The occupation of Runet? The tightening state regulation of the Russian-language section of the Internet

Language-revised version, 19 October 2018

Markku Lonkila, Larisa Shpakovskaya & Philip Torchinsky

Abstract

In this article we scrutinise the Russian state's regulation for political purposes of the Russian-language section of the Internet or "Runet", as it is often dubbed in Russia). We will focus on those regulative actions which came into force during and after the opposition protest wave in Russia 2011–2013. Internet and social media played an important role in the mobilising of these protests that challenged the legitimacy of the ruling elite. We argue that the protests marked a watershed in the Russian government's information policy, which had previously mainly functioned through the control of the federal Russian TV channels. After the protests the Kremlin mounted a campaign to regulate the political use of Runet. This campaign was implemented through a wide variety of on- and offline actions, which we call the "occupation" of Runet. Instead of an isolated event, the occupation can be seen as part of the more general trend of restricting Russian civil society during the Putin-Medvedev tandem.

Keywords: Russia, protests, opposition, Internet, social media, censorship, regulation

1. Introduction: The Russian 2011–2013 protest wave as a watershed in Internet regulation

In this chapter we scrutinise the Russian state's regulation of the Russian-language section of the Internet and social media – often dubbed "Runet" by Russian Internet users – for political purposes.[i] We focus on the series of regulative actions whose development and implementation began during and after the anti-governmental protest wave in Russia 2011–2013. Internet and social media played an important role during the mobilisation and organisation of these protests that brought tens of thousands of frustrated Russians onto the streets of Moscow and other Russian cities for the first time since the 1990s, challenging the legitimacy of the Putin-Medvedev government.

The protests served as a wake-up call for the government concerning the ability of the Internet and social media to summon people for public rallies. Contrary to the established state control over traditional media, the Russian-language section of the Internet had remained relatively free until the protests, with the exception of the occasional exertion of pressure on individual Russian bloggers.[ii] The protests marked a clear turning point in the government's information policy, which had mainly been pursued through the control of federal TV channels while the Internet remained largely unregulated. The protest wave compelled the Kremlin to restrict the use of the Russian-language Internet and social media for anti-government debate and mobilisation, which we refer to here as the "occupation" of Runet.[iii]

A complete description of the events and legislative changes related to Internet regulation in Russia would exceed the scope of a single chapter. Instead, we present an overview of what we consider to be a co-ordinated attempt to gain tighter state control over the political uses of Runet. The adoption of regulatory measures accelerated rapidly after the opposition protests and in March 2013 Alexey Mitrofanov – the head of the parliamentary committee on information policy, technology and communications – warned that "the era of an absolutely free Internet in Russia has ended" (Milashina, 2013). His words are corroborated by Gainutdinov and Chikov (2013) in their report on threats to Internet freedom:

> 2012 was a watershed year for the Russian Internet. The Internet moved rapidly away from the margins of social and political life and demonstrated its extremely wide-ranging potential for use by Russian activists to organize themselves. In so doing, it also attracted the close attention of the authorities. For the first time, the Russian state has started to see the Internet as the principal threat to its prosperity and stability. (Gainutdinov and Chikov, 2013)

In their follow-up report in 2017 Gainutdinov and Chikov (2017: 19) stated even more sharply that the attitude of the Russian state towards the Internet had turned into a "military campaign" against the freedom of Runet.

This chapter is structured as follows. In the next section we will briefly describe some aspects of the political context of the occupation and define the notion of Runet regulation. In section three we will examine the years prior to the mass protests, which we call the period of "free" Runet. We argue that until 2012 there was a relatively weak legislative basis for Internet regulation and that the laws were enforced unsystematically. In the fourth section we analyse the years 2012–2014 or the "beginning of the occupation", which we consider to be one of the

most important turning points in the regulation of Runet. This period was chosen because the bulk of the legislation governing Runet monitoring and control was written during these two years: Numerous laws were passed, and their enforcement, as well as instances of other forms of regulation grew quickly indicating the Kremlin's changing attitude towards the Internet in response to the protest wave.

For both periods—the period of "free Runet" and the "beginning of the occupation"—we will first address legislation directly related to Internet regulation and thereafter legislation which is not directly related to Internet but which can and has been used for purposes of political control, such as the law on "extremist activities". We will in addition examine forms of regulation other than legislation that were created by the Russian state to gain control over Internet use.

In the fifth section, covering the expansion of the occupation, we address the most important regulation efforts put in place after 2014 with updates until the spring of 2018. In section six we discuss the success of the occupation and the users' resistance towards the regulation efforts. In the concluding section we present some reflections regarding future developments of Runet regulation.

2. The context and concept of Runet regulation

2.1. Political context of Internet regulation in Russia

The occupation of Runet is part of a more general move to restrict the leeway of Russian civil society under the Putin-Medvedev regime. Two features of the Russian political governance proposed by Vladimir Gel'man are relevant for understanding the context of the protests and subsequent occupation of Runet. First, "electoral authoritarianism" (cf. Gel'man, 2014) refers to the system by which the authoritarian ruling elite still holds elections to legitimise its power and to maintain its façade of a democratic system. Second, "half-freedom of speech" *(polusvoboda slova)* (Gel'man, 2010) denotes the way of controlling the Russian media landscape where the most important media, particularly nationwide TV, are kept under state control but some independent outlets (such as *Novaya Gazeta* or *Dozhd-TV*) are still allowed to function.

Most importantly, prior to the protests, Internet and social media were mostly free from state control, and the daily Internet audience had been growing exponentially from 3 million in

2003 to 32 million in 2011 (Internet v Rossii 2016). This enabled citizens dissatisfied with the Duma elections of autumn 2011 to disseminate images and videos of the blatant falsification of the election ballots in social media. They added to the mounting evidence of misconduct and corruption on the part of the authorities available on Runet for years before the protests. As a result, tens of thousands of protesters gathered on Bolotnaya Square in Moscow on 10 December 2011, marking the beginning of a protest wave which shocked the Kremlin, changing its view on the new digital media.

Another key moment in time is the revival of nationalist sentiment related to the annexation of Crimea in spring 2014, which boosted Putin's popularity and gave the ruling elite *carte blanche* to further regulate Runet. The new information security doctrine explicitly introduced this new approach in 2016 by stressing the need to control the Internet and develop domestic information technology (Pynnöniemi & Kari, 2016; Doctrine of information security of the Russian Federation, 2016).

2.2. The notion of regulation versus censorship

In this article we use the term "Internet regulation" instead of "censorship" since the latter often refers to mechanisms of state control for defensive and protective purposes. Censorship includes practices of screening and pre-emptive prevention of publications in print or broadcast media. By contrast, regulation is a wider and more flexible term describing more aptly the situation currently prevailing in Russia. For example, censorship does not cover either spying or proactive efforts in the form of pro-governmental blogging such as inundating the Runet with bots and organised trolling.

