ANALYSIS

The Digital Counter-Revolution

Why the Kremlin pursues a sovereign Internet

| Antonin Plattner |

November 2019

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

Title:	The Digital Counter-Revolution: Why the Kremlin pursues a sovereign Internet
Author(s):	Plattner, Antonin
Publication date:	November 2019
Category:	Analysis

Keywords: Internet, sovereignty, authoritarianism, democracy, governance, technology, infrastructure, national security, Russia

Cover page photo: People attend an opposition rally in Moscow, Russia, on 10 March 2019. Participants in the rally are protesting against the bill about sovereign RuNet and censorship on the Internet. EPA/Maxim Shipenkov/Scanpix

Disclaimer: The views and opinions contained in this paper are solely those of its author(s) and do not necessarily represent the official policy or position of the International Centre for Defence and Security or any other organisation.

ISSN 2228-2076

63/4 Narva Rd., 10152 Tallinn, Estonia
info@icds.ee, www.icds.ee

Introduction

On 25 July 2019, the Select Committee on Intelligence of the US Senate released a report on "Russian active measures campaigns and interference in the 2016 U.S. election".[1] Its main finding is that "extensive activities" had been carried out "at least from 2014" until "at least 2017" but that "Russian intentions regarding U.S. election infrastructure remain unclear" since "no evidence that any votes were changed or that any voting machines were manipulated" was found. Quoting former Homeland Security adviser Lisa Monaco, the report makes the hypothetical assumption that these "active measures" might have had as an overarching goal "to sow distrust and discord and lack of confidence in the voting process and the democratic process". This analysis aims to support this thesis by substantiating and contextualising the Russian state's active measures in the broader context of Putin's domestic and international digital counter-revolution. It argues that this campaign not only sought to undermine public confidence in democratic processes but also attempted to erode our trust in the freedom of the internet in order to indirectly promote Moscow's calls for "internet sovereignty".

1. Vladimir the Restorer

If Vladimir Putin was a tsar, this is probably the way he would have told people he wanted to be praised and remembered—the Restorer. He lived through the collapse of the USSR, which he regards as a humiliation. He genuinely, and in all modesty, thought he was the chosen one to avenge the insult of the "greatest geopolitical catastrophe of the 20th century".[2] Ever since, an unwavering spirit of restoration has animated his political views: restoring the Kremlin's prestige and strength both domestically and internationally remains his only ideological driver. Thus, his political vision started out with an end in mind.

The "colour revolutions" in Ukraine, Georgia and Kyrgyzstan (and the small-scale protests they inspired in Moscow in 2005) convinced Putin that his reactionary "project" could be transcended by progressive forces, ready to break the spell of a country doomed to be ruled by autocratic regimes. The Restorer had to take the initiative back at any cost. That's when the Kremlin started ringing the bells of a "preventive counter-revolution".[3]

If Vladimir Putin was a tsar, this is probably the way he would have told people he wanted to be praised and remembered—the Restorer

This counterattack took shape through "the elaboration of 'sovereign democracy' as a state ideology", which quickly established itself as the federal government's new political mantra.[4] However, the Kremlin's "preventive counter-revolution" had to deal with a rather adverse environment. The digital revolution had already started to reshape the global and domestic balance of power by transforming information, communication, production and power paradigms. The internet quickly catalysed the government's hysteria, which (temporary) reached its peak in 2014 when Putin called it a "CIA conspiracy".[5]

[1] U.S. Senate, "Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts Against Election Infrastructure With Additional Views", Report 116-XX (Washington, DC, July, 2019) (accessed 7 August 2019).

[2] Andrew Osborn, "Putin: Collapse of the Soviet Union was 'catastrophe of the Century'", *The Independent*, 26 April 2005 (accessed 7 August 2019).

[3] Robert Horvath, *Putin's Preventive Counter-Revolution: Post-Soviet Authoritarianism and the Spectre of Velvet Revolution* (Abingdon: Routledge, 2013).

[4] Ibid., 1.

[5] Vladimir V. Putin, "*Mediaforum Nezavisimykh Regionalnykh i Mestnykh SMI*" (Forum of Regional and Local Independent Mass Media), *Prezident Rossii*, 24 April 2014, transcript (accessed 7 August 2019).

Being intrinsically international, the internet has become the most serious challenger to the authoritarian "sovereign democracy". The restoration of the Russian federal state's power and prestige needed a digital counter-revolution. In 2015, Nikolay Nikoforov, Putin's zealous minister of communications, came up with an original suggestion: that "sovereign democracy" be supplemented by the concept of "internet sovereignty".[6] This brilliant idea has sought ever since to hijack the features that have made the internet a success: its intrinsic freedom and borderless nature. The move constitutes a desperate attempt to restore Moscow's central power by imposing absolute and unrestricted power over domestic information and communication technologies (ICT). Internationally, "internet sovereignty" aims ultimately to "digitalise" Moscow's power politics by enforcing a neo-Westphalian, state-centric global internet governance. Moreover, to force the international community to support Nikoforov's outstanding idea, Putin decided to enact his worst nightmare: a global internet-based campaign of disruption aimed at sowing "distrust and discord and lack of confidence" in the freedom of the internet.[7]

Being intrinsically international, the internet has become the most serious challenger to the authoritarian "sovereign democracy". The restoration of the Russian federal state's power and prestige needed a digital counter-revolution

2. The Media President

Everybody knows Vladimir Putin—this omnipotent, omnipresent and omniscient "new tsar" roaming ruthlessly around his kingdom, bare-chested on the back of his stallion and exhibiting an inspirational will to resolve all kind of issues.[8] This political iconography has been popularised within Russia and widely projected abroad. However, there is a stark contrast between this rather unequivocal and media-friendly image of Putin's absolute power and the polyphony, if not anarchy, of Russian governance. Given the expertise of the country's security services in this field, the image of the "new tsar" icon could even represent a successful long-running piece of *maskirovka*, the military doctrine of deception, denial and disinformation inherited from Soviet times. Even if the concept of "power vertical", which "defines the regime of Russia as a system of faithfulness, loyalty and complete subordination to one person" is relevant in the realm of Russian tactical decision-making, it may be misleading when addressing issues related to the design and implementation of long-term strategies.[9]

In reality, the Russian political sphere is a largely informal bullring in which different factional and individual interests struggle for primacy. Sam Greene, director of the King's Russia Institute, describes this political system as a "hybrid authoritarianism" that is "both disengaged and deinstitutionalized, seeking to minimize points of contact between the state and its citizens and, where contact is necessary, failing to structure that engagement along coherent, predictable patterns".[10] A specialist on Russian systemic corruption, Alena Ledeneva, named this murky and clientelist form of governance the *Sistema.* She describes Putin as the public face and central node of a complex assemblage of power networks that

[6] Anastasia Galtitsyna, Elizaveta Ser'gina, "*Ministr Svyazi Predlozhit Pravitelstvu Vsyat' Runet Pod Kotrol'*" (Minister of Communication proposes that government takes control of Runet), *Vedomosti,* 26 March 2015 (accessed 7 August 2019).

[7] U.S. Senate, "Report of the Select Committee on Intelligence".

[8] See Steven Lee Myers, *The New Tsar: The Rise and Reign of Vladimir Putin* (Knopf, 2015).

[9] Marius Laurinavičius, "Putin's Russia: The Nature and Contradictions of the Regime", *Lithuanian Annual Strategic Review* 14*,* (2015-2016): 121; The new National Defence Control Centre (NDCC), established in Moscow in 2014 and supported by one of the most powerful computers in the world, functions as a "wartime government" able to swiftly coordinate all spheres of Russian state power.

