CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Security Studies

Master's Thesis

2022 **Adam Novák**

CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Security Studies

Internet Governance in Putin's Russia – a long-term perspective

Author: Adam Novák

Study programme: Security Studies

Supervisor: Mgr. Anzhelika Solovyeva

Year of the defence: 2022

Declaration

1. I hereby declare that I have compiled this thesis using the listed literature and resources only.
2. I hereby declare that my thesis has not been used to gain any other academic title.
3. I fully agree to my work being used for study and scientific purposes.

In Prague on 21st August 2022

Adam Novák

References

NOVÁK, Adam. *Internet Governance in Putin's Russia – A Long-Term Perspective.* Praha, 2022. 103 pages. Master's thesis (Mgr.). Charles University, Faculty of Social Sciences, Institute of Political Science. Department of Security Studies. Supervisor Mgr. Anzhelika Solovyeva

Length of the thesis: 239 498

Abstract

This longitudinal case study is dedicated to the analysis of the development behind Russia's approach to Internet governance. By qualitatively researching the development of the Kremlin's approach to Internet governance, this thesis aims to capture the learning process behind regulating the cyberspace in Russia. As such, the aim is to understand what kind of events have shaped its perception of how Internet and the underpinning infrastructure should be approached to increase the regime's stability. Building on the concepts of digital authoritarianism and authoritarian learning and by understanding learning as a long-term process with turning points, this thesis aims to answer these research questions. How does Russia's digital authoritarianism manifest? Which events, both domestic and international, hastened the pace and intensity of cyberspace regulation in Russia? Can we identify a learning process behind Russia's long-term approach towards Internet regulation? For these ends, the turning points refer to events after which we can identify a change in the perception of Internet governance and/or intensification in controlling the online information space. As such, with the help of periodization, the thesis traces the evolution of Russia's digital authoritarianism across events such as Putin's rise to power, colour revolutions, the Arab Spring and the 2011 mass protests in Moscow, Snowden's revelations about mass surveillance in the US, Euromaidan and the annexation of Crimea, and Russia's 2022 invasion of Ukraine. While some events represented a serious red flag for the Kremlin's stability and prompted Russia to change its approach to Internet governance, some represented rather a rhetorical justification for such a change. Even though Russia's approach has for a long term been characterised as decentralised, the results of this research have identified a recent trend towards centralisation.

Abstrakt

Tato longitudinální případová studie analyzuje vývoj přístupu Putinova Ruska k řízení internetu. Kvalitativní charakter zkoumání vývoje přístupu Kremlu k řízení internetu si klade za cíl zachytit proces učení, který stojí za regulací kyberprostoru v Rusku. Cílem je pochopit, jaké události formovaly vnímání Kremlu toho, jak by se mělo přistupovat k internetu a podpůrné infrastruktuře za účelem zvýšení stability režimu. Na základě konceptů digitálního autoritářství a autoritářského učení, které je považováno za dlouhodobý proces se zlomovými body si tato práce klade za cíl odpovědět na tyto výzkumné otázky. Jak se projevuje ruské digitální autoritářství? Které domácí

a mezinárodní události urychlily tempo a intenzitu regulace kyberprostoru v Rusku? Dá se za ruským dlouhodobým přístupem k regulaci internetu identifikovat proces učení? Pro tyto účely reprezentují výše zmíněné zlomové body události, po kterých se dá identifikovat změna vnímání řízení internetu a/nebo zintenzivnění kontroly online informačního prostoru. S pomocí periodizace tak práce sleduje vývoj ruského digitálního autoritářství napříč událostmi jako je Putinův nástup k moci, barevné revoluce, arabské jaro, masové protesty v Moskvě v roce 2011, Snowdenova odhalení masového tajného sledování v USA, Euromaidan a anexe Krymu, anebo ruská invaze na Ukrajinu v roce 2022. Zatímco některé události představovaly vážnou výstrahu pro stabilitu Kremlu a přiměly Rusko ke změně přístupu k řízení internetu, některé představovaly spíše rétorické ospravedlnění takové změny. Přestože byl ruský přístup dlouhodobě charakterizován jako decentralizovaný, výsledky tohoto výzkumu identifikovaly nedávný trend k centralizaci.

Keywords

cyberspace, Putin, internet governance, authoritarian learning, Russia, digital authoritarianism

Klíčová slova

kyberprostor, Putin, řízení internetu, autoritářské učení, Rusko, digitální autoritářství

Název práce

Řízení Internetu v Putinově Rusku – dlouhodobá perspektiva

Acknowledgement

I would like to express my deepest gratitude and appreciation for all the comments and support that I have received from my academic supervisor, Mgr. Anzhelika Solovyeva, throughout the process of writing this project.

I am also very grateful to my parents for all their continuous support throughout my university studies.

Table of Contents

Introduction 9
1. Literature review 12
2. Conceptual framework 14
2.1 Internet governance 14
2.2 Digital authoritarianism 18
2.2.1 Offline – online nexus 22
2.3 Policy diffusion, learning, authoritarian learning 24
3. Methodology 28
4. Empirical analysis 30
4.1 Origins of the Runet and Putin's rise to power 30
4.2 Colour revolutions, sovereign democracy, and Putin-Medvedev tandem (2004 – 2011) 36
4.3 Arab Spring and mass protests in Moscow (2011 – 2013) 41
4.4 Snowden, Euromaidan, and the annexation of Crimea (2013 – 2021) 52
4.5 Russia's invasion of Ukraine 76
Conclusion 85
Bibliography 93

Introduction

The Internet started to grow significantly in mid-1990s to the extent that 1995 is often referred to as the Internet's "year zero" and by the end of the millennium, the global community was becoming aware of its economic relevance.[1] The more both the governments and the private sector began to be conscious about the significance of global networks, the more apparent the necessity for Internet governance began to be as well. In 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) was created in order to, among other things, manage the Domain Name System.[2] As such, it has played a central role in Internet governance and challenged the authority of existing organisations like the International Telecommunication Union (ITU). It was created as a private NGO that operated in accordance with the Memorandum of Understanding with the US Department of Commerce under the Californian law.[3] At that time, no country showed a particular interest in this organization apart from the USA, Australia, and the EU.[4] However, with the increasing importance of digital technology during the early 2000s, more countries began to show their interest in Internet governance and began to call for ICANN to reflect more of its global reach and capacity. Most problematically, ICANN is not a subject of international law and therefore does not bear any international legal responsibility. This, together with the fact that the US never took on any international responsibility for the sustainability of the Internet makes the stability of systems in the information communication technology milieu contingent on the political setting in particular states.[5]

Therefore, the US played the most significant role in the development of the Internet and thus its governance regime has been reflecting the multi-stakeholder model under the American leadership.[6] In the early 1990s, in the context of Cold War and the triumph of market economies, deregulation in telecommunications, anti-authoritarian and anti-government beliefs that many

[1] Hannes Ebert and Tim Maurer, "Contested Cyberspace and Rising Powers," *Third World Quarterly* 34, no. 6 (2013): 1054–74., p. 1059
[2] Tang Lan, "International Governance of/in Cyberspace," in *Routledge Handbook of International Cybersecurity*, ed. Eneken Tikk and Mika Kerttunen (New York: Routledge, 2020), 79–93., p. 79
[3] Carol M. Glen, "Internet Governance: Territorializing Cyberspace?," *Politics & Policy* 42, no. 5 (2014): 635–57., p. 641
[4] Ebert and Maurer, "Contested Cyberspace and Rising Powers.", p. 1061
[5] Andrei V. Krutskikh and Anatoli A. Streltsvo, "International Information Security - Problems and Ways of Solving Them," in *Routledge Handbook of International Cybersecurity*, ed. Eneken Tikk and Mika Kerttunen (New York: Routledge, 2020), 260–68., p. 261
[6] Ebert and Maurer, "Contested Cyberspace and Rising Powers.", p. 1054

Internet initiate countries held, the US government opened the Internet to the public and pushed for minimal governmental role in favour of the private sector.[7] Ideally, the multistakeholder-model includes governments, private companies as well as NGOs with no hierarchy in between them.[8] Indeed, it was the US who set the precedent for deregulated Internet governance, and because the Internet became the vehicle of economic development in the evolving global economy in which national borders and sovereignty were less relevant, many countries have chosen to follow the same path out of the fear that government infringement would put them to a secondary economic position.[9]

At the same time, apart from being a vehicle of economic development, there was an initial euphoria that by facilitating horizontal networks and exchange of information across the globe, the Internet would empower activist and challenge authoritarian style of governance. However, with the course of time, scholars have become increasingly preoccupied that the same technologies can empower autocrats and lead to increased governmental control over the online public sphere and therefore supress oppositional movements by either monitoring the activity of regime's dissent or by manipulating and censoring information on the Internet. In the last decade, digital surveillance has been on the rise in authoritarian regimes as compared to democracies who saw some retreat in surveillance due to international scandals caused by revelations by Edward Snowden[10] or Cambridge Analytica. As such, authoritarian regimes relying on mass digital surveillance are often referred to as digital authoritarianism. While the most well-known example of such regime is China, scholars have increasingly started to analyse Russia along the same lines.

Thinking about Internet governance in Russia, we can go back to the beginning of 1990s when the first Russian connections to the global Internet were made, and the Internet service provider (ISP) market started to develop. It was already in the first years of Putin's presidency, when his government proclaimed the importance of cyberspace along the lines of national security in the Doctrine for Information Security adopted in September 2000. Democracy promotion policies were only partially successful in Russia and the various NGOs arguing for them were soon to be perceived as "foreign elements" in the Russian state. They were generally understood as a tool to

[7] James A. Lewis, "Sovereignty and the Role of Government in Cyberspace," *The Brown Journal of World Affairs* 16, no. 2 (2010): 55–65., p. 56
[8] Ebert and Maurer, "Contested Cyberspace and Rising Powers.", p. 1057
[9] Lewis, "Sovereignty and the Role of Government in Cyberspace.", p. 56
[10] Xu Xu, "To Repress or to Co-Opt? Authoritarian Control in the Age of Digital Surveillance," *American Journal of Political Science* 65, no. 2 (2021): 309–25., p. 309

undermine Russia's position in the international arena to the benefit of the US and the West in general. Gradually, this narrative continued and spread into the online environment. Just as Russia started to be worried about a global order dominated by Western institutions, it also became worried about cyberspace dominated by the same institutions due to the historical development of Internet infrastructure and predominating character of global Internet governance as mentioned above.

This logic of foreign actors operating inside Russia is increasingly being replicated also in the Russian cyberspace where foreign elements are either blocked or confronted with counter-information. Elsewhere, Arab Spring has further demonstrated the possible danger that cyberspace represents for authoritarian governments by its ability to stark popular unrest, further motivating authoritarian governments to confront and adjust information that appears in their online environment. Gradually, being aware of these trends, Russia has called for digital sovereignty and highlighted the importance of national media sphere, national critical infrastructure, and national Internet.[11]

This thesis will analyse the development of Russia's approach towards regulating the online environment from a long-term perspective. For this, I will analyse the evolution of Russia's cyberspace regulation since the beginning of 1990s, throughout Putin's rule, until the current invasion of Ukraine. Additionally, I attempt to periodise this time frame with respect to important turning points and see if and how these turning points contributed to Russia's learning process behind using Internet governance for the sake of regime stability.

For these ends, I ask myself these research questions. *How does Russia's digital authoritarianism manifest? Which events, both domestic and international, hastened the pace and intensity of cyberspace regulation in Russia? Can we identify a learning process behind Russia's long-term approach towards Internet regulation?*

[11] Mika Kerttunen and Eneken Tikk, "The Politics of Stability: Cement and Change in Cyber Affairs," in *Routledge Handbook of International Cybersecurity*, ed. Mika Kerttunen and Eneken Tikk (New York: Routledge, 2020), 52–64., p. 56

1. Literature review

The concept of digital authoritarianism in Russia has been investigated in the academia only to a limited extent. Often, it has been compared to the state of digital authoritarianism in China and its implications for societal control and regime stability. As such, Henry and Howells argued that Russia's variation is less comprehensive and consistent, but potentially more easily exportable to other polities.[12] Similarly, in their policy brief, Polyakova and Meserole compare the exportability of China's and Russia's model of digital authoritarianism while concluding that the one of Russia's is more easily transferable due to its predominant reliance on "repressive legal regime".[13]

Other scholars were examining how and to which countries this style of governance, and the underpinning technology, is being exported by these two powers. Morgus concluded, that besides normative initiatives among international organisations, there is a little evidence of their mutual cooperation in spreading this style of governance – while, in theory, there are reasons to suggest a cooperation in this regard, they also compete with each other in supplying the underpinning technology to strategically important markets (e.g. the Central Asian Republics).[14] In another instance, Weber has found that China exports information controls more easily to countries affiliated with the Belt and Road Initiative, whereas Russia enjoys favourable position in the Commonwealth of Independent States.[15]

In 1999, Carothers discussed a learning curve regarding Western policies of democracy promotion.[16] After the colour revolutions in Russia's near abroad were aided by such policies, Larry Diamond shared his preoccupations in 2005 that due to colour revolutions, authoritarian regimes were becoming more repressive and called for the necessity to deal with authoritarian

[12] Laura A. Henry and Laura Howells, "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet Governance," *Communist and Post-Communist Studies* 54, no. 4 (2021): 1–27.
[13] Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," Policy Brief, Democracy & Disorder (The Brookings Institution, 2019).
[14] Robert Morgus, "The Spread of Russia's Digital Authoritarianism," Artificial Intelligence, China, Russia, and the Global Order (Air University Press, 2019)., p. 95
[15] Valentin Weber, "The Worldwide Web of Chinese and Russian Information Controls" (Centre for Technology and Global Affairs, 2019).
[16] Thomas Carothers, *Aiding Democracy Abroad : The Learning Curve* (Washington DC.: Carnegie Endowment for International Peace, 1999).

learning.[17] Some scholars have heard his call. In 2010, Thomas Ambrosio, tried to outline a framework of "authoritarian diffusion" and contended that the concept of policy diffusion that is related to learning, indeed has become to be studied more extensively after colour revolutions as the political dynamics "in one country appeared to affect those in another".[18]

For some, the series of Arab uprising represented another incentive to investigate this phenomenon. Similarly, as with the colour revolutions, scholars were interested in what kind of tactics and/or policies were the governments replicating in order to accommodate the protests or limit their protest action. Heydemann and Leenders concluded that the authoritarian incumbents in countries like Algeria, Morocco or Jordan learned from the events and factors that helped to overthrow the governments of Egypt, Tunisia, or Libya (this included for example financial motivation for both armed forces and constituencies, raising stakes for citizens' participation in mass unrest, or gather support from regional counter-revolutionary allies).[19] Scholars were also interested in how China and Russia responded to these popular unrests. Bunce and Koesel argued that both China and Russia increased their "diffusion-proofing" mechanism after both Arab Spring and colour revolutions while recognising that "diffusion is no illusion".[20]

While there have been studies on digital authoritarianism and/or authoritarian learning, they were aimed in other direction. Studies of authoritarian learning did not focus specifically on Russia, nor were they aimed in the direction of cyberspace regulation and studies of Russian digital authoritarianism were not based on longitudinal research. More so, I have not found a single study that would connect digital authoritarianism with authoritarian learning. By providing a longitudinal study of Russia's approach to Internet governance, I am to capture the learning process behind the development of Russia's digital authoritarianism and thus contribute to the literature on authoritarian learning from the long-term perspective.