Internet regulation is a multifaceted and multilevel phenomenon. First, it may involve several actors ranging from international organisations to states, private corporations, institutions and individual citizens. In addition to human and social actors, the role of search engines and social media application algorithms is growing in importance. Second, Internet regulation may occur online (e.g. blocking websites) and offline (e.g. intimidating individual bloggers). Third, regulation can be defensive (e.g. censoring contents), pro-active (e.g. paid pro-government bloggers), or "neutral" (e.g. spying and monitoring traffic without taking action). Fourth, regulation may also be implemented covertly, when legislation passed ostensibly on other topics is *de facto* used to regulate the Internet (e.g., combatting child pornography or extremism). Finally, important preparatory steps towards Internet regulation include the

acquisition of shares in the relevant Internet companies in preparation for tightening the control in the future—just in case (Pallin, 2017).

In what follows we will focus our attention on a wide variety of measures, both legal and non-legal as well as on- and offline, taken by the Russian state to gain more control over the use of the Internet by civil society actors. Due to our wide focus and the wealth of events we have to be selective in order to pinpoint what we consider the milestones in a series of activities leading Russia towards an increasingly regulated Internet.

3. "Free Runet": Runet regulation before the protest wave

3.1. Internet-related legislation

Prior to the opposition protest wave Runet was relatively free: Users could share information and express political opinions without fear of legal consequences or harassment by the authorities, but gradually law enforcement agencies became interested in the functioning and political impact of Runet. The first regulation measures concerned legislation focused on content filtering and blocking in order to inhibit political extremism and terrorism (see also Sivetc's chapter in this volume).

The legal and technical bases for Internet regulation in Russia originated in the 1990's through the System for Operative Investigative Activities (*Sistema Operativno-Rozysknykh Meropriyatii,* SORM) legislation. Its first implementation (SORM-1) in 1995 required telecommunication operators to install hardware provided by the FSB (*Federal'naya Sluzhba Bezopasnosti*) to monitor phone, mail and web browsing communications metadata. While SORM-1 was about giving the FSB access to log files (metadata) and records of phone calls, the implementation of SORM-2 in 1999 gave the FSB online access to data transmission in real time and direct access to Internet service provider hardware.

SORM-2 required the FSB to get a court warrant to access user data, but soon after Putin's taking office the number of agencies entitled to access collected data was increased. Moreover, surveillance could start before the warrant was issued or even requested; there was no need to show the warrant to anyone, and the warrant was not needed for retrieval of metadata (Maréchal, 2017).

In 2012 SORM was extended to include social media platforms and in 2014 an updated version made use of deep packet inspection (DPI) technology. This technology enables the provider not only to monitor the traffic but also to identify in the data stream users who discuss certain topics or visit certain websites or social media. This implementation brought the Russian system much closer to the idea of mass surveillance (Soldatov, 2015: 75).

The Ministry for Communication, or *Minkomsviaz*, is the highest state institution responsible for the development and regulation of the Internet. Subordinated to *Minkomsviaz*, the Federal Service for Supervision of Telecommunications, Information Technology and Mass Communication, or *Roskomnadzor* (*Federal'nya sluzhba po nadzory v sfere svyazi, informatsionnykh tekhnologii I massovykh kommunikatsii*), is responsible for the monitoring of the Internet, licensing Internet providers and registering Internet media. It also has, in addition to the courts, the authority to decide whether a certain website will be blocked. (Franke & Pallin, 2012: 54; Kelly et al. 2013: 592)

According to Franke and Pallin (2012: 55) one of the most important laws used for Internet regulation prior to 2012 was the law "On counteracting extremist activities".[iv] Amendments introduced in 2006[v] extended the notion of extremism to include, among other things, the creation and distribution of extremist material intended for public use.

In the opinion of Alexander Verkhovsky of the SOVA Centre, the problem with the Russian legislation on extremism lies in its vague language – e.g., "inciting social discord" – which leaves ample room for interpretation. As a solution, the courts and prosecutors have turned to a roster of experts to judge which writings should be banned as extremism. (Dresen, 2013)

Some of the proposals presented to regulate the Internet failed, only to resurface years later following the protest wave. In February 2008, for example, a member of the Federation Council, Vladimir Slutsker, proposed that Internet sites with more than 1000 visits a day should be required by law to register as media outlets—an initiative which in a modified form was six years later enacted as the so-called "blogger's law". Similarly, in October 2008 the president of the Russoft Association proposed the creation of a gateway between Runet and the global Internet after the Chinese model—a proposal that was forgotten until in spring 2014 the newspaper *Kommersant* leaked information about plans in the state administration to implement a Chinese-inspired firewall in Russia (Novyi et al., 2014).

Since 2014, plans to gain total control over the Runet by cutting it off from the global Internet have surfaced at times (Golitsyna & Prokopenko 2016; Ristolainen 2017), but have not so far been implemented. In 2015 experiments were already conducted to test the model for Runet isolation and in March 2018 German Klimenko, advisor to Putin on questions concerning the Internet, announced that the country was technically ready for this (Dushnov, 2018).

3.2. Other regulative measures

Between 2008 and 2010 the human rights association Agora identified 43 cases of harassment and prosecution as threats to freedom of expression on the Internet. They included two murders, three physical assaults, 19 criminal prosecutions and 19 lawsuits. Of the murders, only the killing of Magomed Evloev, the owner of the website ingushetiya.ru while in police custody in 2008 resulted in a legal prosecution and sentence. (Gainutdinov & Chikov, 2013). Of the violent assaults, probably the best known is the brutal beating of Oleg Kashin, the *Kommersant* journalist in 2010, the motive of which was linked by some observers to Kashin's personal blog. In addition, Agora reported five cautions from the prosecutor's office and the federal oversight agency *Roskomnadzor*, eight instances of restricted access to the Internet or particular websites, two cyberattacks and five threats related to users' Internet activity (Gainutdinov & Chikov, 2011).

The first criminal charge against an Internet blogger in Russia was the case of the LiveJournal blogger Savva Terentyev in 2008. The case was also one of first occasions for the triggering of Article 282 of the Russian criminal code against "the incitement of hatred or hostility [...] on the basis of sex, race, nationality, language, ethnicity, religion, or reference to a social group."[vi] In the Terentyev case, a prosecutor called policemen a "social group", a questionable and ill-defined term which has subsequently facilitated the prosecution of a wide range of cases (Maza, 2018).[vii]

Although the cases listed above had serious, and in some cases fatal consequences, they were unsystematic and relatively few in number. With the exception of murders, the future occupation of the Runet evoked by the protest wave multiplied the number of all forms of restrictions.

As with traditional media, the Kremlin has also taken decisive steps to obtain ownership in the pivotal Internet-related enterprises (cf. Pallin, 2017). The important actors include, among others, a Kremlin-friendly businessman Alexander Mamut, who obtained full ownership of the company SUP Media after having acquired 50% of the shares from the oligarch Alisher

Usmanov in 2012. In 2007 SUP Media had bought the Russian-language section of LiveJournal and in 2008 it took full control of the site gazeta.ru. In March 2013 Mamut and Vladimir Potanin agreed to merge SUP Media with Afisha-Rambler, creating the fourth largest group of Russian Internet businesses in terms of user base. The most popular Russian social networking site VKontakte came under the control of Usmanov when its founder, Pavel Durov, was forced to emigrate from Russia in 2014 (Pallin, 2017).

These incidents during the period of "free Runet", however, were only a prelude. The protests evoked a proliferation and enlargement of the scale of regulative measures by the authorities, which we dub the "occupation of Runet".