[10] Samuel A. Greene, *Moscow in Movement: Power and Opposition in Putin's Russia* (Stanford, CA: Stanford University Press, 2014): 220.

"lock politicians, bureaucrats and businessmen into informal deals, mediated interests and personalised loyalty".[11]

The main feature of the *Sistema* is that it permits power to be exercised in an indirect and opaque manner, thereby avoiding any kind of public scrutiny. This indirect governance creates a protective "soft focus" for illegal and arbitrary political practices while delivering, when needed, significant potential for plausible deniability by the political leadership. It is therefore clear that the survival of this informal and remote *Sistema* depends on the shadow in which it operates. Any bright light shone on those networks would threaten the entire state apparatus. This shows the vital importance for the regime of maintaining and nurturing the grotesque "new tsar" iconography in Russia and abroad and thereby underlines the strategic significance of keeping ICT under government control.

3. The Domestic Digital Counter-Revolution

The fact that "media and the Internet are crucial for Putin's 'managed democracy', media campaigns and media rule" should not be surprising as it is "consistent with the *modus operandi* of the Soviet administrative system, where media executives were a key part of the nomenklatura".[12] The regime therefore regards the control of information as a top priority for its own security. Sustaining the information smokescreen that protects the shadowy *Sistema* from any public scrutiny and projecting an iconic image of stable and uncontested power abroad remains a matter of survival for Putin's restoration regime. This results in an ever-growing and endless securitisation of communications. In fact, the leaders of the Russian state are trapped in the vicious paranoid spiral that characterises authoritarian and arbitrary regimes: its fear of information is nurtured by its own deceitful use of the media.

Because the control of the so-called "traditional media" was attracting most of the government's efforts during Putin's first and second terms, the internet quickly revealed itself as a formidable platform for challenging the supremacy of the official narrative.[13] Indeed, the Russian political leadership didn't immediately grasp the subversive potential of the digital revolution within the information sphere. New information technologies were even viewed positively and used by officials under Medvedev's presidency. However, a turning point was reached with the colour revolutions of the 2000s, the Arab Spring and the 2012 mass protests in Russia, in which online social networks played a significant role. The political leadership then recognised the emancipatory role of internet-based media.

The regime also felt deeply destabilised by the "the blurring [of] lines between police and citizens, which questions the traditional theorization of state power" in cyberspace.[14] Indeed, the digital truncheon hasn't yet been invented and thus laws can't be enforced online in the same way as offline. As a matter of urgency, president Putin's *media*ted authoritarianism and its mutually responsible inter*media*ries had to impose their arbitrary power in cyberspace, and therefore shift the focus of its information control policies towards web-based media and communications: the digital counter-revolution was launched.

Sustaining the information smokescreen that protects the shadowy Sistema *from any public scrutiny and projecting an iconic image of stable and uncontested power abroad remains a matter of survival for Putin's restoration regime*

[11] Alena V. Ledeneva, *Can Russia Modernise? Sistema, Power Networks and Informal Governance* (Cambridge, UK: Cambridge University Press, 2013): i.
[12] Ibid.: 81, 90.
[13] Carolina Vendil Pallin, "Internet control through ownership: the case of Russia", *Post-Soviet Affairs* 33, No.1 (2017): 20.
[14] Azadeh Akbari & Rashid Gabdulhakov, "Platform Surveillance and Resistance in Iran and Russia: The Case of Telegram", *Surveillance & Society* 17 no.1/2 (2019): 224.

4. The International Digital Counter-Revolution

The digital revolution also brought changes in the international system. On the one hand, it fostered the multiplication of actors in international politics and provided small countries with a new dimension in which physical boundaries could be overcome. On the other, it reduced the political impact of brute force, which is a historical asset of the Russian Federation. Indeed, in contrast with the physical space, "the power of a network is not determined by resources but by the number of nodes on it, which equates to the power of information/influence".[15]

Cyberspace must therefore be considered a realm in which the paradigm of power cannot apply in symmetry with the physical world. The cards of power are thus redistributed in the online context, giving a chance to smaller actors to play at the same level as entities that would be out of their reach in the physical world. The celebrated case of Jonathan James, the 15-year-old who hacked into the US National Security Agency from his bedroom, is the best illustration of this point.[16] But this is also true at the level of communication, where an ordinary citizen can potentially have an impact similar to the ICT industry by "addressing a mass audience" with messages that "are not sent just once but can be re-sent or rediscovered at various points in time".[17] This is mostly due to the accessibility and low cost of cybertechnologies that multiply exponentially the number of stakeholders as well as their capacities. In addition, it is generally assumed that cyberspace offers a permanent advantage to offensive actions, in contrast to the difficulty of digitally defending oneself. This all creates the ideal setting for asymmetrical information warfare between physical world powers and digital dissidents.

In an attempt to counterbalance the emancipating effects of the digital revolution, the governments of countries like China, Iran and Russia now invest tremendous effort in controlling domestic online activity while conducting cyber operations abroad

The various approaches of countries to this new "online power paradigm" can be divided into two categories. On the one hand are the liberal, stable and/or small countries that have seen this digital revolution as an opportunity to foster their social and economic development and transcend their physical constraints (such as surface area, population size or natural resources limitations). Indeed, liberal policymakers tend to view the digital revolution as an opportunity to engage closer with their citizens rather than as a threat to their authority. "E-democracy" doesn't simply offer bureaucratic efficiency but could also provide states with a new form of grassroots checks and balances that can help to inform and effectively implement political decisions.

On the other hand, authoritarian and fragile regimes have quickly felt threatened by this self-managed digital wind of freedom and emancipation that was blowing domestically and internationally. They nonetheless grasped the potential of the internet in terms of internal surveillance and external espionage and disruption. In an attempt to counterbalance the emancipating effects of the digital revolution, the governments of countries like China, Iran and Russia now invest tremendous effort in controlling domestic online activity while conducting cyber operations abroad.

[15] Jason Andress, Steve Winterfeld & Lillian Ablon, *Cyber Warfare, Techniques, Tactics and Tools for Security Practitioners,* 2nd edition (Waltham, MA: Syngress, 2014): 5.

[16] David Stout, "Youth Sentenced In Government Hacking Case", *The New York Times*, 23 September 2000 (accessed 7 August 2019)

[17] Pallin, "Internet control through ownership": 20.

5. Decree 646

Official doctrines are the usual starting point for the analysis of any country's cyber-strategy. In the case of Russia, *Ukaz* (Decree) 646 of 2016 can be considered the nearest equivalent to cyber-related white papers in the West.[18] This requires, first and foremost, an important clarification regarding the way Russia relates to cyber-security, which is referred as the broader concept of "information security". Within this framework, the internet is seen both as a tool and as a threat. This concept defines the "state of safety from internal and external informational threats for the individual, society and the state in which it is possible to realise constitutional order, … sovereignty, territorial continuity … and the defence and security of the state".[19]

Essentially, Decree 646 stresses the need to counter the "destruction of sovereignty and the undermining of territorial integrity" caused by the internet.[20] In order to do so, it prescribes measures at the national and international level. Domestically, it calls for "an increase in the security of cyber-infrastructures, prohibiting foreign control over them and ensuring a secure and stable interconnection of the state's organs".[21] At the international level, it advocates the "formation of a stable system of peaceful interstate relationships in cyberspace" and the "creation of an international governing system of information security … for the defence of the Russian Federation's sovereignty in the information space".[22] This resort to the notion of sovereignty reveals a set of legal and conceptual tensions. They are catalysed in the expression used to define what the Kremlin considers its national cyberspace. Indeed, the "Russian Federation's segment of the internet" is a rather unclear and highly problematic term.[23]

6. Russkii isn't Rossiskii

Given the multi-dimensional nature of the effects of a cyber-strategy, analysing them presents a real challenge. Indeed, the Internet is simultaneously national and international, as well as physical and digital. Isolating these aspects can be tempting for the sake of a simplified and traditional analysis, but doing so would inevitably lead to flawed results. In the case of Russia, semantic precision is crucially important. It is a common and misleading mistake to use the term "Russian" in internet-related concepts (e.g. "Runet", "Russian cyberspace", "Russian blogosphere", "Russian active measures"). The English language lacks the ability to make a clear-cut distinction between the Russian words *russkii* and *rossiskii*. The former defines an ethnic and linguistic quality, while the latter relates to the federal state and could be translated as "citizen of the Russian Federation" (*Rossiskaya Federatsiya*). It is vital to underline the fact that millions of Russians (*russkii*) are not citizens of the Russian Federation (*rossiskii*). Conversely, millions of citizens of the Russian Federation are not ethnic Russians.

