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The earlier perception that online media were far less significant than television and print is no longer valid.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.