4. The Beginning of the occupation of Runet in 2012–2014

In this section we describe the Runet regulation measures from the beginning of 2012 until the end of 2014. We will start by scrutinising the Internet-related legislation and then move on to address the legislation which is not directly related to Internet control but can nevertheless be used to limit the freedom of expression such as the laws combating "extremism" and "terrorism".[viii] Finally, we will examine other than legal forms of Runet regulation.

4.1. Internet-related legislation

The Agora Human Rights Association has monitored the freedom of the Russian Internet since 2008. Table 1, based on Agora's reports, reveals an abrupt and sudden increase in most forms of Runet regulation in 2011 coinciding with the beginning of the protest wave.

INSERT TABLE 1 HERE

Table 1 indicates a steep growth in proposals and legislative initiatives designed to regulate the Internet from five in 2011 to 49 in 2012. This growth continued, with the exception of 2015, until 2017.

One of the best known laws regulating Runet at this time is generally known as the "Internet blacklist law" of 2012, which includes, among other things, the creation of a register of websites distributing illicit information, including child pornography, production and distribution of drugs, and information encouraging suicide.[ix] The vague notion of prohibited information, however, enlarges the area of application. Access to such a site can be blocked by

an authorised state organ without a court order. If the Internet provider removes the harmful content within three days, the access to the site will be unblocked (see Sivetc's chapter in this volume on the blacklisting procedure).

This legislation enabled the blocking of access to opposition websites. Due to the request by the Attorney General of the Russian Federation, for example, the popular sites www.grani.ru, www.kasparov.ru and www.ej.ru, all of which expressed views critical of the government, were added to the blacklist in March 2014 because they "contained incitements to illegal activities and participation in mass action conducted without respect for the established order". In a similar manner, the LiveJournal blog of the prominent Russian opposition leader Alexey Navalny (http://navalny.livejournal.com) was added to the blacklist, and Navalny himself was placed under house arrest by a Moscow court.

The Internet blacklist law of 2012 was followed in December 2013 by the "Lugovoi law"[x], which entered into force during the Euro-Maidan protests. The law authorised the Russian Prosecutor General and his deputies to issue emergency orders without a court order to block websites inciting to unauthorised protests or "promoting extremism".

In addition, the "anti-piracy law" lists a range of information intermediaries (e.g., telecom operators, hosting providers or web-site owners) who may be found responsible for the reproduction, use and distribution of illegal content on the Internet. According to critics, the law allowed lawsuits to be initiated against almost any websites, opening the doors to unfair harassment. (Eremenko, 2013). [xi]

As of 2014, proposals for additional legal measures to control the Internet began to emerge in the public debate fuelled by Putin's speech of April 2014, in which he referred to the Internet as a special project of the CIA and as a danger to national security (Agamalova & Golitsyna, 2014). Putin's comment reflected the view of Russia as a fortress besieged by outsiders and increased the stress laid on the political use of the Internet.

During 2014 a number of amendments to the existing legislation were passed which markedly increased the possibilities for extending political control over Runet. In particular, the "bloggers law"[xii] obligated blog owners to register with *Roskomnadzor* public websites (among them pages on social networking sites, blogs and online forums) with more than 3,000 daily visitors. This obligation was removed in 2017 by a law which, however, imposed on bloggers the same responsibilities and legal constraints as on the mass media without providing the

same protection (Human Rights Watch, 2017)[xiii]. These sites are considered mass media and the owners are held responsible for the accuracy of the information published on them. Hosting providers are obligated to store the bloggers' personal data on Russian territory for six months.

Four further laws passed between May and July 2014 are relevant for our argument of the "occupation of Runet" as they all increase the power of the government to control Runet. First, the "law against money laundering"[xiv] increased the regulation of electronic payments within the Russian Federation. Besides combatting money laundering, the law may be used against political opposition candidates' fundraising campaigns. The Prosecutor General's office claimed in 2013, for example, that Alexey Navalny's mayoral campaign might be financed from abroad – a claim which was widely interpreted as an effort to discredit Navalny.

Second, the "law prohibiting the distribution and financing of extremist activity, including on the Internet"[xv] augmented the criminal sanctions for financing extremist activity to up to three years' imprisonment.

Third, the "localisation law" requires the storage of personal data of Russian citizens in data centres in Russia, which further increases the Kremlin's chances to identify and control dissent[xvi]. The law led to conflict with big companies such as Twitter, Facebook, LinkedIn and Google, which were officially requested to move information about Russian users in the Russian Federation. By early 2018 most big western companies had complied with the law, with the notable exceptions of LinkedIn, which was banned in Russia in 2016, and Facebook, which was formally warned in April for its failure to comply (Newton and Summers, 2018; Cuthbertson, 2018).

Finally, the "law increasing fines for activities which endanger the territorial integrity of the Russian Federation"[xvii] was passed containing calls for incitement to such activities through mass media and Internet.

In addition to the abovementioned laws, numerous legal initiatives on Runet regulation were launched during the period 2012–2014. According to the newspaper *Kommersant*, for example, a plan was being prepared in spring 2014 by a working group in the presidential administration for the division of Russian Internet providers into local, regional and national. The networks of all three types of providers would be interconnected, but only those of the national providers would be allowed to connect to international networks. On all levels the

network contents would be filtered, and the placement of domain name system (DNS) servers with domain names .ru and .рф outside the Russian Federation would be prohibited. Moreover, the working committee on the initiative proposed to transfer the rights to allocate domain names .ru and .рф from the present coordinating centre to the state organs. (Novyi et al., 2014).

In sum, this avalanche of Internet-related laws adopted in the wake of the Russian opposition protest wave clearly indicates the Russian state's abrupt and strong willingness to regulate Runet for political purposes. True, many of the laws – e.g. those against piracy and money laundering – have justifiable grounds, but with the current state of Russian court practices and the vague formulations of laws (e.g., the definition of "extremist activity") many of these laws can, and indeed have been misused.[xviii]

4.2. Other legislation

In addition to the laws directly regulating the Internet, a great number of laws constraining civic freedoms were enacted in the Russian Federation between 2012 and 2014 with the intention to suppress the opposition protests. They are reviewed briefly here to show that the occupation of Runet was not an isolated campaign but a part of a more general and deliberate campaign launched against the Russian opposition after the mass protests.

Several laws enacted in summer 2012 were clearly drafted for this purpose. For instance, the law tightening the regulation of mass events[xix] increased the penalties for violation of the order during meetings and demonstrations. Although not directly related to the Internet, under the law the protest organisers may be fined if they disseminate information about the events, for example, through social networking sites without government approval. (Laws of Attrition, 2013)

In a similar vein, "the law re-establishing libel as a criminal offence"[xx] carrying fines or prison sentences of up to three years was passed in 2012. The law not only afforded an opportunity to sue one's political opponents for libel but also contains a special clause on libel against judges, prosecutors and law enforcement officials.