> *The English language lacks the ability to make a clear-cut distinction between the Russian words* russkii *and* rossiskii*…This subtle but important semantic distinction has strong political implications*

[18] President of the Russian Federation, Ukaz no. 646, "*Ob Utverzhdenii Doktriny Informatsionoi Bezopasnosti Rossiiskoj Federtsii*" (Reinforcing the Cyber Security Doctrine of the Russian Federation), 5 December 2016 (accessed 7 August 2019).

[19] Ibid., I.2.(v).

[20] Ibid., III 15.

[21] Ibid., IV 23 (g).

[22] Ibid., IV 28 ; II 8 (d).

[23] Ibid., IV 29.

This subtle but important semantic distinction has strong political implications, especially in the Baltic states and Ukraine, where a proportion of the population use Russian as their mother tongue without having any ties to the Russian Federation. The common Western confusion between "Russian-speaker" and "Russian citizen" constitutes an ideal fulcrum for Moscow's extensive kin-state policy and cyber-strategy.[24] In the same vein, by claiming sovereignty over the "Russian Federation segment of the internet", Decree 646 makes an extremely contentious declaration. The architecture of the internet is by its very nature international and trans-border. The three layers (logical, physical and social) that make up cyberspace are decentralised. Thus, the very idea of digital borders in cyberspace is at best a delusion of out-of-touch policymakers and at worst a call for territorial aggression.[25]

The three layers (logical, physical and social) that make up cyberspace are decentralised. Thus, the very idea of digital borders in cyberspace is at best a delusion of out-of-touch policymakers and at worst a call for territorial aggression

Putin's regime isn't seeking *control* of the "Russian Federation's segment of the internet"; it wants to *create* it. From this perspective, the risk of seeing the Kremlin instrumentalising the aforementioned semantic confusion at the cyber level should not be underestimated. Indeed, the so-called Runet bears no relation to the physical border of the Russian Federation. It should be considered multinational and sovereignty-free as it alone defines the part of the internet available in the Russian language.

Putin's regime isn't seeking ***control*** *of the "Russian Federation's segment of the internet" – it wants to* ***create*** *it*

The Russian Federation can, however, legitimately claim sovereignty over the physical, logical and social layers of cyberspace that are built or hosted entirely within its territory. As the *Tallinn Manual* argues, "[t]he physical layer of cyberspace … within a State's territory is self-evidently subject to that State's sovereignty", which also gives it "the right to control aspects of the logical layer of cyberspace within [its territory]" and "regulate the cyber activities of those on its territory".[26]

The juridical propositions of the *Tallinn Manual* have nonetheless been judged extremely unsatisfactory by Moscow. To understand why, the next section will analyse what the Russian Federation has done in order to fulfil the two main goals articulated in Decree 646: the exclusion of foreign control over "Russian" cyber infrastructure and the "formation of a stable system of peaceful interstate relationships in cyberspace".[27] This will demonstrate that enjoying national sovereignty in the form of absolute state control over each of the Russia-based layers of the internet does not imply unconditional authority over any kind of "segment" of cyberspace. Moscow has been unable to enforce its "digital borders". As a consequence, and despite all the Kremlin's efforts, the Russian population is still able to override the state's censorship and surveillance to access the free internet.

[24] Kristina Kallas, "Claiming the diaspora: Russia's compatriot policy and its reception by Estonian-Russian population", *Journal on Ethnopolitics and Minority Issues in Europe* 15, No. 3 (2016): 1–25.

[25] "The physical layer comprises the physical network components (i.e., hardware and other infrastructure, such as cables, routers, servers, and computers). The logical layer consists of the connections that exist between network devices. It includes applications, data, and protocols that allow the exchange of data across the physical layer." Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, UK: Cambridge University Press, 2017): 12.

[26] Ibid., rules 2.4, 2.6 and 2.7.

[27] President of the Russian Federation, Ukaz 646, IV 28.

7. Land-based Infrastructure

In Russia, the land-based internet uses broadband access cables laid alongside railway lines. These cables are under the control of Transtelekom (TTK), which is owned by Russian Railways, a state-owned joint-stock company.[28] Internet cables are then connected through exchange points, a sort of "data road junction". The internet exchange points located in the territory of the Russian Federation are managed by an organization called MSK-IX, nicknamed the "heart of the Runet", which is ultimately controlled by the state-owned Rostelekom.[29]

Russia-based core physical infrastructure (cables and exchange points) may therefore seem to fall under the total control of the Kremlin. This, however, would be to ignore the specific way these installations work. Indeed, MSK-IX relies on the Anycast routing technology to convey data. Extremely popular among the network operators, this technology "will select the desired path on the basis of number of hops, distance, lowest cost, latency measurements or based on the least congested route".[30] Put simply, when internet users are browsing the web, their connection to sites may transit physical infrastructure located in different countries and depend on various factors such as the cost of electricity at a given time and in a specific region.

To save money and increase efficiency, MSK-IX exchange points therefore split their distributed DNS between servers located in Asia, Europe, South America and North America.[31] In practice, this means that a connection from a Russian computer to a website hosted by a US-based server may transit Prague and New York at a given time but Singapore and Los Angeles a few hours later. Total sovereignty over land-based connections would therefore imply enforcing sovereignty over shared infrastructure located in other countries or even in sovereignty-free territories (such as intercontinental cables laid in international waters). This illustrates the difficulty, if not impossibility, of addressing "internet sovereignty" in purely Westphalian terms. As the *Tallinn Manual* underlines, "[t]he fact that cyber infrastructure located in a given State's territory is linked to cyberspace cannot be interpreted as a waiver of its sovereignty".[32]

> *Total sovereignty over land-based connections would therefore imply enforcing sovereignty over shared infrastructure located in other countries or even in sovereignty-free territories. This illustrates the difficulty, if not impossibility, of addressing "internet sovereignty" in purely Westphalian terms*

8. Censorship

The Russian authorities are also attempting to control web content through filtering and censorship. The so-called "blacklist" laws (139-FZ and 398-FZ) allow the censorship of websites "containing child pornography, advocacy of drug abuse and advocacy of committing suicide … and extremist speech".[33] Federal Law 398-FZ of 2013 "empowers Roskomnadzor [Federal Service for Supervision of Communications, Information Technology and Mass Media] to include on the blacklist websites containing calls for mass unrest, committing extremist activities or participating in public meetings conducted in violation of the law".[34] This unclear legal framework gives the law-enforcement agencies and the justice department blurred and arbitrary room for manoeuvre.