[17] Larry Diamond, Authoritarian Learning: Lessons from the Coloured Revolutions, interview by Kenta Tsuda and Barron YoungSmith, Brown Journal of World Affairs, 2006.
[18] Thomas Ambrosio, "Constructing a Framework of Authoritarian Diffusion: Concepts, Dynamics, and Future Research," *International Studies Perspective* 11 (2010): 375–92., p. 376
[19] Steven Heydemann and Reinoud Leenders, "Authoritarian Learning and Authoritarian Resilience: Regime Responses to the 'Arab Awakening,'" *Globalizations* 8, no. 5 (2011): 647–53.
[20] Karrie J. Koesel and Valerie J. Bunce, "Diffusion-Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations against Authoritarian Rulers," *Perspectives on Politics* 11, no. 3 (2013): 753–68.

2. Conceptual framework

This section introduces core concepts that are going to be analysed in this paper. First, I discuss the international context and development that has been shaping Russian perception of internet governance and information security. The aim is not to provide an exhausting review of Internet governance literature, but rather to explain what the debate about international cyberspace regulation has been about and what are the main approaches that have been shaping Internet governance and in what sense does the Russian approach differ compared to the one preferred by the Western countries. Second, I discuss the notion of digital authoritarianism and how it is relevant to Russia while acknowledging the fact that there is a connection between offline and online authoritarian practice – the so called offline-online nexus. Third, I focus on my understanding of (authoritarian) learning and how it will be traced in this thesis.

2.1 Internet governance

Initially, the general assumptions behind Internet governance revolved around the conviction that due to the decentralised nature of the Internet, it would be difficult to regulate it by governments.[21] Moreover, one of the fundamental principles underlying the basis of the Internet in its initial phases of development was network neutrality defined as the "right of users to access content, services and applications on the Internet without interference from network operators or government", together with the "right of network operators to be reasonably free of liability for transmitting content and applications deemed illegal or undesirable by third parties".[22] Importantly, building on these principles was made possible due to the approach of the US and other Western states who adhered to these norms and adopted policy decision in the 1990s that kept Internet governance institutions out of their direct control.[23] Gradually, however, these principles characterising the Internet as "open commons"[24] began to be challenged which is something I turn to now.

[21] Ronald J. Deibert and Masashi Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls," *Global Governance* 18 (2012): 339–61., p. 341
[22] Deibert and Crete-Nishihata., p. 342
[23] Deibert and Crete-Nishihata., p. 342
[24] Glen, "Internet Governance: Territorializing Cyberspace?", p. 644

On the global level, the discussion about internet governance has been revolving around the question whether its model should be based on decentralisation with many stakeholders involved or whether it should represent a multilateral model based on centralisation. Flonk et al. argue that defenders of the former belong to the liberal sphere (Western states), whereas the defenders of the latter belong to the sovereigntist sphere (China, Russia, and others) and as such, represent distinct spheres of authority that argue for "normative orders about common goods".[25]

Some scholars offer three options. According to Ebert and Maurer, there have been two more approaches to internet governance besides the multistakeholder model argued for by the USA – those are "intergovernmental" and "sovereigntist" models. The former one seeks to limit US dominance by shifting authority to an International Governmental Organisation "in order to embed the US power in rules and institutions that channel and limit the ways that power is exercised".[26] The latter strives to control cyberspace in a more traditional sense by invoking a Westphalian idea of sovereignty with the help of a multilateral organisation such as the International Telecommunication Union (ITU)[27] where states cooperate in decision-making in order to create "international communications and telecommunication policies".[28] Similarly, Glen introduces three archetypes as well. The first - open multistakeholder model – includes only "limited regulation, freedom of expression, and free market interests" and goes along the lines of the initial research of the US Department of Defense that conceptualised the Internet as "open commons" in which innovation and freedom of expression would thrive.[29] The second – repressive multilateral model – includes governments utilizing the Internet to foster domestic security and argue for more internationalised approach to Internet governance.[30] Likewise, the third – open multilateral model – includes those who argue for more internationalised approach, but without the primary stimulus of domestic control, while their main concern is accountability in Internet governance.[31]

[25] Daniëlle Flonk, Markus Jachtenfuchs, and Anke S. Obendiek, "Authority Conlifcts in Internet Governance: Liberals vs. Sovereignists?," *Global Constitutionalism* 9, no. 2 (2020): 364–86., p. 366
[26] Ebert and Maurer, "Contested Cyberspace and Rising Powers.", p. 1059-1060
[27] Ebert and Maurer., p. 1060
[28] Glen, "Internet Governance: Territorializing Cyberspace?", p. 637
[29] Glen., p. 643-644
[30] Glen., p. 646
[31] Glen., p. 648

The liberal sphere and the (open)multistakeholder model perceive the Internet as an opportunity space that ought to be self-regulated based on voluntary participation and expertise. States should play a minimal role as opposed to individuals, companies and civil society who should enjoy a considerable amount of freedom to lead the development of the Internet.[32] The sovereigntist sphere, and the repressive multilateral model perceive the Internet rather as a threat. States should govern the Internet by intergovernmental institutions while respecting national sovereignty by limiting the third sector to have only advisory role, if any.[33]

As such, authoritarian regimes who argue for sovereigntist principles under the repressive multilateral model hope to reflect their national policies in the international bodies. This involves collaboration with other agreeable governments and making intergovernmental institutions (where they enjoy the most influence) responsible for Internet governance to limit the voices of the third sector.[34] In other words, they consider international organisation and institutions as tools for nationalisation.[35]

In 2003, the first World Summit on the Information Society (WSIS) convened which was characterised by some as a start of "the battle over the soul of the Internet".[36] It included both democratic and non-democratic governments that felt the necessity to voice their preferences regarding the global Internet governance regime. It was here where the sovereigntist sphere argued for strengthening the role of the ITU[37] according to the multilateral approach. Gradually it made its way into the diplomatic agenda and in 2005, during the second WSIS in Tunis, Internet governance was defined by the United Nations as "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet".[38] Overall, both of these summits pushed forward the bottom-up multistakeholder model of global Internet governance,[39] highlighting the "important roles of private sector and civil

[32] Flonk, Jachtenfuchs, and Obendiek, "Authority Conlifcts in Internet Governance: Liberals vs. Sovereignists?", p. 366
[33] Flonk, Jachtenfuchs, and Obendiek., p. 366
[34] Glen, "Internet Governance: Territorializing Cyberspace?", p. 646
[35] Deibert and Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls.", p. 348
[36] Ebert and Maurer, "Contested Cyberspace and Rising Powers.", p. 1062
[37] Ibid.
[38] Lan, "International Governance of/in Cyberspace.", p. 80 and also Ebert and Maurer, p. 1058
[39] Glen, "Internet Governance: Territorializing Cyberspace?", p. 642

society", while also contending that "policy authority for Internet-related public policy issues is the sovereign right of States'".[40]

It was in 2012 during the World Conference of International Telecommunications (WCIT) when various opposing ideas regarding Internet governance clashed. Put simply, the clash was among governments that cherished freedom of expression, and those who sought to utilize the Internet for censorship and population control.[41] The conference was organised by the ITU and the main rationale behind it was to update International Telecommunication Regulations (ITRs) treaty from 1998 to reflect on the emerging menace of cyberwarfare and cybercrime. The resulting revision proved to be highly controversial and effectively divided the participants along the lines of liberal and sovereigntist approaches. Whereas the liberals preferred to maintain the limited role of ITU, the sovereigntists wanted to make ITU the preferred body in terms of Internet regulation instead of the UN and thus effectively arguing for the replacement of the multistakeholder model preferred by the liberal sphere.[42] As the Internet turned out to be a crucial telecommunications medium, the ITU gained on importance in relation to the debate about the Internet governance. Depending on the country's position towards internet governance mentioned earlier, the intergovernmental structure of the ITU either sparked hopes or fears that the multistakeholder approach would be replaced with a multilateral one by giving the ITU the ability to manage the Internet.[43] The main argument of sovereigntists states such as Russia is, that the present multistakeholder Internet governance regime is too meddlesome into legitimate internal affairs of states.[44]

Russian opposition to American dominant role in cyberspace governance is visible also on the level of rhetoric and terminology. In 1998, then Russian foreign minister Igor Ivanov, proposed a draft resolution regarding "the use of information technologies for purposes incompatible with missions of ensuring international stability and security".[45] Since then, Russia has been arguing for the prohibition of "information aggression" at the levels of the UN which Deibert and Crete-

[40] Flonk, Jachtenfuchs, and Obendiek, "Authority Conlifcts in Internet Governance: Liberals vs. Sovereignists?", p. 373
[41] Glen, "Internet Governance: Territorializing Cyberspace?", p. 643
[42] Flonk, Jachtenfuchs, and Obendiek, "Authority Conlifcts in Internet Governance: Liberals vs. Sovereignists?", p. 374
[43] Glen, "Internet Governance: Territorializing Cyberspace?", p. 637
[44] Flonk, Jachtenfuchs, and Obendiek, "Authority Conlifcts in Internet Governance: Liberals vs. Sovereignists?", p. 381
[45] Ebert and Maurer, "Contested Cyberspace and Rising Powers.", p. 1065-1066

Nishihata interpret as "ideological attempts, or the use of ideas, to undermine regime stability".[46] According to the Russian information concept from September 2000, information security implies the "protection of its national interests in the information sphere defined by the totality of balanced interests of the individual, society, and the state" while int the US diplomatic circles, "cyber-security" directly rules out content control.[47]

Because of this rhetorical competition, information security entered the human rights debate and ceased to be a purely (cyber)security issue. It started to represent an issue of contention among these two spheres. Ebert and Maurer argue that Western states understand information security as a "Trojan horse for content control and censorship" by countries like China and Russia.[48] However, from the point of view of China and Russia, this argument can be reversed along the lines that the multi-stakeholder model of internet governance includes various advocacy groups and human rights NGOs that penetrate their sovereignty and act like Trojan horses for the Western states and their interests. While Lan argues that the top-down logic of "state sovereignty as the basis of power cannot be replicated in cyberspace"[49], we can see that it is precisely this logic that some countries, including Russia, are trying to replicate and argue for in the international arena. As China and Russia seem to share this perception of cyberspace and because China is being discussed through the lenses of digital authoritarianism frequently, it makes sense to be examining Russia along the same lines. Therefore, I am now proceeding to the discussion of the concept of digital authoritarianism.

2.2 Digital authoritarianism

After introducing the debate about international internet governance and cyberspace regulation, it is time to investigate what can governments do in order to regulate internet and/or cyberspace as a whole at home. Discussing digital authoritarianism allows me to integrate cyberspace control into the general discussion about international internet governance and authoritarian learning. In other words, in these paragraphs, I will explain, what does the so-called

[46] Deibert and Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls.", p. 346
[47] Ebert and Maurer, "Contested Cyberspace and Rising Powers.", p. 1066
[48] Ebert and Maurer., p. 1055
[49] Lan, "International Governance of/in Cyberspace.", p. 89

digital authoritarianism incorporate and how it can be connected to the concept of authoritarian learning that is discussed in the next subchapter.