Still another example of the laws which at first glance appear have justified intentions but which nevertheless may restrict the leeway of the opposition is the law banning advertising alcohol on the Internet.[xxi] In fact, this law may work in favour of state-controlled traditional

media since advertising is the main source of revenue of the independent Internet (Kelly et al., 2013: 596).[xxii]

One of the laws with the most concrete impact on Russian civil society organisations is **"**the foreign agent law" of 2012.[xxiii] This law obliges those NGOs that receive grants from abroad and are engaged in political activities to register as "foreign agents". Such NGOs have to mark their publications with the label "foreign agent" and they are subjected to extensive reporting and auditing requirements. Refusal to comply with the law by the founders or leaders of such organisations is sanctioned by heavy fines or prison sentences. The law has complicated the work of such well-known organisations as the election monitoring organisation GOLOS, the independent polling agency Levada Center and it led to the dissolution of the Russian committee against torture in 2015. The law was complemented in fall 2012 with the **"**law imposing administrative obligations on NGOs and their officials for failing to register as foreign agents or for late reporting".[xxiv] (List of repressive laws, 2014).

This legislation trend continued through 2013 and 2014. Paragraph 148 of the "law protecting citizens' religious convictions and sentiments"[xxv] imposed sanctions on the public violation of religious beliefs. Breaking the law may be punished by a maximum fine of R300,000 or three years in prison. The public discussion of the law revolved not only around the harsh punishments but also around the vagueness of its formulation. The law does not, for example, define what comes under "religious feelings" and how their violation could be detected.

The "Russian anti-gay law"[xxvi] attained a lot of publicity, also outside Russia, due to the international interest focused on Russia on the eve of the Olympic Games. The law prohibits the distribution of "propaganda on non-traditional sexual relations" among minors. If the violation of the law is perpetrated through the mass media, the punishment will be more severe. The law was criticised for its inability to differentiate between propaganda, information dissemination and education, which serves to increase its range of applicability.[xxvii]

Other similar laws enacted in 2014 included "the law increasing penalties for extremist crimes"[xxviii]; "the law expanding the powers of FSB"[xxix]; and "the law obliging Russian citizens to to report to the Ministry of Internal Affairs on the obtaining of a residence permit or citizenship of another country".[xxx]

4.3. Other regulative actions

Table 1 reveals the strong growth of most forms of regulative acts concerning the Russian Internet between 2010 and 2011, corroborating further our argument of the co-occurring of the "occupation of Runet" with the start of the protest wave. According to the Agora report (Gaidutnikov & Chikov, 2013), in 2012 Russian Internet activists started to flee the country for the first time in significant numbers and many website owners began to choose foreign jurisdictions. Both media representatives and public opposition figures and regular users and activists were subjected to pressure and harassment.

Criminal cases against users were mostly based on accusations of "extremist" activities in the Internet and social networking sites but also on insulting officials and libel. Instances of administrative pressure presented in Table 1 were related to the imposition of administrative sanctions on users, website administrators and providers, and to the issuing of official cautions by the prosecutor's office or local branches of *Roskomnadzor*.[xxxi]

A well-known example of harassment of users during 2013 is the case of the journalist and blogger Sergey Reznik, who in his blogs and articles criticised local corruption in Rostov-on-Don. In November 2013 he was sentenced to 18 months in a labour camp for bribery and insulting a public official. Reznik was found guilty one month after being assaulted and badly beaten in the street. Even before he had served his first sentence a new case was brought against him in 2014. Russia's Human Rights Center Memorial considered Reznik a political prisoner. He was released from prison in 2016 and the following year was awarded the Andrey Sakharov prize "For freedom of thought" by the European Parliament.

Before and during the Sochi Winter Olympics in February 2014 the control over civil society, journalists and Runet use intensified. In November 2013 Prime Minister Medvedev signed a decree authorising data collection on phone calls and Internet contacts made by organisers, athletes and foreign journalists (Soldatov & Borogan, 2013).

During 2014 the harassment of Internet users and social media in Russia continued, including notably the pressure on the opposition leader and blogger Alexey Navalny, who in April 2014 was fined USD 8,400 for libelling a district councillor on Twitter (Freedom on the Net, 2014). In December Navalny, who had been under house arrest since February, got a suspended prison sentence of three and half years, while his brother Oleg was sentenced to three and a half years in prison in a trial which was generally considered a Soviet-style show.

In addition to these restrictive and reactive measures, e-mails leaked in 2012 and allegedly belonging to the leaders of the pro-Kremlin youth movement Nashi suggested that the movement had been engaging in proactive digital activities, such as paying commentators to post content, disseminating DDoS attacks, and hijacking blog ratings. (Freedom on the Net, 2013). Moreover, in 2013 an organised case of pro-government trolling was exposed and debated in the press. According to journalists, over 200 people worked around the clock in a four-storey building on Savushkina Street in St. Petersburg with instructions to disseminate pro-government views and discredit the opposition on social media platforms such as Livejournal and VKontakte (Garmazhapova, 2013; Ahonen, 2014; Butsenko, 2014). The operation of pro-government trolling and automatic bots has resulted in the polarisation and "pollution" of the political debate not only on Runet, but also on the global Internet, as the discussion concerning Russian influence in the U.S. elections has revealed.

5. "Occupation expands": Runet regulation since 2014

If prior to 2014 the most important actions of Russian authorities were related to the drafting and passing of legislation, the ensuing years of the "occupation" were characterised by the implementation and elaboration of these adopted laws, methods of website blocking and filtering and the expansion of the number of controlling authorities. While the number of proposals to regulate Internet diminished in 2015, there was an increase in criminal prosecutions and administrative pressure on bloggers, Internet service providers and site owners, in the restrictions on access and skyrocketing of the number of court orders prohibiting information. There was also a sudden increase in prison sentences with 18 people being sentenced to up to five years (see Table 1).

According to Gaidutninov and Chikov (2016) the authorities seem to have begun to understand the ineffectiveness of the blocking and filtering strategy and to have moved on to the selective punishment of users. This trend of charging and convicting internet activists continued throughout 2016, accompanied by a marked increase in all forms of Runet control. As in previous years, the bulk of the regulation was related to content filtering and blocking and to the prohibition of information (Gaidutninov & Chikov, 2016). In the legislation the most significant change in 2016 was the "Yarovaya Package", also known as the Yarovaya Law (see also Lehtisaari's chapter in this volume), named after State Duma deputy Irina Yarovaya.

The package consists of two federal antiterrorist laws[xxxii] and amends the existing legislation by the extension of the powers of law enforcement, increases the penalties for terrorist activity,

expands the concept of "terrorist activity" and introduces new requirements for mobile operators and Internet providers. The amendments allow the prosecution and punishment of Internet users for a wide variety of activities due to the vaguely defined notion of terrorist activity. They allow law enforcement authorities to access email messages and require mobile operators and Internet providers to store metadata on calls, SMS content and traffic activity for three years and to surrender it to the authorities upon request.

According to a senior Internet researcher at Human Rights Watch, the implementation of the law can take surveillance to a whole new level where "no digital communication would be safe from government snooping, no matter how innocuous or unrelated to terrorism." (Human Rights Watch, 2016). Due to the storm of criticism the implementation of the requirement to preserve the information during three years was postponed until 2023.