As a typical cause and effect of Russia's *Sistema*, signs of the opaque merging of informality and officialdom are perceptible when identifying the actors and processes of

[28] Pallin, "Internet control through ownership": 22.
[29] "MSK-IX"; Igor Korolev, "Rostelekom Kupil Serdtse Runeta" (Rostelekom buys the heart of the Runet), *Cnews*, 15 January 2015 (accessed 7 August 2019).
[30] Wikipedia, "Anycast" (accessed 7 August 2019).
[31] "MSK-IX".
[32] Schmitt, *Tallinn Manual*, Rule 1.6.
[33] Liudmila Sivetc, "State regulation of online speech in Russia: the role of internet infrastructure owners", *International Journal of Law and Information Technology* 27, No. 1 (2019): 30.
[34] Ibid., 41.

internet censorship in Russia. More precisely, it is commonly accepted that about four main factions participate in the polymorphic Russian political arena: the *Siloviki* or "Securocrats", hardliners emanating from the state's security services; the Ideologists, such as Church representatives; the Liberals, focused mostly on the economic aspects of liberalism; and the Oligarchs. This polyphony is visible in the internet control policies as "new initiatives for increasing control come from ministries and agencies as well as from Duma deputies, the Russian Orthodox Church, conservative political organizations and think tanks, and regional politicians".[35]

To alleviate the physical and technical impossibility of reviewing and assessing the huge amount of internet content, the Russian government is falling back on psychological methods

To alleviate the physical and technical impossibility of reviewing and assessing the huge amount of internet content (e.g. 500 hours' worth of videos is uploaded every minute on YouTube alone), the Russian government is falling back on psychological methods.[36] In fact, the rather intricate mix of public/private and official/informal actors and processes is aimed at establishing self-censorship through the institution of a climate of legal randomness in which "no pattern as to who will be charged according to the new restrictive laws or for what could ever be captured".[37] As noted by Sarkis Darbinyan, the head of Roskomsvoboda's legal team, and Sergei Smirnov, chief editor of MediaZona, the repressive component of the internet policy is operated "randomly", targeting not only political opponents but also nationalists, atheists, LGBT advocates and so on.[38] This is principally done on account of the variable geometry of articles 280 and 282 of the Criminal Code, which prohibit "inciting people to extremism" and "extremist hate speech".[39] This wide range of victims of censorship reflects the interests of the different *Sistema* factions involved in policy-making and remote governance. In the same way, no distinction is made between posting original content and re-posting or "liking" it. Pushing even further, the Ministry of Interior declared the "failure to report a witnessed crime as an act of crime in itself", thereby echoing the call for civilian participation in the censorship process.[40]

Legal provisions and their random implementation are complemented by official incentives designed to foster the active contribution of lambda citizens in the censorship process. In this way, the Safe Internet League is recruiting volunteer internet users to signal "dangerous content" but also "flag positive content", thus constituting a body of unpaid voluntary censors. In an attempt to expand the scope of Roskomnadzor's censorship beyond Russia's national borders, this official organisation is also promoted internationally, underlining once more the transnational tendencies of Russia's "internet sovereignty".[41]

However, this bunch of messy and unfair measures did not deter or foresee the somewhat fierce online disobedience and resistance of Russian society. A high level of mobilisation in favour of internet freedom in civil society ensued: "a set of individual practices, know-how, or *arts de faire*, is being developed by RuNet users to bypass access restrictions or protect their communications from governmental surveillance".[42] In fact,

[35] Pallin, "Internet control through ownership": 17.
[36] J. Clement, "Hours of video uploaded to YouTube every minute as of May 2019", *Statista*, July 15, 2019 (accessed 7 August 2019).
[37] Pallin, "Internet control through ownership": 17.
[38] Roskomsvoboda is a Russian non-profit, non-governmental organisation for the defence of online freedom. MediaZona is a Russian independent media outlet, focusing on judicial matters; Interview with Sarkis Darbinyan and Sergei Smirnov (among others), "In 'kontakt' with the cops", *Meduza*, 7 July 2016, transcript (accessed 7 August 2019).
[39] Ibid.
[40] Azadeh & Gabdulhakov, "Platform Surveillance and Resistance in Iran and Russia": 226.
[41] Ligainternet.ru, "The Safe Internet League" (accessed 7 August 2019).
[42] Ksenia Ermoshina & Francesca Musiani, "Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era", *Media and Communication* 5, No.1 (2017): 42.

repressive measures taken by the government often trigger public reaction, ranging from public demonstrations such as those following the banning of the messaging app Telegram to protests by experts and the private sector and retaliation by homegrown hackers. For example, Digital Revolution, a group of cyber-dissidents, publicly released 7.5 terabytes of highly secret projects related to the control of the internet stolen by a secret crew of hackers by hacking FSB servers on 13 July 2019.[43] This exploit is not the fruit of an isolated and spontaneous online mobilisation; it is the latest example of long-standing and strengthening active online resistance. The group had already been involved in the 2018 hacking of the Kvant research centre, whose activities are monitored by the FSB and focus on social media analytics.[44] Similarly, in March 2019 a cyber-attack targeted the government's censorship system as a protest against the "internet sovereignty" bill.[45]

Powerful online dissent underlines the failure of the Russian government to impose its power on the web

This powerful online dissent underlines the failure of the Russian government to impose its power on the web. It also implies that any radical actions, such as drastically reducing broadband speed (as in Iran) or building a "great firewall" (as in China) would very probably trigger an intensification of this sort of "cyber-guerrilla".[46] This fiasco can be explained by the particularly high level of mobilisation and cyber skills in Russian society, which contrast with the situation in China, for example. But it is also the result of the authorities' original attempt to simply duplicate "predigital practices of surveillance" such as "fines, criminalities, and injunctions" at the cyber level.[47] Such "old-school" coercive techniques may be effective in spheres where information producers, infrastructure and consumers are physically limited and identifiable, but this isn't the case in cyberspace. Restraining and overseeing online speech thus requires distinct and adapted procedures such as "internet infrastructure-centric" techniques and a strategy of "control through ownership".[48]

"Control through ownership" strategy consists in encouraging loyal oligarchs to take over the information and communication sector, letting compliant businesses dominate the Russian market and digital products featuring built-in censorship, filters, back-doors and other control devices

9. Control Through Ownership

In practice, the "control through ownership" strategy consists in encouraging loyal oligarchs to take over the information and communication sector. This would in turn result in the possibility of letting compliant businesses dominate the Russian market and digital products (hardware and software) featuring built-in censorship, filters, back-doors and other control devices. This strategy is pursued mostly through laws and official requirements.

[43] Andrej Sochnikov & Svetlana Rejter, "Moskit, Nadezhda, Nautilus: Khakery Raskryl Sut'Projektov Tajnovo Podryadtchika FSB" (*Mosquito, Hope, Nautilus*: Hackers Disclose the Substance of a Secret FSB Contractor's Projects), *BBC Russkaja Sluzhba*, 19 July 2019 (accessed 7 August 2019).

[44] "Khakery Zayavili O Raskrytii Ispolz'uemoj FSB sistemy Monitoringa Sotsetej" (Hackers unveil hidden usable system of social network monitoring), *Newru.com*, 20 December 2018 (accessed 7 August 2019).

[45] Alexander Balkanov, "As Russians protested 'Internet isolation' last weekend, hackers launched DNS attacks against Yandex, exploiting flaws in the government's censorship system", *Meduza*, 14 March 2019 (accessed 7 August 2019).

[46] Azadeh & Gabdulhakov, "Platform Surveillance and Resistance in Iran and Russia": 225.

[47] Jack M. Balkin, "Old-school/New-school speech regulation", *Harvard Law Review* 127, No.8, (2014): 2297.