While it is true that digital technology can help societies and individuals to oppose oppressive regimes, it can also provide governments with tools to observe and follow regime opponents, giving the government the capability to subdue organised dissent.[50] Indeed, the technologies that were perceived by many as instruments for emancipation are increasingly used to counter dissent and limit the activities of civil society.[51] In order to capture this logic, Tiberiu and Lupu argue for focusing on preventive repression that is defined as "the set of activities governments use to reduce the risk that opposition groups threaten government's power, including opposition effort to mobilize and organise public dissent".[52] Striving to achieve a strategic upper hand for the regime, governments adopt "technological, legal, extralegal, and other targeted information controls", and, as already indicated, cooperate regionally or bilaterally to promote authoritarian-friendly norms.[53]

Considering the extent of cyberspace regulation in various countries, scholars tried to categorise individual countries into the so called three generations of cyberspace controls. The first generation of controls encompasses physical filtering via national firewalls installed at key Internet choke points as in the case of China.[54] The second generation of controls encompasses the initiative for legal and normative regime that specifies under which conditions access to information resources can be denied.[55] It also includes features of hidden surveillance, censorship and disguised functionalities that governments demand for manufactures and service providers to install into their products under the threat of taking away their licence.[56] Such transfer of responsibility is known as intermediary liability and includes legal obligations to archive user data and share it with government agencies if required, often without the need for legal warrant.[57] Finally, the third generation of controls represents a multidimensional approach to build capabilities in order to

[50] Tiberiu Dragu and Yonatan Lupu, "Digital Authoritarianism and the Future of Human Rights," *International Organization* 75 (2021): 991–1017., p. 992
[51] Ronald J. Deibert, "Authoritarianism Goes Global: Cyberspace Under Siege," *Journal of Democracy* 26, no. 3 (2015): 64–78., p. 64
[52] Dragu and Lupu, "Digital Authoritarianism and the Future of Human Rights.", p. 993
[53] Deibert, "Authoritarianism Goes Global: Cyberspace Under Siege.", p. 64-65
[54] Ronald J. Deibert et al., eds., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (London: The MIT Press, 2010)., p. 4
[55] Ronald J. Deibert and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," in *Access Controlled: The Shaping of Power, RIghts, and Rule in Cyberspace* (London: The MIT Press, 2010), 15–33., p. 24
[56] Deibert, "Authoritarianism Goes Global: Cyberspace Under Siege.", p. 67
[57] Deibert and Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls.", p. 344

confront and compete with potential foes in informational space. The focus is less on denying access itself, but rather to create an uncertain informational environment by flooding information sphere with counterinformation that "overwhelm, discredit, or demoralise opponents, (…) including warrantless monitoring of Internet users and usage.[58] This approach is mostly offensive in character and includes "surveillance, targeted espionage, and other types of covert disruptions".[59] As I will trace the process of authoritarian learning, I will be assessing whether Russia's approach to cyberspace regulation has been moving across these generations.

Polyakova and Meserole define digital authoritarianism as "the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations".[60] Yaykobe and Brannen define digital authoritarianism as "the use of the Internet and related digital technologies (…) to decrease trust in public institutions, increase social and political control, and/or undermine civil liberties" whereas the goal is to form the society according to the respective authoritarian image.[61]

As already mentioned, digital surveillance is the crucial activity that underpins digital authoritarianism. In this regard, however, authoritarian regimes are not alone. A study conducted in 2011 by Howard, Agarwal and Hussain even found that since 1995 democracies have interfered with networks overall more than authoritarian regimes, although with less frequency. At the same time, they argue that after 2002, authoritarian regimes started to use network interference as a governance instrument.[62] In Xu's comparison to US surveillance though (that predominantly concentrates on international communications), authoritarian regimes principally focus on activity within its borders.[63] According to him, digital surveillance allows authoritarian leaders to address the vertical information problem by replacing large scale repression and/or co-optation with more accurate, targeted and/or preventive repression.[64] As this thesis analyses the implications of cyberspace regulation for regime stability, the focus will be mainly on the domestic situation. This however does not mean that Russia would not draw lessons from the international environment.

[58] Deibert and Rohozinski, "Control and Subversion in Russian Cyberspace.", p. 27
[59] Deibert, "Authoritarianism Goes Global: Cyberspace Under Siege.", p. 68
[60] Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models."
[61] Erol Yayboke and Sam Brannen, "Promote and Build: A Strategic Approach to Digital Authoritarianism," Policy Brief (Center for Strategic and International Studies, October 2020)., p. 2
[62] Philip N. Howard, Sheetal D. Agarwal, and Muzammil M. Hussain, "The Dictator's Digital Dilemma: When Do States Disconnect Their Digital Networks?," *Issues in Technology Innovation* 13 (2011): 1–11., p. 2
[63] Xu, "To Repress or to Co-Opt? Authoritarian Control in the Age of Digital Surveillance.", p. 309
[64] Xu., p. 310

On the contrary. While Russian international initiatives regarding cyberspace regulation will be mentioned as well, the reason behind this is to demonstrate that such initiatives serve a self-interested venture that seeks to normalise its domestic practice.

Most typically, governments meddle into digital networks to defend political authority, political leaders and institutions, dealing with election crisis, countering propaganda and dissent, and to protect national security.[65] Initiatives to counter propaganda are usually aimed towards information that undercut the regime position.[66] Election times are also very threating to authoritarian rule and thus prone to digital network interference either before, while, or after elections took place.[67] This is related mainly to the third generation of cyberspace controls that are usually time sensitive and occur during significant political events such as already mentioned elections, but also anniversaries or public manifestations. These "just-in-time disruptions can be as severe as total Internet blackouts".[68]

Moreover, governments can interfere also under the pretext to protect cultural and moral character of the given country in light of profane or offensive information.[69] Like countering propaganda, this category is problematic mainly because of the possibility to be interpreted broadly in order to repress dissent. By using these strategies, authoritarian regimes are contributing to something that Deibert and Crete-Nishihata labeled as "norm regression in global governance" – a practice that "degrade cyberspace as open commons of information and communication"[70] as it was initially conceptualised by the founders of the Internet. In their view, information controls refer to an activity that seeks to "deny, disrupt, manipulate, and shape information and communications for strategic and political ends" through technology or other regulatory measures such as laws or policies. This includes "media regulation, licensing regimes, content removal, libel and slander laws, and content filtering".[71]

[65] Howard, Agarwal, and Hussain, "The Dictator's Digital Dilemma: When Do States Disconnect Their Digital Networks?", p. 6, 7
[66] Howard, Agarwal, and Hussain., p. 7
[67] Howard, Agarwal, and Hussain., p. 7
[68] Deibert, "Authoritarianism Goes Global: Cyberspace Under Siege.", p. 69
[69] Howard, Agarwal, and Hussain, "The Dictator's Digital Dilemma: When Do States Disconnect Their Digital Networks?", p. 7
[70] Deibert and Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls.", p. 341
[71] Deibert and Crete-Nishihata., p. 343

As already mentioned, China is often presented as the most developed case of digital authoritarianism. Another reason why applying the concept of digital authoritarianism to Russia is relevant is because the 2018 Freedom of the Net report 'The Rise of Digital Authoritarianism' had discovered that Russian media elites and government officials were invited to China to take part in "weeks-long seminars on new media or information management."[72]

2.2.1 Offline – online nexus

Digital media, together with social networks, have altered the manner for dissent to organise. Social movements have been organising and coordinating collective action increasingly online not only to initiate local protest but also to connect with international social movements, and/or share their political grievances with international media.[73] With the citizens' more increasing reliance on digital communication technology, the ability of authoritarian leaders to gauge dissent in real time before it spreads increases as well. Governments can, under certain circumstances, access and investigate citizens' digital footprints because their digital communication is facilitated by information and communication technology (ICT).[74] Such practice allows to identify radical dissent and then "stop it through harassment, intimidation, or detention", allowing to maintain the stability of the regime at lower cost without the need for large scale co-optation.[75]

While writing about the way authoritarian governments use cyberspace control for the sake of regime stability, it is important to keep in mind, that it is a continuation of offline authoritarian practices. Therefore, the idea behind dealing with cyberspace and the internet milieu is to see how Putin's Russia adapted its strategy in light of new possibilities for dissent to form and organise and *learned* how to increase the resilience of its regime in the digital age and thus contribute to its stability.

The rise of digital technology has created dilemmas not only for authoritarian regimes. Lan argues that phenomena such as rivalry among state and non-state actors, or growth of digital economy at the expense of political security, have influenced the character of global network

[72] Adrian Shahbaz, "The Rise of Digital Authoritarianism," Freedom on the Net (Freedom House, 2018)., p. 9
[73] Howard, Agarwal, and Hussain, "The Dictator's Digital Dilemma: When Do States Disconnect Their Digital Networks?", p. 3
[74] Xu, "To Repress or to Co-Opt? Authoritarian Control in the Age of Digital Surveillance.", p. 310
[75] Xu., p. 310, 312

governance.[76] However, authoritarian regimes such as Russia are structurally opposed to the empowerment of non-governmental actors that could compromise their regime stability[77] precisely because of they perceive them as Trojan horses pursuing policy goals of the West. I hypothesize that cyberspace regulation in Russia represent a continuation of Russia's repressive policies against the "foreign elements" inside of Russia's political discourse and/or civil society such as NGOs who receive foreign funding. In that way, the cyberspace regulation would only represent a logical continuation of managing the (digital) public sphere for the sake of regime security that goes along the lines of offline-online nexus

Cyberspace as a whole has evolved into a crucial strategic space for governments and there is a consensus that besides Internet technology, it comprises of network infrastructure, and human behaviour and relationships.[78] Therefore, it represents a human-made environment with changeable parameters[79] that is predominantly owned by private actors who operate associated infrastructure and services[80] in diverse jurisdictions.[81] Because of this, it is feasible to separate a country and its citizens from the Internet in order to "protect" it from foreign influence.[82] While the concept of cyberspace, in theory, could function a sort of borderless global commons, according to Lewis, this understanding is no more than an illusion as the concept affects national, as well as international security, and argues such understanding of cyberspace is unsustainable precisely because of the fact that governments are interested in controlling it.[83] Therefore, even though there are scholars, such as Lan, who argue that the top-down logic of "state sovereignty as the basis of power cannot be replicated in cyberspace"[84], we can see that it is precisely this logic that some countries, including Russia, are trying to replicate and argue for in the international arena. It is this logic of seeing the digital milieu as an "extension of sovereign territory"[85] that supports the logic of the notion offline-online nexus.

[76] Lan, "International Governance of/in Cyberspace.", p. 79
[77] Ebert and Maurer, "Contested Cyberspace and Rising Powers.", p. 1063
[78] Lan, "International Governance of/in Cyberspace.", p. 80
[79] Ebert and Maurer, "Contested Cyberspace and Rising Powers.", p. 1056
[80] Deibert and Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls.", p. 340-341
[81] Krutskikh and Streltsvo, "International Information Security - Problems and Ways of Solving Them.", p. 261
[82] Kerttunen and Tikk, "The Politics of Stability: Cement and Change in Cyber Affairs.", p. 59
[83] Lewis, "Sovereignty and the Role of Government in Cyberspace.", p. 56
[84] Lan, "International Governance of/in Cyberspace.", p. 89
[85] Henry and Howells, "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet Governance.", p. 3

This is possible not only because of the man-made, privately owned technological infrastructure but also because of the human aspect of its users that can orchestrate targeted information operations in order to shape and counter information to the benefit of the regime. Therefore, it is assumed that regulating Internet is possible both offline and online by "intimidating individual bloggers" or "blocking websites" respectively.[86] As such, digital authoritarianism is never purely digital and always contains various offline elements.

2.3 Policy diffusion, learning, authoritarian learning

As this thesis is interested in the analysis of the learning process behind countering threats to Putin's regime, this section will explore concepts that are connected either generally to policy diffusion/transfer and/or sophistication of authoritarian regime practices (i.e., learning). After doing so, I will explain my understanding of (authoritarian) learning and how it will be used in the context of this thesis.

Behavioral research from the entrepreneurial environment contends, that organisational learning has a strategic character as it refers to the company's ability to "identify, react and adapt to the changes in the environment."[87] While originating from a different research setting, the principles remain relevant for this research as well. Indeed, the same logic applies to governments who learn either from their experience or experience of other governments. Relatedly, Rose has established the concept of lesson-drawing. However, this concept refers to the desired goal of imitating a certain programme or policy. That is, to transfer it from one place to another after some initial screening. If the lesson is evaluated positively, the respective policy is suitably adapted. If it is evaluated negatively, "observers learn what not to do from watching the mistakes of others."[88] Nevertheless, in a similar manner, it is entirely possible to draw a lesson also from one's own experience.

[86] Markku Lonkila, Larisa Shpakovskaya, and Philip Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet," in *Freedom of Expression in Russia's New Mediasphere*, ed. Mariëlle Wijermars and Katja Lehtisaari (London: Routledge, 2020), 17–39., p. 20
[87] Stéphanie Moyson and Peter Scholten, "Theories on Policy Learning: Existing Approaches and Future Challenges," in *Knowledge, Policymaking and Learning for European Cities and Regions. From Research to Practice*, ed. N. F. Dotti (Cheltenham (UK): Edward Elgar Publishing, n.d.)., p. 2
[88] Richard Rose, "What Is Lesson-Drawing?," *Journal of Public Policy* 11, no. 1 (1991): 3–30., p. 4

Writing about Arab Spring uprisings, Heydemann and Leenders write about a top-down process of authoritarian learning and adaptation to the changing societal conditions and atmosphere inside the Arab states. According to them, there was a sort of dual learning in which on the one hand, the protests represented a result of social learning by Arab citizens, while on the other hand, the approaches of the counter-revolutionary regime represented a form of authoritarian learning and emulation amid regime elites.[89] Similarly, Von Soest understands learning as a "change of beliefs, skills or procedures based on the observation and interpretation of experience" and he contends that this learning relates to opposition movements as well.[90] While I recognise this dual learning, my main focus lies at the top-down process of authoritarian learning that is related primarily to governments. However, societal moods will be mentioned as well to either see to what phenomena the government is reacting to, or to evaluate the effectiveness of government's reaction.

As mentioned, I deal with learning to capture the process of internet governance for the regime stability. Bunce and Koesel suggest that when focusing on "protest-proofing", one should expect authoritarian leaders to limit "coordinative resources" for its citizens and opposition groups, while maintaining control over the "organizational space"[91] (i.e. the public sphere). But under which conditions can we expect learning to occur? Sources of learning according to Bank and Edel include "geographical proximity, a common language, a shared ideology, and well-established prior relations between the ruling elites of different countries."[92] As such, I hypothesize, that sophistication of Russian cyberspace regulation is related to the "protest-proofing" as characterised by Bunce and Koesel in order to increase regime stability.