Furthermore, "the news aggregators' law" was passed in 2016 and entered into force in January 2017.[xxxiii] It holds Russian-language news aggregators with more than one million visitors a day responsible for the veracity of their news reports which do not come from media outlets registered in Russia. The law also stipulates that only Russian citizens or companies may own such news aggregators. The obvious aim of the law is to prevent the dissemination of views critical of the Kremlin.[xxxiv] As consequence, the large Russian news portal Yandex.news dropped news outlets not registered with *Roskomnadzor*, such as blogs and foreign media, among which is Meduza, a Latvian-based Russian-language opposition-minded news site. This selection of sources is likely to produce a biased view on social and political life in Russia.[xxxv]

Concerned about the ineffectiveness of website blocking by the government, the Duma in 2017 introduced a bill declaring illegal any technologies, such as VPN-services, that allow users to bypass the blocks.[xxxvi] Another bill accepted in 2017, reinforced the control over Runet users by requiring the teleoperators to identify their customers by connecting the SIM cards to identified users.[xxxvii] Both laws increase the authorities' chances of identifying individual Runet users, thereby curtailing the expression of anti-government opinions online.

In the same year *Roskomnadzor* began requiring instant messenger services in Russia to register as "information distributors" (*organizatory rasprostranenija informatsii*) – with the obvious purpose of monitoring the messenger traffic (Lihachov, 2017). The law regulating the duties of information distributors dates from 2006[xxxviii], but only in 2017 it was for the first time implemented on the popular messenger service Telegram. The authorities argue that Telegram should hand over the encryption key for the investigation and prevention of serious

crimes and violent extremism, whereas the company defended users' rights to privacy in communication.

After the company refused to share its encryption keys, a Moscow district court decided to block Telegram in April 2018 and Russian Internet service providers started to implement blocking. The founder and CEO of Telegram Pavel Durov, however, considered the court ruling unconstitutional and started to develop built-in features in the software to circumvent the ban.[xxxix] In its attempt to prevent access to Telegram, *Roskomnadzor* had for technical reasons to block millions of IP addresses not related to Telegram, thus disrupting Russian online businesses.

Alexey Navalny's use of YouTube channels and video to bypass state-controlled media[xl] and communicate directly to Russians turned the state's attention towards the video service. Navalny's videos accusing Prime Minister Medvedev, Deputy Prime Minister Sergei Prikhodko and the oligarchs Alisher Usmanov and Oleg Deripaska of corruption gained tens of millions of viewers in 2017 and 2018. They led to court judgements requiring Navalny to remove the videos, which he refused to do.

6. Did the occupation succeed?

Andrei Soldatov (2017, 43) concludes that despite the limitations of control technology, the Kremlin has achieved its key objective of reducing the free self-expression area in Runet. For example, the harassment of bloggers and the selective punishments have created uncertainty about what can be written in Runet. Currently publication, sharing or even "liking" messages which criticise the authorities in social networking services, has become risky. Violations of the law against the dissemination of prohibited information are often reported to Roskomnadzor by pro-government whistle-blowers supported by state agencies, such as Mediaguard (*Mediagvardia*) – a branch of the Young Guard of United Russia and the League of Safe Internet (*Liga bezopaznogo interneta*).

The increasing regulation efforts have also met with resistance from users. One example was the closure of rutracker.org file sharing site by court decision in 2015. The site continued to function after closure, however, since Internet activists published instructions for users on how to avoid blocking on the websites such as rutracker.org and OpenRunet.org. Similar resistance was organised to oppose the closing of virtual libraries and file storage sites by

promoting alternative methods of access such as Tor network or Telegram message service and opening mirror sites.

In another burst of collective action against Runet control, thousands of people participated in a protest against the Yarovaya Package in Moscow in August 2016, and by 22 April 2018 a petition against the package had gathered 631,192 signatures.[xli] In addition, the grassroots movement promoting international cryptographic methods has organised training sessions in Russia for journalists, human rights activists and NGO staff members and websites such as *Roskomsvoboda* advise on encrypting user data and communications and circumventing website blocking. (Ermoshina & Musiani, 2017).

In 2018, the founder and CEO of Telegram messaging service Pavel Durov initiated a nationwide demonstration encouraging Russians to fly paper aeroplanes from their windows on Sunday, 29 April at 7 p.m. Moscow time to protest the government ban on Telegram.[xlii] The following day thousands of protesters flooded the streets of Moscow to show their support.

As mentioned above, social media, and recently particularly YouTube, play an important role in Aleksei Navalny's political communication strategy.[xliii] The YouTube video "Don't call him Dimon" accusing Prime Minister Medvedev of corruption launched nationwide anti-corruption protests by 2017 and had gathered 27 million viewers by April 2018. Navalny seems to implement the "cute cat theory" of digital activism, according to which operating on well-liked social media platforms used mainly for purposes other than political is beneficial for activism since shutting down such platforms by the government may cause popular discontent. (Zuckerman, 2017).

Many liberal activists have migrated "virtually" in Navalny's footsteps from Russian applications to YouTube, Facebook and Twitter, some have moved physically from Russia and some have withdrawn from public online debates. Many have moved to using Telegram channels developed by VKontakte's founder Pavel Durov, of which the Russian-language liberal StalinGulag channel has more than 150,000 subscribers to date.

7. Conclusions: The future of the regulation of Runet

In this article we described how mass demonstrations by the Russian opposition in 2011–2013 forced the political elite to take the power of the Russian-language Internet and social media

seriously. We have shown, using numerous sources, how the various regulatory actions in Runet proliferated in the period 2012–2014 and transformed from relative freedom to an ongoing ”occupation”.

At the time of writing the Kremlin considers Runet to constitute a serious political threat. The 2016 information security doctrine sees Russia – analogously with offline events – as ”cyberfortress under siege”. Russia's dependence on the global Internet and information technology is perceived by the state as a risk, and the doctrine emphasizes the need to constantly monitor information threats. The formulations in the doctrine suggest that the regulation of Runet will continue in the future. (Pynnöniemi & Kari, 2016).[xliv]

The specific future forms of “Runet occupation” depend on Russia's economic, social and political development, the fate of authoritarian rule in Russia, and the decisions of the ruling elite, which are hard to predict. As long as the opposition poses no immediate danger, the government may refrain from abrupt and visible control measures. If the opposition gains support, regulatory efforts may be stepped up with the help of the existing legislation.

The future scope of regulatory measures may include compulsory registration of .ru websites, a simplified procedure for closing wesites, pressure on service providers, pressure on bloggers and selective arbitrary punishments, and ultimately the isolation of Runet from the global Internet (cf. Ristolainen 2017).

Political regulation of Runet is unlikely to be of great importance to average users, who mostly surf the web for other purposes. Nevertheless, the constraints on the freedom of expression in Runet already regulate not only politics but also, for example, the articulation of citizens’ religious and sexual views. With increasing surveillance and control these constraints cause an oppressive atmosphere in Russian civil society.

For a user with political interests, Runet and social media constitute both an opportunity and a threat. On the one hand, social media provide an instrument for the organisation of civil society, but on the other, they give the government unprecedented means of controlling citizens.

The heated discussion about Russia’s cyberoperations in the Internet from 2016 to 2018 through applications such as Facebook in order to influence, say, the U.S. elections, has ignored similar operations in the Russian Federation. Research is urgently needed to ascertain to what

extent the Kremlin is collecting data on average Russian social media users for political purposes, organising pro-government trolling and possibly influencing the operating principles and algorithms of VKontakte, Yandex or other popular Runet platforms.