[48] Sivetc, "State regulation of online speech in Russia": 31; Pallin, "Internet control through ownership": 16–33.

The first step of this strategy tried to cut the Russian Federation out of the global market in order to offer it to the financial power of homegrown oligarchs. Indeed, an amendment to article 19.2 of law 305-FZ prohibited foreign companies from entering the domestic mass media market by limiting those companies' stakes to a maximum of 20%.[49] In the same vein, Federal Law 57-FZ labelled the ICT sector a "strategic branch" in which only Russian majority ownership is allowed.[50] Following the same trend, the 2014 law 242-FZ required internet service providers (ISPs) to "store personal data of Russian citizens, used by Internet services, on the territory of the Russian Federation".[51] These "nationalising" measures removed any international competition in the domestic market, and were intended to give free rein to the oligarchs, which they did.

Mandatory compliance with new regulations is made without any state support and is at the company's own expense. This creates particularly adverse conditions for small domestic businesses and boosts the ever-growing monopoly of a small clique of oligarchs

The implementation of these laws and requirements constitutes the second step of the strategy. Indeed, mandatory compliance with new regulations is made without any state support and is at the company's own expense.[52] This creates particularly adverse conditions for small domestic businesses and boosts the ever-growing monopoly of a small clique of oligarchs. For example, the compulsory installation, maintenance and updating of the mass surveillance system SORM forced any small ISP "to give about 20%–30% of its annual income to buy [SORM] equipment".[53] In June 2016, the so-called Yarovaya law required Russian telecommunications operators "to store all traffic (including calls, letters, documents, images and video) for six months, and related metadata for three years".[54] This law represents a total disconnect with technical reality. Indeed, the CEO of the Moscow State Telecom Network, Andrey Ershov, confessed that "[t]oday we do not have any equipment in order to be able to put the 'Yarovaya law' into practice".[55] Furthermore, this law does not take into account that most of the data that would hypothetically be stored are encrypted. Decrypting them (even if it were possible) would entail tremendous costs and delays. As underlined by Ermoshina and Musiani, this represents a rare case of a law pre-dating technology and is leaving internet operators with impossible requirements to fulfil, once again at their own expense.[56]

These tactics of systematic "control through ownership" have left a domestic ICT market under the overwhelming dominance of a few oligarchs. The Russian cellular network—the most popular way to access the internet in Russia—is a good example of how things work in the ICT sector.[57] Indeed, the cellular market is still under the monopoly control of four companies (MTS, MegaFone, Beeline and Tele2 Russia), all of which are controlled by Kremlin-friendly oligarchs. MTS' parent company (with 50.01%), JSFC Sistema, is controlled by Vladimir Evtushenkov (59%).[58] Alisher Usmanov, through his USM Holdings, controls MegaFone (59%) alongside the Komersant Publishing House and the Mail.ru Group.[59] (The latter in turn controls the "leading Russian language social networks,

[49] Sivetc, "State regulation of online speech in Russia": 30.

[50] Pallin, "Internet control through ownership": 21.

[51] Ermoshina & Musiani, "Migrating Servers, Elusive Users": 47.

[52] Ibid., 44.

[53] SORM is a country-wide system of communication interception that allows the FSB and law-enforcement agencies to conduct deep-packet inspections. See Leonid Volkov's blog, "*Arifmetika Protiv Strakha*" (Anti-fear arythmetics), May 28, 2015.

[54] Ermoshina & Musiani, "Migrating Servers, Elusive Users": 45.

[55] Ibid.

[56] Ibid.

[57] A recent survey showed that smartphones and the internet are generally considered more important by the Russian population than living in the "motherland". See https://romir.ru/studies/net-jizni-bez-smartfonov-interneta-i-rodiny.

[58] J'son & Partners, "The Russian cellular market, 2013–2020", 16 June 2019 (accessed 7 August 2019); Sistema.com, "Joint Stock Financial Corporation Sistema" (accessed August 7, 2019).

[59] "USM Group" (accessed 7 August 2019).

VKontakte and Odnoklassniki".)[60] Tele2 Russia is dominated by T2 PTK Holding, which is itself under the authority of the state-owned Rostelekom.[61] And finally, Beeline-VEON (formerly Vimpelcom) is 59%-owned by A1, which belongs to Alfabank's Mikhail Fridman.[62] Each of these entities and individuals falls under the Russian Federation's jurisdiction and are thereby compelled to comply with the state's censorship and surveillance requirements. Russia's operators and platforms are therefore under the Kremlin's direct or indirect control.

International platforms such as Facebook, Twitter and Google remain nonetheless independent. Indeed, the unsuccessful attempt to ban the encrypted messaging application Telegram underlines the difficulty Russia has in dealing with them. In fact, Telegram's owner, Pavel Durov, managed to tie his application to other international online services. When Telegram was blocked by the Russian authorities, other platforms such as Google, Google Drive and YouTube became simultaneously inaccessible in the country.[63] The disruption of service that followed resulted in two billion US dollars'-worth of losses for Russian business, which forced the ban to be unofficially lifted.[64] This convinced the regime that it needed the collaboration of the international platforms. Without their help, it simply couldn't enforce any type of error-free, watertight and unalterable filtering and surveillance.

10. International Platforms: Carrot and Stick

Despite the reticence of the international digital services and platforms to take part in the Kremlin's censorship and surveillance venture, the Russian government has had some success. Moscow firstly tried to export its *Sistema* abroad in order to take over some of the most successful foreign platforms. Thanks to the Panama Papers, the case of Facebook is well documented.

In 2010, Yuri Milner, a Russian oligarch who snapped up Medvedev's commission for digital development, surprised the world of finance when he bought 1.96% of Facebook for 200 million US dollars. This bold move valued the social networking site at "around $10 billion, or well above the $3 billion that private equity investors reportedly valued the site at".[65] As the results of various investigations showed, this investment was in fact made by the Kremlin-controlled Gazprom Investholding and VTB bank.[66] Whatever the true origins and intentions behind this investment, Yuri Milner and Mark Zuckerberg became close friends, as the latter's invitation to Milner's wedding in 2011 testifies.[67] In a 2015 interview, Milner was asked about what he got in return for his generous investments (800 million dollars in total, split between Twitter and Facebook). He replied that he had not joined the companies' boards officially but took part in the decision-making process "on an informal basis" and that

Despite the reticence of the international digital services and platforms to take part in the Kremlin's censorship and surveillance venture, the Russian government has had some success

[60] Ibid.
[61] "*Sovet Direktorov Sovmestnovo Predpyatiya Tele2 i Rostelekoma Vozglavil Predstavitel'VTB*" (A representative of VTB leads the executive board of the Tele2–Rostelekom joint venture), *Forbes*, 24 April 2014 (accessed 7 August 2019).
[62] "A1 Group" (accessed 7 August 2019).
[63] Azadeh & Gabdulhakov, "Platform Surveillance and Resistance in Iran and Russia": 228.
[64] Ibid.
[65] Parmy Olson, "Facebook's New Billionaire Backer", *Forbes*, 27 May 2009 (accessed 7 August 2019).
[66] Jesse Drucker, "Kremlin Cash Behind Billionaire's Twitter and Facebook Investments", *The New York Times*, 5 November 2017 (accessed 7 August 2019).
[67] Jon Swaine & Luke Harding, "Russia Funded Facebook and Twitter Investments Through Kushner Investor", *The Guardian*, 5 November 2017 (accessed 7 August 2019).