Naturally, the pursuit of political stability is not unique to Russia. The polity's stability is central to all kinds of regimes and is sought by virtually every government in power. According to Tikk and Kertunnen, stability is about "entity's capacity to resist unavoidable threats and accommodate to inevitable changes" in order to ensure systemic functionality and thus it is

[89] Heydemann and Leenders, "Authoritarian Learning and Authoritarian Resilience: Regime Responses to the 'Arab Awakening.'", p. 648

[90] Christian von Soest, "Democracy Prevention: The International Collaboration of Authoritarian Regimes," *European Journal of Political Research* 54 (2015): 623–38., p. 628

[91] Koesel and Bunce, "Diffusion-Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations against Authoritarian Rulers.", p. 755

[92] André Bank and Mirjam Edel, "Authoritarian Regime Learning: Comparative Insights from the Arab Uprisings," Working Paper, Legitimacy and Efficiency of Political Systems (German Institute for Global and Area Studies (GIGA), 2015)., p. 7

common to emphasize securing essential "industrial and information and communications systems in the name of stability".[93] Nevertheless, the perception of what, why and how a certain aspect of political order needs to be stabilised differs depending on the character of the regime.[94] However, in an authoritarian system, regime stability often hinges "on the ability to control and manipulate information."[95] Unexpected threats that can lead to political uncertainty thrive in the online environment. Even though I acknowledge that the offline and online dimension of authoritarianism are inseparable, this thesis is primarily interested in information control, manipulation and/or surveillance because information flows nowadays appear predominantly online. Crisis management of an authoritarian regime therefore often includes both online and offline interference such as blocking access to political websites or even the whole online and mobile network, arresting public figures such as journalists, bloggers, or activists. By proxy, they can also manipulate Internet service providers. However, authoritarians face a dilemma while blocking Internet access for a long time as it can negatively influence national economy and lead to international political pressure.[96]

According to Levy, there are different levels in which learning can take place. He characterizes *simple* learning as the process than includes changes in means but not ends and *complex* learning as the process in which a value conflict is found that results into an alteration of both means and ends.[97] While regime stability is the end of all regimes, the means to reach it differ (typically a combination of foreign and domestic policies). While I recognise these two forms of learning, my analysis will stay mainly at the level of simple learning. That is because complex learning includes an alteration of "both means and ends" (typically a foreign policy goal change), whereas simple learning refers to the pursuit of the same end (regime stability) while sophisticating the means to reach it (in my case sophistication of cyberspace regulation and Internet governance). As such simple learning is assumed to happen when Russian cyberspace regulation was adapting and reacting to the current trends (be it at home or in other authoritarian regimes) without alternating

[93] Kerttunen and Tikk, "The Politics of Stability: Cement and Change in Cyber Affairs.", p. 54, 58
[94] Kerttunen and Tikk., p. 53
[95] Jason Gainous, Kevin M. Wagner, and Charles E. Ziegler, "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections," *Democratization* 25, no. 2 (2018): 209–26., p. 209
[96] Howard, Agarwal, and Hussain, "The Dictator's Digital Dilemma: When Do States Disconnect Their Digital Networks?", p. 4, v5
[97] Jack S. Levy, "Learnig and Foreign Policy: Sweeping a Conceptual Minefield," *International Organization* 48, no. 2 (1994): 279–312., p. 286

its foreign policy as a whole and complex learning is assumed to happen in conjunction with foreign policy alteration.

Ambrosio argues that currently, autocrats focus more on safeguarding the conditions under which the state sovereignty is protected and at the same time, regime change is delegitimized.[98] Tossun and Croissant argue that international organisations "can stimulate the adoption of a policy innovation (...) in exchange for resources or membership.[99] Not that Russia would be using cyberspace regulation and norms along these lines. However, being aware of the role of international organisations regarding influencing policy, it has been trying to shape the international cyberspace regulation to its benefits via the UN Group of Governmental Experts on Information Security (UNGGE), as a member of the International Telecommunication Union (ITU) or Shanghai Cooperation Organization (SCO). Indeed, according to Solingen, international institutions can hasten or hold the diffusion of "norms, authority, and best practices"[100] so the analysis of Russian initiatives in this body is relevant to this thesis.

Because of this, my analysis will be complemented by Russian actions in various international bodies to find out what has Russia been doing on the international level to further support its perception of internet governance and thus safeguard the conditions under which state sovereignty is protected on the international level. Therefore, on the international level, authoritarians try to protect the sacred principle of state sovereignty no matter the circumstances while on the domestic level, they try to delegitimise those who undermine this principle by advocating for universal human rights, freedom of speech, media freedom etc. That is, the focus on regime protection is both inwards and outwards as efforts in both spheres go hand in hand.

My approach of learning to some extent overlaps with the 'governmental learning' of Etheredge and Short who described it as "the process by which governments increase their intelligence and sophistication and, in this manner, enhance the effectiveness of their action."[101] In my case, sophistication refers to the sophistication of cyberspace regulation and internet control, whereas effectiveness refers to the ability to counter dissent in the digital milieu in order to shape

[98] Ambrosio, "Constructing a Framework of Authoritarian Diffusion: Concepts, Dynamics, and Future Research." 2010, ibid, p. 378

[99] Jale Tosun and Aurel Croissant, "Policy Diffusion: A Regime-Sensitive Conceptual Framework," *Global Policy* 7, no. 4 (2016): 534–40. Ibid, p. 536

[100] Etel Solingen, "Of Dominoes and Firewalls: The Domestic, Regional, and Global Politics of International Diffusion," *International Studies Quarterly* 56 (2012): 631–44., p. 634

[101] Moyson and Scholten, "Theories on Policy Learning: Existing Approaches and Future Challenges.", p. 2

information space for the sake of regime stability. Therefore, my approach to learning will stay on this governmental level of regime elites while focusing mainly on inward-looking policies directed towards domestic population, but also supplementing this effort with outward-looking policies and initiatives directed towards international organisations in order to legitimise the Kremlin domestic actions.

As the scholarly literature on policy diffusion and learning can be quite contentious, it is important to clarify the logic and operationalisation of learning for the purpose of this thesis. Importantly, this thesis does not work with policy diffusion per se, but rather policy innovation along the lines of lesson-drawing as conceptualised by Rose. Therefore, in this case, learning is not about emulation but rather about the fear of emulating an undesired scenario or simply preventing such scenario by observing either foreign or domestic development and *drawing a lesson* from such experience. That being said, it should be noted that learning itself is difficult to prove, especially when one wants to prove that it was learned by a certain actor from another actor instead of being created by contemporary trends or correlated unrests.[102] However, my goal is not to prove that *something* was learned from *someone* but rather capture the process of adapting precisely to contemporary trends and drawing lessons from either international events that can be related to Putin's Russia due to the similarity of political systems, historical experience or domestic events that proved detrimental to the stability of Putin's regime.

3. Methodology

I understand learning as a long-term process with turning points. These turning points refer to events after which we can identify a change in the perception of Internet governance and/or intensification in controlling the online information space. As my aim is to capture the way Russian authorities have been thinking about and/or implementing Internet regulation in a period of more than twenty years, this thesis represents an in-depth longitudinal case study based on secondary data. As such, with the help of periodization, I will trace developments within a single country over time. By qualitatively researching the development of Russia's cyberspace regulation, I aim to capture and describe the learning process behind the Kremlin's approach to Internet governance and understand what kind of events, both international and domestic, have shaped the Kremlin's

[102] Peter Burnell and Oliver Schlumberger, "Promoting Democracy - Promoting Autocracy? International Politics and National Political Regimes," *Contemporary Politics* 16, no. 1 (2010): 1–15., p. 5

perception of what needs to be done in order to use the Internet to the benefit of the regime. By doing so, I am mainly interested in the developments in Russia itself and I do not seek to generalise the pattern of authoritarian learning. Therefore, my approach is idiographic rather than nomothetic.

I am now moving to the introduction of the turning points that I find important for this process and explain the logic of their selection. The first (1) turning point represents a period when the first internet connections in Russia appeared and when government circles were discussing for the first time how internet governance should be approached. Here we are talking about the second half of the 1990s, just before Putin got to power and early 2000s when he slowly started appropriating this issue.

The second (2) turning point is the series of colour revolutions in the former soviet-space – Georgia (2003), Ukraine (2004) and Kyrgyzstan (2005). From the perspective of Putin's inner circle, these events that allowed regime change in the former-soviet republics were evaluated negatively and hence it drew a lesson and strategically learned what needs to be done not to allow similar scenario at home as the country shared similar historical experience and proximity - the process that Horvath has called "a preventive counter-revolution".[103] It is this counter-revolution that made Putin's Russia more hostile towards the international order dominated by the West and thus contributed to the revisionist character of its policies and governance, while also contributing to his hostility towards both organisations and individuals inside of Russia that advocated for societal principles typical for the Western world – the logic of so called "Trojan horses" or "fifth column".

The third (3) turning point is Arab Spring and 2011/2012 mass protests in Moscow. The series of revolution in the Arab world have been compared in the literature to the colour revolutions. Importantly for Russia though, the shared experience of Soviet style rule and post-Soviet governance was no longer there. Nevertheless, they can be seen as another turning point because the large-scale protests happened either because of an absence of election all together or because elections were seen as a farce. After the Duma election in December 2011, Russian citizens felt the same grievances and found elections as futile, even more so after the presidential elections in March 2012, when Medvedev handed the presidency back to Putin. Importantly, social media proved to be instrumental in organising all these protests.

[103] Robert Horvath, *Putin's Preventive Counter-Revolution: Post-Soviet Authoritarianism and the Spectre of Velvet Revolution*, 1 (New York: Routledge, 2013).

The fourth (4) turning point are Snowden's revelations about secret mass surveillance in the US, Ukraine's Euromaidan, and the subsequent Russian annexation of Crimea. Solingen argues that "Arab Spring triggered firewalls within and beyond the region". He argues that the direction of diffusion can be changed by "learning from, improving and diversifying causal mechanism, and adapting them to their medium and to levels of sedimentation of prior diffusion."[104] It is true that this level of sedimentation of prior diffusion might have been significant in Russia if we consider the reasons behind developing the strategy of preventive counter-revolution and the adoption of the ideology of sovereign democracy in light of colour revolutions. It is because of these suggestions that this thesis expects cyberspace regulation to occur after events such as colour revolutions, Arab Spring uprising or Euromaidan. At this point, with its ambitious and aggressive foreign policy including the annexation and supporting separatist war in eastern Ukraine, the Kremlin started a period characterised by increased hostility with the West, informational competition about its role in Ukraine and the state's role in governing both online and offline spaces.

The fifth (5) turning point is Russia's full-scale invasion of Ukraine. Compared to the previous turning points, in this case, the difference is that Russia was reacting to an event that it initiated itself. As the war started, the reason to control information space arguably increased to justify the occupation for the domestic population.

4. Empirical analysis

In this section I will track Russian learning from one turning point to another, while taking into account various factors such as institutional arrangements, technological innovations, and attempts to international regulatory norms.

4.1 Origins of the Runet and Putin's rise to power

As mentioned, one of the main reasons why the Internet is prone to be controlled by Russian authorities is due to its public sphere character – a sphere in which information flows and opinions clash. To an extent, this can be seen as an imperial legacy that Russia has inherited from the public

[104] Solingen, "Of Dominoes and Firewalls: The Domestic, Regional, and Global Politics of International Diffusion." Ibid, p. 638

sphere character of the Soviet Union that had always strived to dominate the flow and distribution of information and ideas. According to Sundstorm, by the end of 1990s, the society-state relations in Russia were more of a corporativist character rather than liberal one. During the Soviet rule, citizens were exposed to a state-led model of civil society that was setting the rules for political participation for its citizens and thus, the perception that the state should play a substantial role in citizens' lives remained widespread.[105] This soviet-style state corporativism focused more on possibilities how to control and limit rather than facilitate public participation and flow of information. Therefore, the legacy of the soviet state was that interest groups were to control citizens rather than represent them.[106]

Information distribution had always been controlled in the Soviet Union. There was a strong tradition of telephone calls interceptions, and speech recognition research and telephone wiretapping were connected and conducted under the umbrella of the KGB.[107] Mass communication were often referred to as "tools" or "instruments" that the party had at its disposal – this perception has proved to remain the same also after the USSR's collapse when the Internet started to be governed for the sake of regime stability.[108]

In August 1990, there was the first Soviet link to the global internet.[109] In 1994, RuNet commenced as the Russian domain .ru was created[110] and by 1995, Russia is thought to had established then-contemporary national communications.[111] At the same time, the former KGB was splitting into various agencies that represented the new security apparatus. According to Soldatov and Borogan, it was no coincidence that the KGB's division that had the responsibility to intercept phone calls was transformed into the Committee of Government Communication and later into Federal Agency for Government Communications and Information (FAPSI).[112]

---

[105] Lisa McIntosh Sundstorm, *Funding Civil Society: Foreign Assistance and NGO Development in Russia*, 1st ed. (Standford University Press, 2006). p. 7
[106] Ibid, p. 8
[107] Andrei Soldatov and Irina Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries* (PublicAffairs, 2015)., p. 7
[108] Gulnaz Sharafutdinova, "The Limits of the Matrix - Ideas and Power in Russian Politic of the 2000s," *Problems of Post-Communism* 59, no. 3 (2012): 17–30., p. 24
[109] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 30
[110] Laura H.C. Howells, *Digital Authoritarianism in China and Russia: A Comparative Study*, vol. 166 (Honors Project, 2020)., p. 37
[111] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 47
[112] Soldatov and Borogan., p. 52

In 1998, Russia warned the UN that information technologies could potentially be used "for purposes incompatible with the objectives of ensuring international security and stability".[113] Following this warning, the first ideological incentive for regulating the Internet and the information that flows within proved to be the Doctrine of Information Security that was passed in September 2000 and that proved Putin's willingness to control information.[114] According to the doctrine, national security concerns now included both media and Internet policy. In particular, obtaining information was considered vital "for the purposes of ensuring the stability of the constitutional order, sovereignty and territorial integrity of Russia, as well as political, economic and social stability (…)".[115] Relatedly, at this time, Russia also started to shape the international discussion about the role cyberspace. As part of the UN, there is a specialised group called United Nations Group of Governmental Experts on Development in the Field of Information and Telecommunications in the context of International Security (UNGGE). It was created in 2001 based on a Russian proposal and its main goal is to discuss "common norms, rules and principles for responsible state behaviour in cyberspace".[116]

Another Soviet tradition that was resurrected in this period is the strategy of indirect governance.[117] The Russian government had shown a big interest in the Internet service provider (ISP) market and started to develop policies remindful of the Soviet bureaucratic management.[118] As did the ISP market develop, so did the Russian policy toward them. By 2003, there was five operators who controlled about 84% of the market (one of them – Relcom – was owned entirely by the government). However, in total there was about three hundred ISPs competing for Internet access revenues[119], meaning that the majority of ISPs were small companies with limited budget.