REFERENCES

Agamalova, Anastasia & Golitsyna, Anastasia. 2014. Putin uveren, chto internet voznik kak spetsproekt TsRY. *Vedomosti,* 24 April.

Ahonen, Anneli. 2014. Pietarilaisessa talossa yli 200 ihmistä kehuu työkseen Putinia. *Helsingin Sanomat*, 17 November.

Alexandrov, Evgeny & Medvedev, Sergey. 2017. Russian Federation: Internet Anti-Piracy Enforcement In Russia. *Mondaq*, 11 July, http://www.mondaq.com/russianfederation/x/609282/Copyright/Internet+AntiPiracy+Enforcement+In+Russia

Butsenko, Anton. 2014. Trolli iz Ol'gino pereekhali v novyi chetyrekhetazhnyi ofis na Savushkina. *dp.ru*, 28 October, https://www.dp.ru/a/2014/10/27/Borotsja_s_omerzeniem_mo/

Cuthbertson, Anthony. 2017. Facebook could be banned in Russia over data law violations, regulator suggests. *Independent*, 18 April, https://www.independent.co.uk/life-style/gadgets-and-tech/news/russia-facebook-ban-data-laws-privacy-telegram-a8310436.html

Doctrine of Information Security of the Russian Federation, 2016. The Ministry of Foreign Affairs of the Russian Federation, https://bit.ly/2tVlJgX

Dresen, Joseph. 2013. *Anti-Extremism Policies in Russia and How they Work in Practice*. Kennan Institute, 14 January.

Dushnov, Denis. 2018. Rossiya podgotovilas' k otklyucheniyu o Interneta. *Forbes*, 7 March.

Eremenko, Alexey. 2013. Russia's Internet: Between Regulation and Censorship. *Sputnik international*, 5 July. https://sputniknews.com/analysis/20130705182078941-Russias-Internet-Between-Regulation-and-Censorship/

Ermoshina, Ksenia & Musiani, Francesca. 2017. Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era. *Media and Communication*, 5 (1): 42–53.

Freedom on the Net. Russia. 2011. Freedom House, https://freedomhouse.org/sites/default/files/inline_images/Russia_FOTN2011.pdf

Freedom on the Net. Russia. 2012. Freedom House, https://freedomhouse.org/sites/default/files/Russia%202012.pdf

Freedom on the Net. Russia. 2013. Freedom House, https://freedomhouse.org/report/freedom-net/2013/russia

Freedom on the Net. Russia. 2014. Freedom House, https://freedomhouse.org/report/freedom-net/2014/russia

Freedom on the Net. Russia. 2016. Freedom House, https://freedomhouse.org/report/freedom-net/2016/russia

Freedom on the Net. Russia. 2017. Freedom House, https://freedomhouse.org/report/freedom-net/2017/russia

Franke, Ulrik & Pallin, Carolina Vendil. 2012, *Russian Politics and the Internet in 2012*. Swedish Research Defence Agency FOI report FOI-R-3590-SE, December.

FZ-5, February 3.2.2014. O vnesenii izmenenii v ugolovnyi kodeks Rossiiskoi Federatsii i statyu 31 ugolovnogo-protsessualnogo kodeksa Rossiiskoi Federatsii, http://www.rg.ru/2014/02/04/extremizm-site-dok.html

FZ-65, 8.6.2012. O vnesenii izmenenii v kodeks Rossiiskoi Federatsii ob administrativnykh pravonarusheniyakh i federalnyi zakon 'O sobraniyakh, mitingakh, demonstratsiyakh, shestviyakh i piketirovaniyakh', http://www.rg.ru/2012/06/09/mitingi-dok.html

FZ-97, 5.5.2014. O vnesenii izmenenii v federalnyi zakon ’Ob informatsii, informatsionnykh tehnologiyakh i o zashite informatsii i otdelnye zakonodatelnye akty Rossiiskoi Federatsii po voprosam uporyadocheniya obmena informatsiei s ispolzovaniem informatsionno-telekommunikatsionnykh setei, http://www.rg.ru/2014/05/07/informtech-dok.html

FZ-110, 5.5. 2014. O vnesenii izmenenii v otdelnye zakonodatelnye akty Rossiiskoi Federatsii, http://www.rg.ru/2014/05/07/terrorizm-dok.html

FZ-114, 25.7.2002. O protivodejstvii ekstremistskoi deyaltelnosti, http://www.rg.ru/2002/07/30/extremizm-dok.html

FZ-121, 20.7.2012, O vnesenii izmenenii v otdelnye zakonodatelnye akty Rossiiskoi Federatsii v chasti regulirovaniya deyatelnosti nekommercheskikh organizatsii, vypolnyayushchikh funktsii inostrannogo agenta, http://www.rg.ru/2012/07/23/nko-dok.html

FZ-130, 5.5.2014. O vnesenii izmenenii v otdelnye zakonodatelnye akty Rossiiskoi Federatsii, http://www.rg.ru/2014/05/07/terror-dok.html

FZ-135, 29.6.2013, O vnesenii izmenenii v statyu 5 Federalnogo zakona ’O zashchite detei ot informatsii, prichinyayushchei vred ikh zdorovyu i razvitiyu’ i otdelnye zakonodatelnye akty Rossiiskoi Federatsii v tselyakh zashchity detei ot informatsii, propangandiruyushchei otritsanie traditsionnykh semeinykh tsennostei, http://www.rg.ru/2013/06/30/deti-site-dok.html

FZ-136, 29.6.2013. O vnesenii izmenenii v statyu 148 Ugolovnogo kodeksa Rossiiskoi Federatsii i otdelnye zakonodatelnye akty Rossiiskoi Federatsii v tselyakh protivodeistiviya oskorbleniyu religioznykh ubezhdenii i chuvstv grazhdan, http://www.rg.ru/2013/06/30/zashita-site-dok.html

FZ-139, 28.7.2012. O vnesenii izmenenii v Federalnyi zakon ’O zashchite detei ot informatsii, prichinyayushchei vred ikhzdorovyu i pazvitiyu’ i otdelnye zakonodatelnye akty Rossiiskoi Federatsii, https://rg.ru/2012/07/30/zakon-dok.html

FZ-141, 28.7.2012. O vnesenii izmenenii v Ugolovnyi kodeks Rossiiskoi Federatsii i otdelnye zakonodatelnye akty Rossiiskoi Federatsii, http://www.rg.ru/2012/08/01/kleveta-dok.html

FZ-142, 4.6.2014. O vnesenii izmenenii v stati 6 i 30 Federalnogo zakona ’O grazhdanstve Rossiiskoi Federatsii’ i otdelnye zakonodatelnye akty Rossiiskoi Federatsii, http://www.rg.ru/2014/06/06/grajdanstvo-dok.html

FZ-148, 27.7.2006. O vnesenii izmenenii v stati 1 i 15 Federalnogo zakona ’O protivodeistvii ekstremistkoi deyatel’nosti’, https://rg.ru/2006/07/29/ekstremizm-protivodejstvie-dok.html

FZ-149, 27.7.2006. Ob informatsii, informatsionnykh tehnologiyakh i o zashchite informatsii, https://rg.ru/2006/07/29/informacia-dok.html