he “sometimes get[s] informal advice from them”.[68] What Milner probably meant at that time is that the *sistema*-like “informal deals ... and personalised loyalty” he established with Twitter and Facebook would grant him and his partners the companies’ favour. For example, Alisher Usmanov’s Mail.ru Group (which served as an intermediary between the Kremlin and Milner during the Facebook and Twitter deal), was among the 61 beneficiaries of Facebook’s secret data access extension.[69] In fact, Mark Zuckerberg offered these companies “access to its users’ data after saying it had restricted access to such data back in 2015”.[70] The Federal Agency on Press and Mass Communications of the Russian Federation also suggests a collaboration between Facebook and the Russian authorities (which could explain why Facebook, WhatsApp and Instagram aren’t yet banned in Russia). Its 2018 report states: “According to the words of the entrepreneur Pavel Durov, ‘in six years, Telegram didn’t pass a single bit of information to third parties’. This is something we can’t say about Facebook and WhatsApp.”[71]

Not all international companies have been as easily seduced as Facebook was. Indeed, some companies were more reluctant to accept Russian funds and comply with the Kremlin’s terms. With these, Moscow used more heavy-handed and protectionist arguments

But not all international companies have been as easily seduced as Facebook was. Indeed, some companies were more reluctant to accept Russian funds and comply with the Kremlin’s terms. With these, Moscow used more heavy-handed and protectionist arguments. One way to force these digital giants “has been to propose a tax on these companies”.[72] As if this wasn’t enough, Russian officials did not hesitate to threaten them with being blocked and thereby losing access to the extensive Russian digital market. The blockage of LinkedIn in 2016 showed that the regime was to be taken seriously in that sense.[73] The risk of missing out on entry to a significant digital market may have been a factor in convincing Google to cooperate with Moscow. In fact, after being threatened with total blacklisting, the company agreed to the Russian terms and is now responding positively to about 70% of censorship requests.[74] Since 2014, the company has also agreed to mark Crimea as part of Russian territory on the Russian version of its popular map service.[75]

11. Pulling the Plug?

The overall relative efficiency of the carrot-and-stick strategy couldn’t satisfy the Kremlin’s need for absolute control over information and communication. Its efforts to control or compel domestic and international companies didn’t prevent Western media from being accessible in Russia. One might therefore wonder why—after so many unsuccessful attempts to impose its rule in cyberspace—authoritarian Russia didn’t simply pull the plug out of the internet socket and eventually build a North-Korea-esque intranet network.

[68] Jordan Crook, “Yuri Milner Wants to Talk to Aliens”, Interview with Yuri Milner, *TechCrunsh*, video published on 21 September 2015 (accessed 7 August 2019).

[69] Jon Swaine & Luke Harding, “Russia Funded Facebook and Twitter Investments Through Kushner Investor”; Isobel Asher Hamilton, “Facebook Relaxed its Rules to Give these 61 Companies Special Access to User Data”, *Business Insider*, 2 July 2018 (accessed 7 August 2019).

[70] Fred Imbert, "Facebook says it gave companies ‘one-time’ access to user data after restricting information 2015”, CNBC, 1 July 2018 (accessed 7 August 2019).

[71] Rospetchat, (Federal Agency on Press and Mass Communications of the Russian Federation), *Rossiskaja Perioditcheskaja Petchat’. Sostayanie, Tendentsii, Perspektivii Raskvitiya v 2018 Godu* (Russian Federation’s Periodic Press: State, Tendencies and Perspectives for the year 2018), 2018, Moscow: 93.

[72] Pallin, “Internet control through ownership”: 27.

[73] Sam Shead, “Russia Has Banned LinkedIn”, *Business Insider*, 17 November 2016 (accessed 7 August 2019).

[74] Kseniya Boletskaya, “*Google Natchal Udalit Iz Poiska Zapreshonye V Rossii Saity*”, (Google starts deleting websites forbidden in Russia from its search engine), *Vedomosti*, 6 February 2019 (accessed 7 August 2019).

[75] TASS, “*Google Vklutchil Na Svoikh Kartakh Krym V Sostav Rossii*” (Google includes Crimea as part of Russia in its Maps), 11 April 2014 (accessed 7 August 2019); Meduza, “Google Maps ‘corrects’ bug that marked Crimea as Ukrainian for Russian users”, 5 March 2019 (accessed 7 August 2019).

This simple but radical idea is, however, frustrated by an unavoidable socio-economic reality shared by most of the countries appearing "digitally aligned" with Russia (e.g. China, Iran and the Central Asian republics). The ever-increasing dependence of their economies on ICT and the internet in particular does not allow them to do without the world wide web. In the case of Russia, oil-and-gas trading is estimated to constitute around 70% of GDP.[76] This financial windfall—an essential condition for the regime's stability and geopolitical ambitions—depends on ICT insofar as the global financial system relies on it for fixing prices.[77] In the same way, banking operations increasingly take place in the digital sphere. Furthermore, the prospective "blockchainization" of oil-and-gas trading underlines the strategic importance of the internet for Russia's economy.[78] This makes it extremely risky for the regime to consider outright and total disconnection from the world wide web—which would very probably be impossible anyway, thanks to the in-built democratisation of the satellite-based internet.

12. Satellite-based Internet

The satellite-based internet isn't a new technology. However, two current projects could revolutionise the sector and ruin Russia's aspiration to digitalise borders. OneWeb and its competitor Starlink are both promising a worldwide high-speed internet connection, accessible even in the most remote areas of the world. A constellation of hundreds of small satellites flying in low orbit would enable sort of worldwide Wi-Fi. This could potentially allow Russian internet users to bypass any kind of land-based installations under government control and access an uncensored version of the web.

When the FSB realised this in October 2018, a wave of panic gripped the *Siloviki.*[79] They urged the government to take action to prevent the project from happening. An emergency joint venture was set up in order to swiftly deploy a textbook case of how the *Sistema* operates: the hawkish minister of communications, Nikolay Nikiforov, was tasked to sort the issue out. Nikoforov's high profile underlines how seriously the "OneWeb threat" was taken by the Kremlin.[80] Without public explanation, he suddenly resigned from his ministerial position and became head of this informal crisis unit. Around him immediately gathered some of the usual clique of media- and communications-oriented oligarchs: Alisher Usmanov, Leonid Michelson, Vladimir Potanin and Piotr Aven.[81] Their mission was to obtain the necessary funds for Gonets, the state-owned satellite agency, to get a 51% stake in OneWeb.[82]

Satellite-based internet could potentially allow Russian internet users to bypass any kind of land-based installations under government control and access an uncensored version of the web. When the FSB realised this in October 2018, a wave of panic gripped the Siloviki

[76] Andrey Movchan, "Just an Oil Company? The True Extent of Russia's Dependency on Oil and Gas", Carnegie Moscow Center, 14 September 2015 (accessed 7 August 2019).

[77] Jian-Feng Guo & Qiang Ji, "How does market concern derived from the Internet affect oil prices?," *Applied Energy* 112 (December 2013): 1536–1543.

[78] Oilprice.com, "How Blockchain Is Changing The Face Of Oil Trading", Nasdaq, 15 February 2019 (accessed 7 August 2019); Linda Pawczuk, Rob Massey & David Schatsky, "Breaking blockchain open: Deloitte's 2018 global blockchain survey", Deloitte Development LLC, 2018 (accessed 7 August 2019).

[79] Maria Kolomychenko, "Exclusive: Russia opposes U.S. OneWeb satellite service, cites security concerns", Reuters, 24 October 2018 (accessed 7 August 2019).