In 1998, the game changer in the ISP market proved to be the government's drafted policy to demand all ISPs to install a device that would link their lines to the FSB computers and thus effectively eavesdrop on their customers' communication, which at that time were mainly emails,

[113] Kerttunen and Tikk, "The Politics of Stability: Cement and Change in Cyber Affairs.", p. 55
[114] Sharafutdinova, "The Limits of the Matrix - Ideas and Power in Russian Politic of the 2000s.", p. 19
[115] Marcus Alexander, "The Internet and Democratization: The Development of Russian Internet Policy," *Demokratizatsiya The Journal of Post-Soviet Democratization* 12, no. 4 (2004): 607–27., p. 619
[116] Flonk, Jachtenfuchs, and Obendiek, "Authority Conlifcts in Internet Governance: Liberals vs. Sovereignists?", p. 375-376
[117] Sharafutdinova, "The Limits of the Matrix - Ideas and Power in Russian Politic of the 2000s.", p. 25
[118] Alexander, "The Internet and Democratization: The Development of Russian Internet Policy.", p. 613
[119] Alexander., p. 611

but also browsing activity and other digital data.[120] It was called SORM (System of Operative Search Measures) and in fact, this acronym referred to the already established practice of monitoring phone calls by the Soviet KGB[121] which at the end of 1990s was updated to SORM-2.[122] According to Soldatov and Borogan, SORM started to be developed by the Central Research Institute of the Communications Ministry in 1994 when "Russian communications switched over from analog lines to digital cables".[123] Crucially, the ISPs themselves had to pay for the device (whet the regulations was passed, the cost amounted roughly 25 000 dollars) without having access to it or benefiting from the device itself.[124] This proved to be an effective strategy for the Kremlin to allow only loyal ISPs on the market. Those who did not comply or simply did not possess enough revenues for the device were forced out of business as the FSB was also in charge of providing licenses to ISPs. In 1999, small providers represented 90% of the ISP market.[125]

Importantly, when SORM was upgraded to SORM-2 to encompass the Internet, it was Putin who was the head of FSB from July 1998 to August 1999, and it is considered to be his achievement.[126] There was no public debate about implementing SORM[127] and initially, the surveillance through it was warrantless. When a smaller ISP threatened to file a lawsuit against the FSB for requiring its customers' data, it was disconnected on the grounds of "licensing errors".[128] Even though the regulation was the adjusted and the warrant was required, the FSB did not have to show it to anyone, not even the operator, and is thus allowed to execute the interception individually. In other words, according to Soldatov and Borogan, the SORM methods followed "the Soviet system of phone wiretapping when no one thought of court-approved warrants."[129]

---

[120] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*; Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models.", p. 8

[121] Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models.", p. 8

[122] Alexander, "The Internet and Democratization: The Development of Russian Internet Policy.", p. 616

[123] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 71

[124] Deibert et al., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*., p. 219

[125] Alexander, "The Internet and Democratization: The Development of Russian Internet Policy.", p. 616

[126] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 89

[127] Soldatov and Borogan., p. 70

[128] Alexander, "The Internet and Democratization: The Development of Russian Internet Policy.", p. 616

[129] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 78

With the emergence of online media and various political sites, the Internet started to gain on societal influence. In 1999, a political technologist Gleb Pavlovski helped to develop a new pro-Kremlin party Unity and created the public relations company the Foundation for Effective Politics which soon turned out to be an important player on the Internet. While it was illegal for the traditional media to publish exit polls during elections, in 1999 Duma elections, Pavlovski launched a website elections99.com where he exploited the fact that the law did not include the Internet and published exit polls from Russian regions, effectively swaying votes in favour of Putin's party that ended up getting 23.3% of voter support.[130] Moreover, he also suggested and facilitated the first, and for a long time only, meeting of Putin with Internet entrepreneurs. The meeting introduced a plan for the government to control the domain .ru and require various organisation "from joint-stock companies to media to schools" to use this domain. Eventually, it was not adopted as Putin saw that all important players in the Internet domain are more or less tied with Kremlin anyway and felt he had the situation under control.[131]

Pavlovski's agility on the Internet was called upon also during the run-up to the 2000 presidential. This time, it was more aggressive as it directly targeted Putin's main opponents of the time – Yuri Luzhkov and Yevgeny Primakov - by launching several news sites (strana.ru, vesti.ru, smi.ru or lenta.ru) that launched campaign against them and also directly ridiculed them on sites primakov.ru, mayor.ru or lujkov.ru.[132] Online-only media platforms started to be the most preferred source of information on the Internet and soon, online alternatives to offline media followed, making campaign websites and party websites "the least popular sources of information."[133] Many of these websites were already tied to Kremlin with pro-governmental figures such as Pavlovski who further developed websites such as strana.ru and turned it into "a Russian national news service" only to sell it in 2002 to "the All-Russia State Television and Radio Broadcasting Company, a state-owned corporation that included a major television channel."[134]

In August 2000, the nuclear submarine Kursk sank in the Barents Sea in which 118 sailors died. Putin, then three months in office, responded to the sinking only after five days which ignited serious criticism in the independent media about the handling of the disaster by the Kremlin. The

[130] Soldatov and Borogan., p. 92
[131] Soldatov and Borogan., p. 93-98
[132] Alexander, "The Internet and Democratization: The Development of Russian Internet Policy.", p. 617
[133] Alexander., p. 617
[134] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 107-108

NTV channel, owned by oligarch Vladimir Gusinky, had been challenging the Kremlin's versions by for example "providing the names of the dead when authorities refused to do so."[135] Boris Berezovsky, who controlled the state channel ORT (now Channel 1) was also critical of the Kremlin's handling of the disaster. In defense, Putin accused both of them for lying and for "manipulating public opinion."[136] Earlier, NTV was uncovering corruption inside of Yeltsin's family, earned its reputation for quality reporting in the first Chechen war and overall established itself as a significant and independent media actor.[137] As such, Putin knew that NTV is an oppositional actor and tried to supress it already in the first months of his first term – he jailed Gusinky and forced him to sell out his Media-Most empire (of which NTV was part of) for his freedom.[138] A few months after the disaster, the Kremlin forced Berezovsky to sell his share in ORT and also seized NTV, effectively bringing both influential media channels under government control.[139] In this environment, the Russian blogosphere started to emerge which started a tradition for many years ahead. Many of them represented former reporters who considered the Internet to be the only place to express their opinions. One of the most popular sites was livejournal.com.[140] Eventually, it was Pavlovski who started to influence the blogosphere through his Foundation for Effective Politics[141] and the Kremlin started to deal with Internet platforms in a way it had dealt with newspapers – through ownership by loyal oligarchs.[142]

In terms of learning, this period represented more of a process of adapting to contemporary trends rather than drawing lessons because the problem of Internet governance was relatively new for Russia as it had a lot of other problems to deal with in the 1990s. The end of 1990s and early 2000s marked the re-emergence of the Russian state from dislocation and bankruptcy, to increased centralisation which also included the approach to information management. By conceptualising

---

[135] Ian Traynor, "Putin Aims Kursk Fury at Media," *The Guardian*, 2000, https://www.theguardian.com/world/2000/aug/25/kursk.russia2.

[136] Matthew Luxmoore, "The Kursk Catastrophe, A Lesson For Putin, Is Fading From Russia's Attention 20 Years Later," *RFE/RL*, 2020, https://www.rferl.org/a/the-kursk-catastrophe-a-lesson-for-putin-is-fading-from-russian-attention-20-years-later/30778500.html.

[137] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 86-87

[138] Soldatov and Borogan., p. 102

[139] Luxmoore, "The Kursk Catastrophe, A Lesson For Putin, Is Fading From Russia's Attention 20 Years Later."

[140] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 109

[141] "Freedom on the Net: A Global Assesment of Internet and Digital Media" (Freedom House, 2009)., p. 88

[142] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 109

gathering of information along the lines of national security, the Kremlin provided a rationale behind the adoption of SORM-2 surveillance technology that allowed the FSB to follow the Soviet practice of telephone interceptions which effectively marked the foundation for developing digital authoritarianism further. To follow up Deibert's and Crete-Nishihata's generations of cyberspace controls, in this period, Russian approach to Internet governance stayed in the second generation of cyberspace control, mainly because of SORM-2. Protecting information space had always been necessary in the Soviet Union because the state pursued a single narrative that was to be protected and enforced. In Russia, after a brief period of liberalisation, a state-led narrative returned. The following section will discuss where this narrative originated and how it had been protected by Internet governance.

4.2 Colour revolutions, sovereign democracy, and Putin-Medvedev tandem (2004 – 2011)

The series of the so-called colour revolutions that occurred in Georgia (2003), Ukraine (2004) and Kyrgyzstan (2005) had changed dramatically the Kremlin's perception of Western policies towards Russia. The democracy promotion policies that helped facilitate them with funding of civil society organisations were seen as a projection of American power, and Putin and his inner circle started to believe that the hidden objective behind democracy promotion policies was to undermine Russia's position in the international arena. Because of the similar post-Soviet historical experience and style of governance, there was a legitimate fear in the Kremlin that the next colour revolution was to happen in Russia itself.

Starting his second term in 2004, Putin's reaction to the events was to further pursue centralisation in Russia and to tie civil society organisations with his regime. For this purpose, the federal institution Public Chamber was created that was supposed to include NGO representatives and represent citizens' perception of the government activity.[143] The focus on NGOs was important because they represented a critical part of Western democracy promotion policies and they also proved vital in mobilising anti-governmental protests during colour revolutions. However, the institution included only those who were tied to the government in one way or another and failed

[143] McIntosh Sundstorm, *Funding Civil Society: Foreign Assistance and NGO Development in Russia*., p. 180

to represent those critical of it.[144] Striving to create a patriotic civil society, this institution was also responsible for allocating grants and thus making sure that only NGOs uncritical of the government will get government funding – this made scholars such as Richter call the institutions ironically as "the ministry of civil society."[145] Furthermore, in 2006, a new law regulating NGOs in general was adopted that was supposed to limit the activity of NGOs funded from abroad. They had to register as separate Russian entities and undertake strict financial and bureaucratic controls. Moreover, a separate federal agency was to monitor whether they adhere to their stated (and government approved) goals.[146] For example, the law forbade the registration of NGOs that were threatening "the national unity, the unique character, cultural heritage or national interests of Russia" which represent very broad and subjective terms and could lead to a ban of virtually any organisation.[147]

Eventually, these events had led Russia to respond with the concept of "sovereign democracy" whose main orchestrator was Vladimir Surkov. The rationale behind this concept was the impression that the sovereignty of Russian state was endangered by Western democracy promotion policies that were bypassing Russian sovereignty by promoting hostile societal values. It was introduced by Surkov in February 2006, during his lecture to the activists of the United Russia party, where he argued that Russia is not a country with a liberal tradition focusing on individual rights, but rather a country based on traditions of collectivism or strong state.[148] According to Ambrosio, Surkov's main argument was the belief that Russian sovereignty is being attacked by various outside forces.[149] According to Sharafutdinova, this narrative can be characterised as a "guardian discourse" whose main goal was to protect Russia from the influence of the West and friends of the West (liberals) inside Russia.[150]

Sovereign democracy did not include only institutional measures such as the Public Chamber or the 2006 NGO law, but also the creation of pro-Kremlin youth organisations. One of them was

[144] Evgeny Finkel and Yitzhak M. Brudny, eds., *Coloured Revolutions and Authoritarian Reactions*, 1st ed. (Routledge, 2015)., p. 17
[145] Jo Crotty, Sarah Marie Hall, and Sergej Ljubownikow, "Post-Soviet Civil Society Development in the Russian Federation: The Impact of the NGO Law," *Europe-Asia Studies* 66, no. 8 (2014): 1253–69., p. 1256
[146] Thomas Ambrosio, *Authoritarian Backlash: Russian Resistance to Democratization in the Former Soviet Union*, 1st ed. (Routledge, 2009)., p. 47
[147] Ambrosio., p. 49
[148] Finkel and Brudny, *Coloured Revolutions and Authoritarian Reactions*. p. 28
[149] Ambrosio, *Authoritarian Backlash: Russian Resistance to Democratization in the Former Soviet Union*. p. 70, 71
[150] Sharafutdinova, "The Limits of the Matrix - Ideas and Power in Russian Politic of the 2000s.", p. 20

Nashi ("Ours"), also curated by Surkov. The reason behind them was not only to facilitate patriotic civil society but also to have a loyal pro-Putin organisation that could fill the streets in critical moments such anti-government protests during election times.[151] Moreover, it was also reported that Nashi activists conducted distributed denial of service attacks (DDOS) against anti-regime activists.[152]

While the ability to call on a youth movement to quickly organise a pro-governmental protest represented an offline dimension of Russia's authoritarianism, the online dimension was represented by having a network of loyal bloggers take part in online discussions trying to mitigate political criticism, support nationalism and fill the Russian blogosphere with pro-regime content during anti-regime protests. Therefore, instead of direct censorship, the Kremlin preferred these "soft approaches to combat undesired content", which turned out to be particularly the case during the 2007 parliamentary and presidential election cycle.[153]