FZ-179, 28.6.2014. O vnesenii izmenenii v otdelnye zakonodatelnye akty Rossiiskoi Federatsii, http://www.rg.ru/2014/07/03/izmenenia-dok.html

FZ-187, 2.7.2013. O vnesenii izmenenii v otdelnye zakonodatelnye akty Rossiiskoi Federatsii po voprosam zashchity intellektualnykh prav v informatsionno-telekommunikatsionnykh setyakh, https://rg.ru/2013/07/10/pravo-internet-dok.html

FZ-208, 23.6.2016. O vnesenii izmenenii v Federalnyi zakon Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii Kodeks Rossiiskoi Federatsii ob administrativnykh pravonarusheniyakh, https://rg.ru/2016/06/28/zashita-dok.html

FZ-242, 21.7.2014. O vnesenii izmenenii v otdelnye zakonodatelnye akty Rossiiskoi Federatsii v chasti utochneniya poryadka obrabotki personalnykh dannykh v informationno-telekommunikatsionnykh setyakh, http://www.rg.ru/2014/07/23/persdannye-dok.html

FZ-245, 29.7.2017. O vnesenii izmenenii v Federalnyi zakon ’O svyazi’, https://rg.ru/2017/08/04/svyaz-dok.html

FZ-274, 21.7.2014. O vnesenii izmenenii v statyu 280 Ugolovnogo kodeksa Rossiiskoi Federatsii, http://www.rg.ru/2014/07/25/uk-dok.html

FZ-276, 29.7. 2017. O vnesenii izmenenii v federalnyi zakon ‘Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii’, https://rg.ru/2017/07/30/fz276-site-dok.html,

FZ-374, 6.7.2016. O vnesenii izmenenii v federalnyi zakon ‘O protivodeistvii terrorizmu’ i otdelnye zakonodatelnye akty Rossiiskoi Federatsii v chasti ustanovleniya dopolnitelnyh mer protivodeistviya terrorizmu i obespecheniya obshchestvennoi bezopasnosti, https://rg.ru/2016/07/08/antiterror-dok.html

FZ-375, 6.7.2016. O vnesenii izmenenii v Ugolovnyi kodeks Rossiiskoi Federatsii i Ugolovnogo-protsessualnogo kodeksa Rossiiskoi Federatsii v chasti ustanovleniya dopolnitelnykh mer protivodeistviya terrorizmu i obespecheniya obshchestvennoi bezopasnosti, https://rg.ru/2016/07/11/uk375-dok.html

FZ-398, 28.10.2013. O vnesenii izmenenii v federalnyi zakon ’Ob informatsii, informatsionnykh tehnologiyakh i o zashite informatsii, http://www.rg.ru/2013/12/30/extrem-site-dok.html

Gainutdinov, Damir & Chikov, Pavel. 2011. Threats to Internet freedom in Russia 2008–2011. An independent survey. *The Agora Association*, http://agora.rightsinrussia.info/reports/june2011

Gainutdinov, Damir & Chikov, Pavel. 2013. Russia – a global threat to Internet freedom. The Agora Association, http://agora.rightsinrussia.info/archive/reports/global-threat

Gainutdinov Damir & Chikov, Pavel. 2016. Svoboda Interneta 2015: torzhestvo tsenzury. An independent survey. The Agora Association, https://bit.ly/1oGxYKA

Gainutdinov, Damir & Chikov, Pavel. 2017. Rossiia. Svoboda internet 2016: na voennom polozhenii. The Agora Association, https://meduza.io/static/0001/Agora_Report_2017_Internet.pdf

Gainutdinov, Damir & Chikov, Pavel. 2018. Svoboda interneta 2017: polzuchaya kriminalizatsiya. The Agora Association, https://meduza.io/static/0001/Agora_Internet_Freedom_2017_RU.pdf

Garmazhapova, Aleksandra. 2013. Gde zhivut trolli. Kak rabotayut internet-provokatory v Sankt-Peterburge i kto imi zapravlyaet. *Novaya Gazeta*, 9 September.

Gel’man, Vladimir. 2010. Lovushka polusvobody. *Slon.ru,* 9.3. http://slon.ru/russia/lovushka_polusvobody-310531.xhtml

Gel'man, Vladimir. 2014. The Rise and Decline of Electoral Authoritarianism in Russia. *Demokratizatsiya: The Journal of Post-Soviet Democratization* 22 (4): 503–521.

Golitsyna, Anastasia & Prokopenko, Aleksandra. 2016. Chinovniki khotkyat podchinit sebe ves' rossiiskii internet. *Vedomosti*, 27 May.

Human rights watch. 2016. Russia: 'Big Brother' Law Harms Security, Rights, 12 July. https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights

Human rights watch. 2017. Russia: New Legislation Attacks Internet Anonymity, 1 August. https://www.hrw.org/news/2017/08/01/russia-new-legislation-attacks-internet-anonymity

Internet v Rossii: dinamika proniknoveniya. 2016. *FOM.ru*, http://fom.ru/SMI-i-internet/13021.

Kelly, Sanja, Truong, Mai, Earp, Madeline, Reed, Laura, Shahbaz, Adrian & Greco-Stoner, Ashley eds. (2013). *Freedom on the Net 2013. A Global Assesment of Internet and Digital Media*. Freedom House. http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf

Knight, Kyle. 2018. Russia's 'Gay Propaganda' Censor Attacks Health Website. *Human Rights Watch*, 10 May. https://www.hrw.org/news/2018/05/10/russias-gay-propaganda-censor-attacks-health-website

Laws of attrition. Crackdown on Russia's Civil Society after Putin's Return to the Presidency. 2013. *Human Rights Watch*. http://www.hrw.org/sites/default/files/reports/russia0413_ForUpload_0.pdf

Lihachov, Nikita. 2017. Roskomnadzor zablokiroval sait Line posle otkaza messenzhera zaregistrirovatsya v Rossii. – *TRjournal* 2 May. https://tjournal.ru/43870-roskomnadzor-zablokiroval-sayt-line-posle-otkaza-messendzhera-zaregistrirovatsya-v-rossii

List of repressive laws adopted by the State Duma of the Russian Federation under Vladimir Putin's presidency. 2014. Foundation Inostrannyi Agent, http://euromaidanpress.com/wp-content/uploads/2014/10/1.10.-ZAKONY-eng.pdf

Maréchal, Natalie. 2017. Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. *Media and Communication* 5 (1): 29–41.

Maza, Cristina. 2018. Russian feminist blogger charged with inciting hatred against men could be jailed for 5 years. *Newsweek*, 2 October.

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

Newton, Matthew & Summers, Julia. 2018. Russian Data Localization Laws: Enriching "Security" & the Economy. Henry M. Jackson School of International Studies, University of Washington, https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy/

Novyi, Vladislav, Balashova, Anna, Skorobogatko, Denis & Rozhkov, Roman. 2014. Domen – i tochka. Rossiiskii segment interneta gotovlyat k polnomu kontrolyu. *Kommersant*, 29 April.

Pallin, Carolina Vendil. 2017. Internet control through ownership: the case of Russia. *Post-Soviet Affairs*. 33 (1): 16–33.

Popugaeva, Nina. 2018. Russia's first blogger convicted for extremism wins support from Court of Human Rights. *The Barents Observer*, 4 September.

Pynnöniemi, Katri. & Kari, Martti. 2016. Uusi informaatioturvallisuuden doktriini: Venäjä tehostaa piiritetyn kyberlinnakkeen vartiointia. *FIIA comment* 26/2016.

Ristolainen, Mari. 2017. Should 'RuNet 2020' be Taken Seriously? Contradictory Views About Cybersecurity Between Russia and the West. *Journal of Information Warfare*, 16 (4): 113–131.

Soldatov, Andrei, & Borogan, Irina. 2013. Surveillance at the Sochi Olympics 2014. *Agentura.ru*, October (without date), http://www.agentura.ru/english/projects/Project_ID/sochi/

Soldatov, Andrei. 2015. The Taming of the Internet. *Russian Politics and Law*, 53 (5–6): 63–83.

Zuckerman, Ethan. 2007. The connection between cute cats and web censorship.16 July. http://www.ethanzuckerman.com/blog/2007/07/16/the-connection-between-cute-cats-and-web-censorship/

[i] We use the nickname Runet to refer to 'the segment of the Internet where the Russian language and Cyrillic letters are used predominantly, and the domain addresses of which end in ".ru," or at times ".su"or "рф".' (cf. Franke and Pallin 2012; Pallin 2017). Runet is, however, more a cultural than a technical phenomenon consisting of a set of social media platforms (such as VKontakte) and web services (such as Telegram) which have content in Russian language, and are popular among people who live in Russia.

[ii] See Popugaeva, 2018.

[iii] We use the metaphor of occupation to refer to the intense efforts by government agencies to regulate Russian citizens' use of the Internet, in contrast to its much weaker regulation in the past.

iv FZ-114, 25 July 2002.

v FZ-148, 27 July 2006.

vi FZ-63, 13 June 1996, chapter 29, article 282. See http://www.sova-center.ru/en/xenophobia/news-releases/2008/07/d13746/; http://www.consultant.ru/popular/ukrf/

[vii] In August 2018 The European Court of Human Rights held unanimously that Terentyev's freedom of expression had been violated.

viii In this section we will draw, among other sources, from the publication of the "Foundation Inostrannyi Agent"which lists 22 such laws dated between June 2012 and October 2014. (List of repressive laws 2014, see also Laws of attrition, 2013 and Freedom on the Net (2011; 2012; 2013).

ix FZ-139, 28 July 2012.

x FZ-398, 28 December 2013.

xi FZ-187, 2 July 2013. Legal rights owners who discover a violation of their rights can appeal to a court requesting access to the relevant platform to be restricted. *Roskomnadzor* will determine the corresponding intermediary (e.g., hosting provider) and send a notice of infringement within three working days. The intermediary is further required to inform the owner of the (online) information resource of this notice and the latter has to remove the illegal contents within one working day. If the information intermediary fails to apply such enforcement measures, the telecom operator concerned,, upon the authorisation of *Roskomnadzor*, is required to block access to the information resource within 24 hours. (Alexandrov & Medvedev, 2017).

xii FZ-97, 5 May 2014.

[xiii] FZ-276, 29.7.2017.

xiv FZ-110, 5 May 2014.

xv FZ-179, 28 June 2014.

xvi FZ-242, 21 July 2014.

xvii FZ-274, 21 July 2014.

xviii On the misuse of anti-extremist laws, see http://www.sova-center.ru/en/misuse/

xix FZ-65, 8 June 2012.

xx FZ-141, 28 July 2012.

xxi FZ-119, 20 July 2012.

xxii The ban on alcohol advertising was lifted in 2014 until the end of 2018 when Russia hosts World cup in football.

xxiii FZ-121, 20 July 2012.

xxiv FZ-192, 12 November 2012.

xxv FZ-136, 29 June 2013.

xxvi FZ-135, 29 June 2013.

xxvii Knight (2018) has noted at least eight cases of censorship based on the law, among them the pressuring and fining of Vera Klimova, the founder of the website 'children-404' established to support LGBT teenagers, and the closing of the website which raised awareness about the HIV epidemic in Russia.

xxviii FZ-5, 3 February 2014.

xxix FZ-130, 5 May 2014.

xxx FZ-142, 4 June 2014.

xxxi http://openinform.ru/news/unfreedom/04.02.2014/29343/

xxxii FZ-374, 6 July 2016, FZ-375, 6 July, 2016.

xxxiii FZ-208, 23 June 2016.

xxxiv https://rsf.org/en/news/new-russian-law-targets-news-aggregators

xxxv https://themoscowtimes.com/articles/how-a-new-law-is-making-it-difficult-for-russias-news-aggregators-to-tell-whats-going-on-57657

xxxvi FZ-276, 29.7. 2017, https://rg.ru/2017/07/30/fz276-site-dok.html, https://www.cactusvpn.com/privacy/russian-duma-bill-ban-vpns/

xxxvii FZ-245, 29 July 2017.

xxxviii FZ-149, 27 July 2006.

xxxix https://phys.org/news/2018-04-russian-blocking-messaging-app-telegram.html

xl https://secretmag.ru/navalnyi/

xli https://www.change.org/p/отменить-пакет-яровой-2

xlii https://meduza.io/en/news/2018/04/23/russia-s-crackdown-on-telegram-disrupts-google-services-across-the-country

xliii https://secretmag.ru/navalnyi/

xliv It is interesting to note the parallels and contacts related to Internet regulation between Russia and China; many of the measures introduced in Runet follow the pattern previously implemented by China. An example of such measures is the practice of identifying users with a mobile phone when creating an Internet connection, for example at airports or cafes. Russia and China are also co-operating in lobbying internationally for the development of Internet governance in a more state-orientated direction (Russia

and China, 2015). Technically, Runet is connected to the global Internet mainly via the state-controlled *Rostelekom*, which has the capability to isolate Russia from the rest of the world. However, the infrastructure, applications and user culture of Runet were able to develop freely until 2012, and, unlike China, it was not isolated by a firewall or monitored strictly by an army of state-employed censors.

Table 1. Internet regulation in Russia 2008–2017

Type of restriction*	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
Murder	1	1	0	1	0	1	1	0	0	1
Violent acts (threats)	1	1	1	10	3	23	26	28	50	66
Proposals to regulate the Internet	6	7	5	5	49	75	87	48	97	114
Criminal prosecution / detention	1	10	8	38	103	226	132	202/18	298/32	411/48
Administrative pressure	2	1	2	173	208	514	1448	5073	53004	22523
Restriction of access	0	6	2	231	609	236	974	1721	35019	88832
Court order prohibiting information	na	na	na	0	124	624	72	7300	24000	2196
Cyber attacks	0	1	1	31	47	63	10	30	122	15
Civil lawsuits	1	8	10	11	26	37	60	49	170	39
Other	0	1	4	0	28	34	168	570	3343	1509
Total	*12*	*36*	*33*	*500*	*1197*	*1832*	*2951*	*15021*	*116103*	*115706*

Sources: Gainutdinov & Chikov 2011; 2017; 2018. The authors note that their monitoring does not take a stand on the issue of the *justness* of all instances of monitoring. The restriction of access may thus include both restrictions on ISIS pages as well as the pages of political and social websites. Nevertheless, threats and assaults can never be justified.