[80] Anastasia Galtitsyna & Elizaveta Ser'gina, "The Minister of Communications Proposes to the Government to take Control Over the Runet"; Pallin, "Internet control through ownership": 28; Anna Balachova, Timofej Dzyadko, Lyudmila Podobedova & Svetlana Burmictrova, "*Obrital'naya Investitsiya: Kak Eks-Glava Minkomsvyazi Poveril V OneWeb*", (Orbital investment: How the former Minister of Communication believed in OneWeb), *RBC*, 28 January 2019 (accessed 7 August 2019).

[81] Ibid.

[82] Konstantin Nagaev& Maria Istomina, "*Dotchka Roskosmosa Polutchila Kontrol Nad Sovmestnym S OneWeb Biznesom*" (Roskosmos' daughter took control of

This joint venture was supported by the state's unfair methods; access to the state-owned infrastructure of Roskosmos used by OneWeb and the release of radio frequencies were used as leverage in negotiations with the company.[83] Nonetheless, Reuters later reported that, despite Nikoforov's efforts, this "control through ownership" operation failed.[84] OneWeb apparently resisted this unfair campaign.

Despite the swift amendment of the law on satellite communications that forbids any connection from Russia to a foreign satellite service, Moscow's officials knew that this legal disposition could not prevent OneWeb and Starlink signals from being accessed from within Russia.[85] This conclusion forced Moscow to launch the "Efir" project. This is a straightforward duplication of other satellite internet projects that is programmed for 2025 and designed to be cheaper and, above all, entirely under Putin's control.[86] But this is likely to be just another (costly) failed attempt to impose absolute control of the web. In fact, Putin's dream of a digital border will at some point or another need the compliance of the heart of the global internet structure: the root servers of the DNS.

Putin's dream of a digital border will at some point or another need the compliance of the heart of the global internet structure: the root servers of the Domain Name System (DNS)

13. The Root (Servers) of Putin's Impotence

The Domain Name System (DNS) works like a phone book. It is the infrastructure able to resolve domain name requests (e.g. icds.ee) into IP addresses (e.g. 217.146.72.84). Put simply, humans understand and remember names while computers only deal with numbers. The DNS is therefore a strategic infrastructure since it manages all connections within the internet. It is constituted of three hierarchical layers: root servers, top level domain servers (TLDs) and authoritative name servers. The two lower layers are already controlled by the Russian state. The coordination centre for the TLDs ".ru" and ".РФ" signed agreements with Roskomnadzor in 2009 and 2010.[87] (This arrangement was confirmed and extended on 19 April 2016.)[88] The authoritative

the joint venture with OneWeb), *RBC*, 18 February 2019 (accessed 7 August 2019)

[83] Maria Kolmytchenko, "*Signal Iz Pravitel'stva: Kak Tchinovniki Uslozhnyayut Rabotu OneWeb V Rossii*", (Signal from the government: How officials are complicating the work of OneWeb in Russia), *RBC*, 26 February 2019 (accessed 7 August 2019).

[84] Maria Kolomychenko & Andrey Kuzmin, "U.S. OneWeb satellite service has not offered stake to Russia", Reuters, 29 December 2018 (accessed 7 August 2019).

[85] Maria Kolmytchenko, "*Signal Iz Pravitel'stva*"; Government of the Russian Federation, "*Postanovlenie Pravitelstva RF Ot 14.11.2014 N 1194 (Red. Ot 25.09.2018)*", (Decree No. 1194 of 14 November 2014 by the Government of the Russian Federation (Redaction of 25 September 2018)), 25 September 2018 (accessed 7 August 2019); Roskomsvoboda, "*V Rossii Planiruyut Vvesti Chtraf za Ispol'zovanie Innostranovo Sputnikovo Interneta*" (Plans to impose fines in Russia for the use of foreign satellite internet), 11 June 2019 (accessed 7 August 2019).

[86] Valeria Chafirko, "*Rossiiskaya Globalnaya Sputnikovaya Sistema Svyasi 'Efir' Smozhet Obespetchit' Dostup K Setn Internet Uz Lyuboj Totchki Mira*" (The Russian global satellite communications system "Efir" will provide access to the internet from anywhere in the world), 360tv, 24 May 2018 (accessed 7 August 2019).

[87] Igor O. Shchyogolev & Andrej V. Kolesnikov, "*Soglashenie O Bzaimodejstvii Mezhdu Ministerstvom Svyazi n Massovikh Komunikatsii Rossijskoj Federatsii n Koordinatsionym Tsentrom Natsionalnovo Domena Seti Internet Po Voprosam Upravleniya Natsionalnym Domenom '.RU'*" (Agreement between the Minister of Telecommunications of the Russian Federation and the Coordination Center for TLDs RU on the management of the national domain), Coordination Center for TLDs RF/RU, 18 February 2009 (accessed 7 August 2019); Igor O. Shchyogolev & Andrej V. Kolesnikov, "*Soglashenie O Bzaimodejstvii Mezhdu Ministerstvom Svyazi n Massovikh Komunikatsii Rossijskoj Federatsii n Koordinatsionym Tsentrom Natsionalnovo Domena Seti Internet Po Voprosam Upravleniya Natsionalnym Domenom '.RF'*" (Agreement between the Minister of Telecommunications of the Russian Federation and the Coordination Center for TLDs RF on the management of the national domain), Coordination Center for TLDs RF/RU, 7 April 2010 (accessed 7 August 2019).

[88] Coordination Centre for TLDs RF/RU, "*Ottchot Direktora ONA Koordinatsionym Tsentrom Natsionalnovo Domena Seti Internet*" (2016 Annual Report of the Director of the Coordination Centre for TLDs RF/RU); Sivetc, "State regulation of online speech in Russia": 45.

name servers are already required by Federal Law 242-FZ to be located on Russian territory.

The only components of the DNS that remain free of Kremlin control are the root servers. For technical reasons, these are limited to 13 in number, each under the supervision of a different organisation. Ten are based in the US, one in Japan, one in the Netherlands and one in Sweden. The synchronisation of these root servers is under the supervision of the DNS Root Server System Advisory Committee (part of the Internet Corporation for Assigned Names and Numbers (ICANN)). What is important to understand here is that, as long as the Kremlin is unable to control those root servers, Russian internet users will always find ways to get round official censorship and surveillance (for example by using VPN software or private DNS). Their capacity to bypass central control will certainly become even more acute with the programmed advent of the satellite internet.

> *Put simply, whoever controls the DNS controls the global internet. For this reason, the ultimate layer of the system (root servers) is internationally managed under the multi-stakeholder governance model*

Put simply, whoever controls the DNS controls the global internet. For this reason, the ultimate layer of the system (root servers) is internationally managed under the multi-stakeholder governance model "in which governments, private companies and non-governmental organizations exist alongside one another in non-hierarchical relations".[89] The model is animated by a spirit of "denationalized liberalism" and "private sector-based, transnational forms of governance, alongside a widespread ethic of self-regulation and civil society".[90] In other words, this defines everything that Putin's counter-revolution is fighting against. Indeed, to fully achieve his despotic restoration project, Moscow needs to convince the international community to scrap the current multi-stakeholder internet governance structure for a multilateral and state-centric system (as described in Decree 646). Such a "security council of the internet" would allow the Russian government to use its traditional power politics (and why not the veto?) in order to enforce its policies of internet control and censorship beyond Russia's physical borders.