By 2008, the Russian search engine Yandex was the most popular search engine on Runet and many had it set up as a home page that daily presented top five news articles to millions of Runet users instead of printed media.[154] Being aware of this, Surkov went to Yandex offices in September 2008 to find out more about how this top five selection works and even requested access to Yandex's interface. As this was a month after the Russo-Georgian war, he was particularly worried about war-related stories and wanted to exclude Georgian sites from the algorithm. Eventually, they agreed to have a sort of a Kremlin-Yandex hotline in case the government had any questions regarding the news selection.[155] In April 2007, before the Duma elections held in December that year, a pro-Kremlin blogger Pavel Danilin and his team successfully managed to influence Yandex's algorithm. An anti-regime march was held in Moscow, so they began to blog about a smaller pro-regime march that was to happen on the same day. Eventually, they "crowded out all the items about the opposition march from the top-five blog posts listing on Yandex."[156] A Day after the Duma elections in December, the popular blogging platform Livejournal was purchased

[151] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 113
[152] Soldatov and Borogan., p. 116
[153] Deibert et al., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*., p. 214
[154] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 111
[155] Soldatov and Borogan., p. 114
[156] Deibert et al., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*., p. 214

by the oligarch Aleksandr Mamut.[157] Besides these informational counterstrategies, the first cases of technical filtering occurred as well in this period, albeit only temporarily and on the regional level. In December 2010, a regional ISP "temporarily blocked access to an environmentalist site because it initiated a petition do dismiss a local mayor."[158]

While the term sovereign democracy lost its prominence in the government discourse when Medvedev became president in 2008, the idea behind it – sovereign Russia without foreign interference – remained the key idea behind Russian foreign policy.[159] One of his first moves was to restructure the Interior Ministry and replaced a bureau against organised crime and terrorism with a bureau against extremism.[160] This bureau is widely referred to as "Center 'E' that patrols the web and refers legal violations to the courts."[161] Together with FSB, it started "a massive program to monitor any kind of civil activity, including surveillance of religious organisations, political parties not in parliament, and even informal youth groups (…) in order to prevent activists from reaching demonstrations."[162] Expressing opinions online started to be targeted by the Article 282 of the criminal code which deals with extremism. As Freedom House report notes, "the term is vaguely defined and includes xenophobia and incitement of hatred towards a social group"[163]. In July 2008, a blogger Savva Terentyev was convicted under the pretext of defaming "the human dignity of a social group – the police – and sentenced to one year of probation."[164] In another case, "the content provider Bankfax was charged under the article 282 with insulting a group of people by referring to them as oligarchs."[165] This was complemented with purchasing sophisticated surveillance technology, including face recognition systems, to be monitoring train stations as well as the subway in Moscow.[166] In addition, the use of SORM technology had become even more

[157] "Freedom on the Net: A Global Assesment of Internet and Digital Media.", p. 89
[158] "Freedom on the Net 2011: A Global Assessment of Internet and Digital Media" (Freedom House, 2011)., p. 27
[159] Sharafutdinova, "The Limits of the Matrix - Ideas and Power in Russian Politic of the 2000s.", p. 22
[160] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 115
[161] Henry and Howells, "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet Governance.", p. 8
[162] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 115
[163] "Freedom on the Net: A Global Assesment of Internet and Digital Media.", p. 89
[164] "Freedom on the Net: A Global Assesment of Internet and Digital Media.", p. 90
[165] Deibert et al., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*., p. 217
[166] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 115-116

prominent. According to Soldatov and Borogan, "the number of intercepted phone conversations and email messages doubled in six years, from 265 937 in 2007 to 539 864 in 2012.[167]

Already in this period, the Kremlin started to perceive the Internet as an extension of media. Even though the Internet, at that time, was not regulated under the Law on Mass Media as it was adopted in 1991 it was still believed that this law should include the Internet as well because its Article 2 states that "it shall cover other form of periodic distribution of mass information."[168] Therefore, under these pretexts of violating media laws, it was possible to target, for example, an online forum as a case of mass media and thus creating a precedent for further prosecution of others.[169] As we shall see in the next chapters, this logic of characterising Websites as mass media was further elaborated on and served as a rationale for further regulation.

On the international level, since 2006, Russia has also turned its attention towards the Shanghai Cooperation Organization (SCO) in order to pursue its information security conceptualizations. The organisation is widely thought to be "a regional vehicle of protective integration against international norms of democracy and regime change."[170] Together with China, Russia and other SCO members have been connecting information control with cybersecurity when participating in global forums in order to hide their intentions behind their interest-driven discourse.[171] Referring to the recent colour revolutions, the principles of sovereignty and non-interference have been typical for Russia's conduct in the international environment. Together with China and four Central Asian states, Russia has stated that the use of information and communication technologies can be used to disrupt the maintenance of international stability and security and urged other nations to refrain from using them "to interfere in the internal affairs of other states or with the aim of undermining their political, economic and social stability".[172]

Overall, in this period, Russia had shown a considerable degree of learning in term of lesson-drawing – in both offline and online environments. Its biggest fear was to emulate the colour revolutions scenario. Therefore, when it learned that Western funded NGOs facilitated the street protests and were the main driving force behind these revolutions, it created the federal institution Public Chamber to tie Russian friendly NGOs with the government and facilitated their funding.

[167] Soldatov and Borogan., p. 243-244
[168] Deibert et al., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*., p. 215
[169] Deibert et al., p. 215
[170] Ebert and Maurer, "Contested Cyberspace and Rising Powers.", p. 1067
[171] Morgus, "The Spread of Russia's Digital Authoritarianism.", p. 93
[172] Kerttunen and Tikk, "The Politics of Stability: Cement and Change in Cyber Affairs.", p. 56

By the same logic, the 2006 NGO law led to an increase in government oversight over NGOs funded from abroad as they were seen as pursuing interests of the West inside Russia and started to be perceived as "foreign agents" in the eyes of Kremlin. The concept of sovereign democracy served as an ideological underpinning of these actions. Accordingly, it created a pro-Kremlin youth movement Nashi as a counterweight to these organisations and a force to be called upon in times of anti-regime protests to fill the streets with pro-regime protesters. However, Nashi were active also in the online domain. By relying on pro-regime bloggers like Nashi to flood the information space with counterinformation when needed, the Kremlin slowly started to move into the third generation of cyberspace controls that cannot be traced directly to the Kremlin.[173] However, cases of the first generation of cyberspace controls occurred as well when access to some websites was filtered, albeit regionally. Despite all this development, the Internet in Russia in this period was still characterised as "the last relatively uncensored platform for public debate" and was considered "partly free".[174]

Importantly, both complex and simple learning occurred in this period. Indeed, a value conflict was found when Putin and his inner circle started to believe that the true intention behind democracy promotion policies was to undermine Russia's position in its near abroad which led to a foreign policy alteration and adoption of the concept of sovereign democracy. Simple learning can be understood as further sophisticating its online content management capabilities by employing pro-Kremlin bloggers, broadly interpreting media laws, having loyal oligarchs buying off various media and online platforms, and the increase in SORM monitoring that had doubled in this period.

4.3 Arab Spring and mass protests in Moscow (2011 – 2013)

Just like the colour revolutions, the Arab Spring uprisings tried to remove authoritarian leaders from power. Not long after the threat of the colour revolutions in post-Soviet republics seemed to be waning, another series of Western-backed revolutions occurred in the Middle East which, for the Kremlin, represented a validation that the narrative created at home was correct and should be further pursued. As the revolutions happened in a Muslim world, another line of argument in

[173] Sharafutdinova, "The Limits of the Matrix - Ideas and Power in Russian Politic of the 2000s.", p. 26
[174] "Freedom on the Net 2011: A Global Assessment of Internet and Digital Media.", p. 27

regime's favour was added. Toppling authoritarian regimes would allegedly strengthen Islamic fanatics and create anxiety amid Muslim population.[175] Indeed, ten days after the revolution in Egypt, during a meeting of National Antiterrorist Committee in North Ossetia (with a significant Muslim population), Medvedev characterised the uprising as a plot and a Western conspiracy[176] by saying "(…) this is the kind of scenario that they were preparing for us, and now they will be trying even harder to bring it about."[177]

Comparing the colour revolutions and Arab uprisings, Bunce and Koesel argue that while the colour revolutions challenged authoritarian leaders at (and after) the polls, the Arab Spring uprisings included large-scale street mobilizations because elections either did not exist or their outcome was a "foregone conclusion."[178] As Russia could not boast with a particularly good election transparency record, the Arab uprising were seen as a threat. Even though the shared experience of Soviet style rule and post-Soviet governance was no longer there, the character of elections in Russia could make Russian citizens find them to be futile and follow the similar logic as the Arab protesters. Therefore, despite happening in another region, the style of governance in the Arab states was also authoritarian so Russia had legitimate fears of a spillover. In fact, already in December 2011, according to White and McAllister, by the time the mass protests in Moscow emerged, Russia has fulfilled two most important precondition that led to colour revolutions elsewhere – "a contested election and widespread social networking use skewed towards the young."[179] Furthermore a 2011 Levada Centre poll found out, that almost 40% of Russian considered "an Egypt Scenario to be a possibility for Russia."[180] This, together with the fact that the uprisings were frequently seen as "Facebook and Twitter revolutions"[181] (foreign-owned platforms) particularly worried the Kremlin and represented another reason to argue that they

[175] Koesel and Bunce, "Diffusion-Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations against Authoritarian Rulers.", p. 760
[176] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 124
[177] Keir Giles, *Handbook of Russian Information Warfare: Fellowship Monograph* (NATO Defense College, 2016)., p. 42
[178] Koesel and Bunce, "Diffusion-Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations against Authoritarian Rulers.", p. 754
[179] Stephen White and Ian McAllister, "Did Russia (Nearly) Have a Facebook Revolution in 2011? Social Media's Challenge to Authoritarianism," *Politics* 34, no. 1 (2014): 72–84., p. 78
[180] Koesel and Bunce, "Diffusion-Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations against Authoritarian Rulers.", p. 760
[181] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 125

represent a tool of Western exploitation because Arab security services did not have access to the social networks' servers that are located in the US and thus failed to forestall the dissemination of messages.[182] Furthermore, according to another Levada poll, adult Russians were becoming more and more active on social media – from 35% in 2011, to 56% in 2013.[183] In numbers, there were 41.7 million social media users in 2010 and 51.8 million in 2012 totalling to 42% of the adult Internet population.[184] Arguably, as the Internet penetration increases, its ability to shape people's attitudes towards societal issues increases as well.[185]

It should be noted, that according to Solingen, the role of social media during Arab Spring is overestimated,[186] and according to Pallin, the literature did not succeed to prove "how and to what extent" were social networks instrumental in influencing the protests.[187] However, Solingen contends that while new media such as bit.ly links or Twitter did not play that of a significant role in spreading information regionally, they would more likely get about the information beyond the region[188] which is something this thesis is interested in. Of course, we know this thanks to several years of hindsight. For the purpose of this thesis nonetheless, it is not important to what extent social networks were actually influential, but what discourse about their importance dominated at the time of happening and what kind of information about their influence Russian government was receiving.

The mast protests of 2011/2012 are widely perceived as a turning point when it comes to Internet regulation in Russia. Lonkila et al. have even called it as a "watershed moment."[189] Just like the colour revolutions and Arab uprisings, Putin's Russia perceived the 2011 protests to be

[182] Giles, *Handbook of Russian Information Warfare: Fellowship Monograph*., p. 43
[183] Mariëlle Wijermars and Katja Lehtisaari, "Introduction: Freedom of Expression in Russia's New Mediasphere," in *Freedom of Expression in Russia's New Mediasphere*, ed. Mariëlle Wijermars and Katja Lehtisaari (London: Routledge, 2020), 1–15., p. 3-4
[184] White and McAllister, "Did Russia (Nearly) Have a Facebook Revolution in 2011? Social Media's Challenge to Authoritarianism.", p. 77
[185] Gainous, Wagner, and Ziegler, "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections.", p. 215
[186] Solingen, "Of Dominoes and Firewalls: The Domestic, Regional, and Global Politics of International Diffusion.", p. 635
[187] Carolina Vendill Pallin, "Internet Control through Ownership: The Case of Russia," *Post-Soviet Affairs* 33, no. 1 (2017): 16–33., p. 18
[188] Solingen, "Of Dominoes and Firewalls: The Domestic, Regional, and Global Politics of International Diffusion.", p. 635
[189] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 17

stimulated by an American "cyber/information campaign against Russia."[190] Compared to other channels of mass communications, the Internet was still regarded as somewhat free.[191] However, when the Kremlin found out that protesters had been mobilised by social media, it began to see the Internet as a real threat.[192] Indeed, the protests on Bolotnaya Square marked the biggest rally since the Soviet times as more than 50 000 people showed up on December 10, 2011.[193] But why were social media seen as particularly threating? We can think of several reasons.

By definition, there is no clear hierarchical leadership structure on social media. Therefore, the protest groups operate horizontally and radically undermine the Kremlin's centralised power vertical.[194] Considering that hierarchical order with a clear power vertical dominated the local political order for centuries, the fact that the rallies were mobilised by horizontal networks[195] (social media) was particularly worrying for Kremlin. The horizontal power of social media is confirmed with Litvinenko's and Toepfl's research that showed that "the most important factor for those who took to the streets was seeing the willingness of their friends on social media to do so."[196] As already mentioned, the other reason why the Kremlin feared particularly Western social media was the fact that their servers were not based on Russian soil and were "perceived as part of a US and European strategy to use the Internet to undermine Russian sovereignty."[197]

Alexei Navalny was gradually becoming Russia's most popular blogger since 2010 when he started uncovering corruption scandals on his blogs. His first stories were related to prominent oil and gas companies in which he had bought significant shares and therefore received the right to be informed about their activity. He argued that "my blog exists only because there is a censorship

[190] Giles, *Handbook of Russian Information Warfare: Fellowship Monograph*., p. 39
[191] Pallin, "Internet Control through Ownership: The Case of Russia.", p. 16
[192] Erik C. Nisbet, Olga Kamenchuk, and Aysenur Dal, "A Psychological Firewall? Rick Perceptions and Public Support for Online Censorship in Russia," *Social Science Quarterly* 98, no. 3 (2017): 954–75., p. 960
[193] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 146
[194] Gainous, Wagner, and Ziegler, "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections.", p. 210
[195] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 146
[196] Anna Litvinenko and Florian Toepfl, "The 'Gardening' of an Authoritarian Public at Large: How Russia's Ruling Elite Transformed the Country's Media Landscape After the 2011/12 Protests 'For Fair Elections,'" *Publizistik* 64 (2019): 225–40., p. 231
[197] Gainous, Wagner, and Ziegler, "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections.", p. 220

in media"[198] which of course did not escape the attention of Kremlin. Compared to the previous period of my analysis, the Internet had begun to play a significantly more important societal role as "the daily internet audience had been growing exponentially from 3 million in 2003 to 32 million in 2011"[199] and the share of daily users was 33%[200] which also meant more audience for bloggers like Navalny. Importantly, the fact that during the 2011 protests the online discourse of the "blogosphere belonged predominantly to oppositional bloggers"[201] represented a big concern for the Kremlin. In this period, according to Kiriya, the total average online reach of oppositional media was around 50%[202] which further depicts the constellation of online public sphere at the time of the biggest unrests in Russia since the Soviet times.

Before the election, Navalny led a campaign in which he encouraged "Internet users to register as official election observers and trained them via social media in how to document electoral fraud."[203] An evening before the Duma election day, on December 3, 2011, the most popular blogging platform LiveJournal was attacked by denial of service (DDOS) attacks. The following morning, the attacks continued and expanded to various independent media outlets such as Echo Moskvy, Kommersant, TV Dozhd, or the election monitor Golos, as well.[204]

In 2011 Duma elections, only 53% of Russians considered "the filling in of ballots and the counting of the votes as fair" compared to 69% in 2001.[205] With social media, users themselves could add to the activity of famous bloggers by sharing content about "falsification of the election ballots."[206] The most popular Russian social networks were VKontakte (modeled after Facebook with 190 million registered users as of 2014) and Odnoklassniki. Both sites enjoyed much bigger

[198] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 120
[199] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 19
[200] Ilya Kiriya, "From 'Troll Factories' to 'Literring the Information Space': Control Strategies Over the Russian Internet," *Media and Communication* 9, no. 4 (2021): 16–26., p. 20
[201] Kiriya., p. 17
[202] Kiriya., p. 22
[203] Litvinenko and Toepfl, "The 'Gardening' of an Authoritarian Public at Large: How Russia's Ruling Elite Transformed the Country's Media Landscape After the 2011/12 Protests 'For Fair Elections.'", p. 231
[204] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 149-150
[205] White and McAllister, "Did Russia (Nearly) Have a Facebook Revolution in 2011? Social Media's Challenge to Authoritarianism.", p. 75
[206] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 19

popularity compared to foreign networks such as Facebook or Twitter.[207] Since LiveJournal was struggling with DDOS attacks during the protests, users started to use Facebook which became a major source of information about the protests, even compared to VKontakte.[208] Navalny himself was active on Twitter, where he was posting about "electoral fraud, including pictures taken on smartphones, in order to rally protesters"[209], but also on VKontakte where he led a protest group that the FSB requested to block. Pavel Durov, the founder of VKontakte, did not comply.[210] Importantly, the main demonstration on Bolotnaya Square was announced on Facebook "by a group called 'Saturday at Bolotnaya Square' and was widely publicised among online social network groups."[211] Navalny did not attend the rally because he was in prison for taking part in anti-electoral fraud protests the day after the elections[212] - events, that were five days later depicted by Russian television as "an attempt by Western powers to instigate a colour revolution in Russia."[213] The company Yandex also proved significant in relation to the protests. Its online payment service Yandex Money is the biggest in Russia and widely used among the middle class for e-commerce. In December, it posted a new application that enabled crowdfunding via Facebook to organise demonstrations. Eventually, the organisers raised more than 4 million rubles for the next rally.[214]

White's and McAllister's research nicely depicts the dynamics between then-already controlled traditional media and then-relatively free Internet and social media. In 2014, they concluded that "the greater the frequency of watching television, the more likely the person was to view the elections as having been fairly conducted; by contrast, more frequent use of the Internet

[207] White and McAllister, "Did Russia (Nearly) Have a Facebook Revolution in 2011? Social Media's Challenge to Authoritarianism.", p. 77
[208] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 153
[209] White and McAllister, "Did Russia (Nearly) Have a Facebook Revolution in 2011? Social Media's Challenge to Authoritarianism.", p. 78
[210] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 153
[211] White and McAllister, "Did Russia (Nearly) Have a Facebook Revolution in 2011? Social Media's Challenge to Authoritarianism.", p. 78
[212] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 141
[213] Litvinenko and Toepfl, "The 'Gardening' of an Authoritarian Public at Large: How Russia's Ruling Elite Transformed the Country's Media Landscape After the 2011/12 Protests 'For Fair Elections.'", p. 231
[214] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 157

resulted in seeing the election as unfair."[215] However, Russian platforms such as VKontakte were "largely bypassed by Western platforms for the promulgation of anti-government information."[216] The same research found Facebook to be the most influential site in spreading anti-regime sentiment as compared to Twitter, VKontakte or Odnoklassniki. Ultimately, they find this to be the result of ownership structures – while VKontakte is a Russian project with servers based in Russia, Facebook "is US-based and less subject to Russian government interference or censorship."[217]

Following Putin's re-election in March 2012, the Kremlin slowly, yet systematically, started to respond to the crisis. Regime campaigns to strengthen his image vis-à-vis the opposition began. Again, the West was blamed for igniting unrest in Russia and pro-regime manifestations were organised.[218] Authority of governmental institutions was increased as well. Institutionally, the Ministry of Communication holds the highest authority regarding Internet regulation and development. Secondary, the Federal Service for Supervision of Telecommunications, Information Technology and Mass Communication (Roskomnadzor) monitors the Internet, provides licenses to ISPs and registers online media, while also having the power to block websites.[219] Since December 2011, Roskomnadzor was authorised to "monitor online content and issue warnings to media users."[220] Measures were taken to allow for systematic online content blocking, particularly social media content, across all Russia. For these purposes, a separate list of banned websites was a created (i.e., a blacklist).[221] Widely 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, information on the production and distribution of drugs, and

[215] White and McAllister, "Did Russia (Nearly) Have a Facebook Revolution in 2011? Social Media's Challenge to Authoritarianism.", p. 79
[216] Gainous, Wagner, and Ziegler, "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections.", p. 211
[217] White and McAllister, "Did Russia (Nearly) Have a Facebook Revolution in 2011? Social Media's Challenge to Authoritarianism.", p. 80-82
[218] Koesel and Bunce, "Diffusion-Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations against Authoritarian Rulers.", p. 761
[219] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 21
[220] Gainous, Wagner, and Ziegler, "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections.", p. 220
[221] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 166

information encouraging suicide."[222] While Roskomnadzor managed the blacklist, the ISPs themselves were responsible for its implementation and also for keeping its content secret as required.[223] Sivetc calls this blacklisting mechanism as a "new-school regulation" because it blocks "allegedly illegal content, before the question of whether websites should be penalised is decided by the courts" and effectively creates an environment in which "judiciary and administrative decision-making receive the same weight"[224] – indeed, no court order was needed to add any site on the blacklist.[225] Moreover, users themselves could add to blacklisting via a special online form on Roskomnadzor's site.[226] Also in 2012, the SORM technology was expanded to monitor social media as well.[227]

To suppress opposition voices and civil society after the mass protests, online-related regulations were complemented with offline-related regulations. Building on the 2006 NGO law mentioned in the previous period, since 2012, politically oriented NGOs who receive foreign money now had to officially register as "foreign agents" and even label their publications with such a badge. Apart from that, they were subject to strict reporting and auditing.[228] Furthermore fines were increased for "violating order during meetings and demonstrations" as well as sharing information about "unsanctioned events."[229] In 2012, the federal anti-extremism "Center-E" expanded its outreach to include "district-level police offices".[230] In the same vein, slander was now characterised as criminal offense, particularly "against judges, prosecutors and law enforcement officials".[231]

---

[222] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 24

[223] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 172-173

[224] Ludmila Sivetc, "The Blacklisting Mechanism: New-School Regulation of Online Expression and Its Technological Challenges," in *Freedom of Expression in Russia's New Mediasphere*, ed. Mariëlle Wijermars and Katja Lehtisaari (London: Routledge, 2020)., p. 42

[225] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 24

[226] Sivetc, "The Blacklisting Mechanism: New-School Regulation of Online Expression and Its Technological Challenges.", p. 43

[227] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 21

[228] Lonkila, Shpakovskaya, and Torchinsky., p. 26

[229] Lonkila, Shpakovskaya, and Torchinsky., p. 26

[230] Henry and Howells, "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet Governance.", p. 13

[231] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 26

The Kremlin also continued with employing pro-regime online warriors – both hackers and trolls. During the elections, DDOS attacks were found to disrupt oppositional websites.[232] Since the protests, the Internet trend in terms of content had moved from blogging to videoblogging. They often showed footage from the demonstrations, depicted police violence against Navalny, or satirical cartoons mocking the authorities.[233] In 2012, the still-active youth movement Nashi proved instrumental for the Kremlin again when they had been paying bloggers for posting pro-regime comments on various websites and social media. According to Anonymous, "Nashi had paid online posters to dislike anti-regime videos on YouTube and to leave pro-Putin comments on negative stories about the Russian president."[234] In 2013, a case of systematic pro-regime trolling was revealed, when more than 200 worked full time in St. Petersburg to post pro-Kremlin and anti-opposition commentaries on online media such as LiveJournal or VKontakte.[235] The company employing these trolls is now widely known as the Internet Research Agency and its activity appropriately depicts that the Kremlin considered the "online public sphere an important battlefield."[236]

Putin stated in 2011, that Russia will strive to "establish international control over the Internet using the monitoring and supervisory capabilities of the International Telecommunication Union".[237] On the international level, compared to the Western states, Russian proposals are scarce of emphasis on human rights such as freedom of expression and/or opinion online and typically include emphasis on "stability and security of society" instead. Since the Arab Spring, the idea of "content as threat" has been increasingly promoted by authoritarian countries[238] such as Russia that represents a telling hint regarding the concept of authoritarian learning.

---

[232] Elizaveta Gaufman, "Cybercrime and Punishment: Security, Information War, and the Future of Runet," in *The Palgrave Handbook of Digital Russia Studies*, ed. Daria Gritsenko, Mariëlle Wijermars, and Mikhail Kopotev (Cham: Palgrave Macmillan, 2021), 115–35., p. 118

[233] Julie Fedor and Rolf Fredheim, "'We Need More Clips about Putin, and Lots of Them:' Russia's State-Commissioned Online Visual Culture," *Nationalities Papers* 45, no. 2 (2017): 161–81., p. 166-167

[234] Seva Gunitsky, "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability," *Perspectives on Politics* 13, no. 1 (2015): 42–54., p. 45

[235] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 28

[236] Gaufman, "Cybercrime and Punishment: Security, Information War, and the Future of Runet.", p. 118

[237] Ebert and Maurer, "Contested Cyberspace and Rising Powers.", p. 1063

[238] Flonk, Jachtenfuchs, and Obendiek, "Authority Conlifcts in Internet Governance: Liberals vs. Sovereignists?", p. 379

In 2011, through the Shanghai Cooperation Organization (SCO), China and Russia proposed the International Code of Conduct for Information Security that was understood to represent an initiative to balance the hegemony of the USA in this sphere.[239] In the same year, together with China, Tajikistan and Uzbekistan, Russia called for a blueprint for Internet security regulation to the General Assembly to the UN. The document argued for sovereignty for states over policy authority regarding the Internet and asked for a global collaboration to limit "dissemination of information which incites terrorism, secessionism, extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment".[240]

SCO members hold joint military exercises to exchange knowledge about countering online opposition that has facilitated colour revolutions in other countries.[241] In March 2012, during a meeting of an antiterrorist group within the SCO, Sergei Smirnov (the first deputy director of FSB) said that "new technologies are being used by Western special services to create and maintain a level of continual tension in society with serious intensions extending even to regime change (…) Our election, especially the presidential election and the situation in the preceding period, revealed the potential of the blogosphere" and concluded that it is necessary to come up with a counterstrategy to such technologies.[242] As such, the mass protests in Moscow have arguably prompted the Kremlin to intensify its initiatives among the international bodies and seek alliance with like-minded governments.

In 2012, during the World Conference on International Telecommunications, Russia argued for equal rights of the members of the International Telecommunication Union (ITU) to control the internet when it comes to naming and numbering and thus proposing an alternative to ICANN.[243] At the same conference, it allied with other authoritarian countries such as "China, Saudi Arabia, Egypt, and United Arab Emirates in order to promote a more centralised and controlled vision for the global Internet" and to introduce "global Internet governance" at the level of ITU – it failed due to the Western concerns about "opening the door to content censorship."[244]

---

[239] Ebert and Maurer, "Contested Cyberspace and Rising Powers.", p. 1055
[240] Glen, "Internet Governance: Territorializing Cyberspace?", p. 647-648
[241] Deibert, "Authoritarianism Goes Global: Cyberspace Under Siege.", p. 72
[242] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 163
[243] Flonk, Jachtenfuchs, and Obendiek, "Authority Conlifcts in Internet Governance: Liberals vs. Sovereignists?", p. 374
[244] Gaufman, "Cybercrime and Punishment: Security, Information War, and the Future of Runet.", p. 127

This period marked probably the biggest turning point when it comes to Internet regulation in Russia. While the previous sections already referred to certain Internet regulation related mechanisms, they served more both as a technological and ideological foundation upon which further regulation escalated after the mass protests. Only in this period, the Kremlin started to see Internet regulation a tool "against perceived external attempts at regime change."[245] While the Arab Spring convinced the Kremlin that the narrative adopted in mid-2000s was correct, the mass protests following the Duma election made it realise that the approach to the Internet up until that moment ("a combination of DDOS attacks and trolls") was not sufficient. For that reason, it adhered to filtering, albeit mediated through ISPs.[246]

The Kremlin drew a big lesson from the public's use of social media during the 2011 protests and learned how to limit their use for the regime benefits. It had learned, that "internet communication can encourage dissidence by providing access to new information that can reshape citizen's attitudes."[247] As such, it had learned that it needed to access these attitudes and expanded the SORM technology to encompass social media. Following Bunce's and Koesel's suggestion that authoritarian leaders interested in "protest-proofing" are expected to limit "coordinative resources" and control "organisational space"[248], indeed, we can see that Putin's strategy towards the Internet, particularly social media, followed this logic. While maintaining the same foreign policy goals as in the previous period in the form of an anti-Western rhetoric, its approach to Internet regulation was significantly sophisticated. Therefore, a considerable degree of simple learning can be identified. Importantly, the offline-online attribute of Russia's digital authoritarianism was found in this period, where the Internet regulative measures are complemented with anti-extremism and/or anti-slander laws, together with pursuing a protective societal narrative.

[245] Gaufman., p. 115
[246] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 172
[247] Gainous, Wagner, and Ziegler, "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections.", p. 211
[248] Koesel and Bunce, "Diffusion-Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations against Authoritarian Rulers.", p. 755 ¨

4.4 Snowden, Euromaidan, and the annexation of Crimea (2013 – 2021)

Edward Snowden's revelations about the NSA's secret mass surveillance programme in the US have changed the global debate about "digital security and surveillance."[249] For Putin's Russia, his revelations represented a handy opportunity to argue for more regulation and pursue the notion of digital sovereignty in order to prevent "the surrender of Russian citizen's data to the American intelligence agencies."[250] Arguably, having this argument is something the Kremlin had been longing for because it allowed it to force Western companies that proved dangerous to the regime stability in the previous period (e.g. Facebook, Twitter) to "put their servers on Russian soil" and "to be subject of Russian legislation."[251] Since 2015, international Internet companies have been legally obliged to run servers in Russia in order to store personal data of Russian citizens.[252] Effectively, the security agencies received more leverage over the Internet based on the argument that Russian personal data need to be protected from the threat of American surveillance.[253] Consequently, Google had put servers to a data center of Rostelecom – a state controlled operator.[254] Overall, the Kremlin has not been consistent in enforcing the requirement. For example, while both LinkedIn and Facebook refused to relocate servers to Russia, only LinkedIn was banned in 2016[255] whereas Facebook continued its business without following the 2015 law.[256] Nevertheless, the law served as a legal justification for financially penalising the companies. In February 2020, both Twitter and Facebook were fined 4 million roubles for not storing data on

[249] Gaufman, "Cybercrime and Punishment: Security, Information War, and the Future of Runet.", p. 121
[250] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 210
[251] Soldatov and Borogan., p. 210
[252] Gainous, Wagner, and Ziegler, "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections.", p. 220
[253] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 217
[254] Soldatov and Borogan., p. 220
[255] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 25
[256] Vera Zvereva, "State Propaganda and Popular Culture in the Russia-Speaking Internet," in *Freedom of Expression in Russia's New Mediasphere*, ed. Mariëlle Wijermars and Katja Lehtisaari (London: Routledge, 2020)., p. 226-227

Russian soil.[257] Similarly, Google was fined 3 million roubles for failing to remove blacklisted content by Roskomnadzor.[258]

Snowden's leak ignited also international action. In April 2014, there was a global conference NETmundial dedicated to Internet governance held in Sao Paulo. Putin had sent his special delegate who argued against the authoritative role of ICANN and wanted to make the intergovernmental organisation ITU the main global regulative body – his remarks were ignored and were not included in the conference's documents.[259] All these events made Putin conclude that the whole Internet was a special CIA project[260] and an "unwelcome source of Western influence on Russian electronic media." [261] As such, he made the societal narrative underpinning Internet regulation even more hostile and viewed Russia as a "fortress besieged by outsiders and underlined the increased state pressure on political uses of the Internet."[262]

When the then-president of Ukraine Yanukovych fled Kiev in the spring of 2014, the Kremlin's concern about domestic uprising resurfaced.[263] With the annexation of Crimea, Putin's popularity increased, and nationalist (anti-Western) attitudes were revived which allowed the Kremlin to regulate the Internet further[264] and to "frame opponents as either extremist or traitors."[265] Indeed, in his speech connected to the annexation, Putin had repeated that "the colour revolutions and the Arab Spring were engineered from the West."[266] As already shown, Russia had been working with the pro-regime activists also in the online domain. In March, activists started a new website predatel.net to flag national traitors (usually "unpatriotic" liberals) and collect their public

[257] "Russia: Growing Internet Isolation, Control, Censorship - Authorities Regulate Infrastructure, Block Content," *Human Rights Watch*, 2020, https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship#_ftn2.
[258] Madeline Roache, "How Russia Is Stepping Up Its Campaign to Control the Internet," *Time*, 2021, https://time.com/5951834/russia-control-internet/.
[259] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 238
[260] Howells, *Digital Authoritarianism in China and Russia: A Comparative Study*., p. 38
[261] Gainous, Wagner, and Ziegler, "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections.", p. 221
[262] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 24
[263] Natalya Kovaleva, "Russina Information Space, Russian Scholarship, and Kremlin Controls," *Defense Strategic Communications* 4 (2018): 133–71., p. 155
[264] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 19
[265] Gainous, Wagner, and Ziegler, "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections.", p. 221
[266] Pallin, "Internet Control through Ownership: The Case of Russia.", p. 19

declarations. It did not omit Alexei Navalny, Boris Nemtsov as well as other activists and public figures who took part in Bolotnaya protests.[267]

Consequently, in 2014, Putin thought it was necessary for Russia to "take into account the risks and threats that exist in the information space as foreign powers use the Internet to pursue political and military objectives against Russia".[268] In the same year, the SORM technology was upgraded once again and started to use "deep packet inspection (DPI) technology (…) that enables the provider not only to monitor the traffic but also to identify the data stream users who discuss certain topics or visit certain websites or social media (…) which brought the Russian system much closer to the idea of mass surveillance"[269] that is one of the core elements of digital authoritarianism. Moreover, the same upgrade also required ISPs to store the information for 12 hours.[270]

Just as Russia finally had some leverage over the Western companies such as Facebook, Twitter, or Google, it needed to develop some leverage over two most popular domestic companies - VKontakte and Yandex. The main rationale behind this was to make people share the Kremlin's perception of what is happening in Ukraine and for that, these two companies were crucial.[271] The way this was done was through infiltrating the ownership structures, just like with the influential platform LiveJournal in 2007, through new legal regulations, as well as with a pressure from FSB. In terms of VKontakte, the FSB demanded for Durov to "hand over the personal data of organisers of the Euromaidan groups" and to "close down the anticorruption group of Alexei Navalny."[272] When he did not comply, he was removed from his chief executive position by the two major shareholders – oligarchs Igor Sechin and Alisher Usmanov.[273] Allegedly, because he was offsetting VKontakte revenues to work on a new messaging platform Telegram.[274] Eventually, Durov emigrated from Russia and Usmanov acquired VKontakte[275] which provided him and his

[267] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 260
[268] Nisbet, Kamenchuk, and Dal, "A Psychological Firewall? Rick Perceptions and Public Support for Online Censorship in Russia.", p. 960
[269] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 21
[270] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 212
[271] Soldatov and Borogan., p. 291
[272] Soldatov and Borogan., p. 293
[273] Soldatov and Borogan., p. 293
[274] Pallin, "Internet Control through Ownership: The Case of Russia.", p. 25
[275] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 22

Mail.Ru Group with a reach to "92 million Internet users a month."[276] The main page of mail.ru also offers the most popular news stories of the day.[277]

To deal with Yandex, the Kremlin's strategy was more complicated. As already mentioned, apart from being a highly popular search engine, Yandex was also aggregating news. Facing Yandex's influential top five news stories list, Putin argued that at the company's beginnings, it was "forced to accept Americans and Europeans in its management" and complained that it was partly registered abroad which started to resemble his rhetoric about the Internet being a CIA project and that there are fifth columnists inside Russia.[278] At first, the CEO of the state-owned Sberbank joined the Yandex's board to mitigate this criticism. Nevertheless, a new initiative was announced to require Yandex to register as a media company which happened later that year when Yandex officially registered its three services – its cloud service, social network, and mail system – with Roskomandzor. It had to store metadata for six months and allow access to FSB. The same happened with Mail.ru and VKontakte.[279] Moreover, since 2016, Yandex News had a legal liability "for its results linking to media outlets not registered with Roskomnadzor."[280] Consequently, alternative news were almost eliminated from Yandex's news index which further increased the domination of the pro-Kremlin online narrative.[281]

Furthermore, because Yandex Money was used to raise money for the 2011 protests, in 2014, a new legislation had set a limit for anonymous donations to 1000 rubles.[282] To limit the opposition further, in May 2014, 'Law Against Money Laundering' was adopted under which it was possible to restrict candidates' crowdfunding campaigns.[283] Relatedly, under the 'Law Prohibiting the Distribution and Financing of Extremist Activity, including on the Internet' from June 2014, financing extremist activity could lead up to three years in prison.[284] In other words, the Kremlin

[276] Pallin, "Internet Control through Ownership: The Case of Russia.", p. 25
[277] Zvereva, "State Propaganda and Popular Culture in the Russia-Speaking Internet.", p. 235
[278] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 295-296
[279] Soldatov and Borogan., p. 296, 302-303
[280] Daria Kravets and Florian Toepfl, "Gauging Reference and Source Bias over Time: How Russia's Partially State-Controlled Search Engine Yandex Mediated an Anti-Regime Protest Event," *Information, Communication & Society*, 2021, 1–17., p. 6
[281] Kiriya, "From 'Troll Factories' to 'Literring the Information Space': Control Strategies Over the Russian Internet.", p. 23
[282] Pallin, "Internet Control through Ownership: The Case of Russia.", p. 26
[283] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 25
[284] Lonkila, Shpakovskaya, and Torchinsky., p. 25

started to approach Yandex because it saw its potential in facilitating protests – both with money and information.

In 2017, Navalny's Fight Against Corruption Foundation published a video investigating corruption around Dimitry Medvedev. It went viral on YouTube gathering more than 22 million views and inspired popular protests in March the same year after the authorities refused to investigate the corruption – the Moscow Court labeled the video's content as unfounded and as an attempt "to discredit the honour, dignity, and reputation of the top state official."[285] Influencing the ownership structure of Yandex search engine and its news aggregator Yandex News proved to be instrumental during these protests. Representative of the state-owned Sberbank joined the Yandex board, already in 2014. By 2020, through Sberbank, the Kremlin possessed "a so-called 'golden share' in Yandex."[286]. Toepfl's and Kravets' comparative study of Yandex's and Google's search results during and after the 2017 anti-corruption protests in Moscow has shown that this significantly influenced search results in times of regime crisis. Compared to Google, Yandex's results were biased against the protesters and sources critical of the Kremlin.[287] For example, upon entering "demonstration" in Yandex, the user would not be presented with a reference to the anti-corruption protest in Yandex's top five list at any point during 20-month period after the protests that was analysed by Topefl and Kravets.[288]

Even though Putin's popularity increased, and most Russians welcomed the annexation of Crimea, it was still necessary to sustain this conviction. Therefore, the Kremlin was further elaborating on the use of the blacklist introduced in the previous period. Popular anti-government sites ej.ru, kasparov.ru, and grani.ru, were blocked due to their alleged extremist nature, because they "contained incitements to illegal activities and participation in mass action conducted without respect for the established order."[289] Similarly, Navalny's blog on LiveJournal was blacklisted when he published poll results organised by his activists that revealed that 84.5% of respondents "viewed Ukraine as a friendly country"[290], and a Moscow court had invoked a house arrest upon

[285] Kovaleva, "Russina Information Space, Russian Scholarship, and Kremlin Controls.", p. 158
[286] Kravets and Toepfl, "Gauging Reference and Source Bias over Time: How Russia's Partially State-Controlled Search Engine Yandex Mediated an Anti-Regime Protest Event.", p. 6
[287] Kravets and Toepfl., p. 13
[288] Kravets and Toepfl., p. 13
[289] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 24
[290] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 261-262

him.[291] Related to the events in Ukraine, a performance artist in Novosibirsk was trying to mirror Russia's discourse about federalisation of Ukraine that served to defend the separatist conflict. When he organised a rally supportive of a bigger autonomy of Siberia from Moscow, Ukrainian outlets such as obozrevatel.com, glavcom.ua, or delo.ua published an interview with him conducted by the Russian BBC. When they refused Roskomnadzor's requests to delete the interview, they were all blocked on Russian territory.[292] Similarly, other Ukrainian sites such as liga.net and correspondent.net got blocked for sharing statements of Crimean Tatars who criticized the annexation. In 2016, RFE/RL's project 'Crimea Realities' got blocked by Roskomnadzor for promoting "extremism and incitement of inter-ethnic hatred."[293]

During Euromaidan protests, the blacklist law was upgraded to warrantlessly block sites that encourage attendance on unauthorised rallies[294] with the so-called 'