public policy degree course for prospective professional military officers in the Swiss army and the ETH and University of Zurich-based MA program in Comparative and International Studies (MACIS); offers and develops specialized courses and study programs to all ETH Zurich and University of Zurich students; and has the lead in the Executive Masters degree program in Security Policy and Crisis Management (MAS ETH SPCM), which is offered by ETH Zurich. The program is tailored to the needs of experienced senior executives and managers from the private and public sectors, the policy community, and the armed forces.
The CSS runs the International Relations and Security Network (ISN), and in cooperation with partner institutes manages the Crisis and Risk Network (CRN), the Parallel History Project on Cooperative Security (PHP), the Swiss Foreign and Security Policy Network (SSN), and the Russian and Eurasian Security (RES) Network.

The Institute for European, Russian and Eurasian Studies, The Elliott School of International Affairs, The George Washington University
The Institute for European, Russian and Eurasian Studies is home to a Master's program in European and Eurasian Studies, faculty members from political science, history, economics, sociology, anthropology, language and literature, and other fields, visiting scholars from around the world, research associates, graduate student fellows, and a rich assortment of brown bag lunches, seminars, public lectures, and conferences.

The Institute of History at the University of Zurich
The University of Zurich, founded in 1833, is one of the leading research universities in Europe and offers the widest range of study courses in Switzerland. With some 24,000 students and 1,900 graduates every year, Zurich is also Switzerland's largest university. Within the Faculty of Arts, the Institute of History consists of currently 17 professors and employs around a 100 researchers, teaching assistants and administrative staff. Research and teaching relate to the period from late antiquity to contemporary history. The Institute offers its 2,600 students a Bachelor's and Master's Degree in general history and various specialized subjects, including a comprehensive Master's Program in Eastern European History. Since 2009, the Institute also offers a structured PhD-program. For further information, visit at http://www.hist.uzh.ch/

Resource Security Institute
The Resource Security Institute (RSI) is a non-profit organization devoted to improving understanding about global energy security, particularly as it relates to Eurasia. We do this through collaborating on the publication of electronic newsletters, articles, books and public presentations.

Any opinions expressed in Russian Analytical Digest are exclusively those of the authors.
Reprint possible with permission by the editors.

Editors: Stephen Aris, Matthias Neumann, Robert Orttung, Jeronim Perović, Heiko Pleines, Hans-Henning Schröder,, Aglaya Snetkov
Layout: Cengiz Kibaroglu, Matthias Neumann, Michael Clemens
ISSN 1863-0421 © 2013 by Forschungsstelle Osteuropa, Bremen and Center for Security Studies, Zürich
Research Centre for East European Studies • Publications Department • Klagenfurter Str. 3 • 28359 Bremen •Germany
Phone: +49 421-218-69600 • Telefax: +49 421-218-69607 • e-mail: fsopr@uni-bremen.de • Internet: www.css.ethz.ch/rad