> *To fully achieve his despotic restoration project, Moscow needs to convince the international community to scrap the current multi-stakeholder internet governance structure for a multilateral and state-centric system*

In November 2017, Moscow proposed to the BRICS governments the creation of an alternative DNS.[91] If this idea is technically possible, the main issue for Russia would be to convince the rest of the world to use it. According to David Conrad, ICANN's Chief Technology Officer, navigating through an alternative Russian-led web would mean that "any person, business, or government agency from outside of Russia would have to reconfigure their phones, laptops, computers, or other devices, not to mention their routers and the DNS resolvers".[92] This is why the proposal is very likely to fail, since even "China, for one, is not likely to follow suit".[93]

Moreover, the success in 2014 of the Brazilian-led Netomundial initiative seriously threatened the chances of Moscow's alternative DNS becoming a reality.[94] This initiative was aimed at enlarging, not abolishing, multi-stakeholder

[89] Julien Nocetti, "Contest and Conquest: Russia and Global Internet Governance", *International Affairs* 91, No.1, (2015): 117.

[90] Ibid.

[91] "Russia to launch 'independent internet' for BRICS nations – report", *RT*, 28 November 2017 (accessed 7 August 2019).

[92] Tracy Staedter, "Why Russia Is Building its own Internet", *IEEE Spectrum*, 17 January 2018 (accessed 7 August 2019).

[93] Roman Goncharenko, "Russia moves toward creation of an independent internet", *DW,* 17 January 2018 (accessed 7 August 2019).

[94] Nocetti, "Contest and Conquest": 128.

governance since the objective was to involve more components from developing countries in the governing body. Furthermore, the anti-capitalist elements of the Brazilian objection to US predominance left Moscow's proposal out of the race for many attending countries. The success of Netomundial therefore severely crippled the Kremlin's "'power of initiative' in contesting the US lead in Internet governance".[95]

Without the approval of Western nations, the Kremlin cannot change the rules of the game. To convince them to do so, Putin set up a "pyromaniac firefighter" strategy. As in any mafia-like business, this is about creating the problem and providing the solution at the same time

It may be assumed that Russia's initial strategy to buy support internationally and to politicise technical organisations such as the ICANN, the International Telecommunications Union and the Internet Governance Forum has been aborted, at least temporarily.[96] It is also clear that, without the approval of Western nations, the Kremlin cannot change the rules of the game. To convince them to do so, Putin set up a "pyromaniac firefighter" strategy. As in any mafia-like business, this is about creating the problem and providing the solution at the same time. In this case, Moscow is increasingly using its talents to showcase how disruptive the freedom of the internet can be when manipulated with malicious intent.

14. The Pyromaniac Firefighter

The strategy chosen by Putin's regime is broadly speaking an attempt to suck liberal democracies into its own spiral of paranoia. Using a full spectrum approach, Russia is aiming to subtly promote its "internet sovereignty" as a remedy for the disinformation campaigns and other cyber-attacks it itself wages in the West.

In September 2011, Russia published a "Draft Convention on International Information Security", which stands in line with the call in Russia's Decree 646 for the "creation of an international governing system of information security."[97] This document places clear emphasis on states' responsibility and argues, among other things, for the need "to act against the use of information and communication technology to violate international peace and security, as well as to set up measures ensuring that the activity of governments in the information space will … correspond to generally accepted principles and norms of international law including principles of … not interfering in internal issues." [98] In the light of the established Russia-led disruption campaigns in Europe and the US, this Russian demand might have sounded paradoxical if it was not an integral part its strategy.

This "pyromaniac firefighter" game plan directly targets our democratic resilience by undermining public confidence in the open, liberal and democratic values of the internet. The equation is simple: the Putin regime will be successful in achieving undisputed domestic control and restoring its international power only if it manages to engender a panicky and inward-looking response from the liberal democracies. On the other hand, if we stand firm on our (online and offline) liberal principles, cherish our self-confidence and sustain our (cyber-) resilience, Putin's digital counter-revolution may simply dry up with the passage of time.

Using a full spectrum approach, Russia is aiming to subtly promote its "internet sovereignty" as a remedy for the disinformation campaigns and other cyber-attacks it itself wages in the West

[95] Ibid.

[96] Ibid., 122.

[97] President of the Russian Federation, *Ukaz* no. 646, II 8 (d).

[98] International Meeting of High-Ranking Officials Responsible for Security Matters, "Convention On International Information Security (concept)", 21-22 September 2011, Ekaterinburg, Russia (accessed 7 August 2019).

Conclusion

After pursuing the establishment of digital borders for more than a decade, the Kremlin has managed to bring most Russia-based internet infrastructure and activities under its yoke. However, insurmountable obstacles are preventing Moscow from imposing by itself an absolute digital sovereignty in each of the three layers of cyberspace (physical, logical and social). First, the Kremlin's control over Russia-based physical infrastructure cannot prevent the transnational operation of data transmission (Anycast routing technology). Moreover, the prospective boom of the satellite internet will certainly allow Russian internet users to bypass any land-based installations. Second, the success of the strategy of "control through ownership" remains questionable in light of the failure to ban the Telegram messaging app in Russia. This observation is confirmed by the significant difficulties Moscow experiences in replicating its strategy of control through ownership at the global level, where international platforms have the means to resist its authority and financial power. As a consequence, a portion of the Russian population manages to exploit these flaws to circumvent Moscow's control and even hack-back some of its most controversial measures.

A change in the governance of the internet sought by Russia would result in shifting the digital balance of power towards authoritarian states by destroying the emancipatory effects of the free internet on states, organisations, businesses and individuals

The regime's current failure to achieve its aspiration for absolute sovereignty over a so-called "Russian segment of the internet" is ultimately due to the multi-stakeholder governance of the DNS, the heart of the internet. By giving the same weight in decision-making to states, experts and technical organisations, this model of governance constitutes the most fundamental obstacle to the Kremlin's project of unchecked online domination. From that perspective, Russia's "internet sovereignty" law, passed in April 2019, should be understood as a rhetorical move designed to market Moscow's plan to dismantle this multi-stakeholder model and replace it with a state-centric, UN-like multilateral form of governance. To attain this goal, a mafia-like "pyromaniac firefighter" strategy has been established by Moscow: create the problem and present its own plans as the only solution. In this case, absolute state sovereignty in the digital sphere is depicted as the only solution to Russia's own campaigns of digital interference.[99] Indeed, the Kremlin's actions are precisely what the "internet sovereignty" law purports to prevent. The aim is to influence the perceptions and expectations of various international stakeholders in the same direction and make Moscow's call for state-centric internet governance more appealing to liberal democracies. However, such a change in the governance of the internet sought by Russia would result in shifting the digital balance of power towards authoritarian states by destroying the emancipatory effects of the free internet on states, organisations, businesses and individuals.

[99] Government of the Russian Federation, "Federal'nyi zakon ot 01.05.2019 no 90-F3 o vnecenii izmenenii v Federal'nyi zakon 'O Svyazi' I Federal'nyi Zakon 'Ob Informatsii, informatsionikh tekhnologiakh I o zashitie informatsii'" (Federal Law of 1 May 2019 no 90-F3 for the introduction of changes to the Federal Law "on Communication" and the Federal Law "on information, information technologies and the protection of information"), 1 May 2019 (accessed 7 August 2019).

About the Author

Antonin Plattner holds a Bachelor's degree in history and Russian studies from the University of Geneva. He is currently following the International Master's programme in Security, Intelligence and Strategic Studies (IMSISS)—an Erasmus Mundus joint degree programme between the University of Glasgow, Dublin City University and Charles University (Prague, Czechia). Following the cooperation agreement between the University of Glasgow and ICDS in the framework of the IMSISS, Antonin worked as an ICDS research intern during the summer of 2019. He specialises in the fields of digital technologies and international security.

Follow us on:

ICDS.Tallinn
@ICDS_Tallinn
ICDS-Tallinn

International Centre for Defence and Security
63/4 Narva Rd., 10152 Tallinn, Estonia
info@icds.ee, www.icds.ee

ISSN 2228-2076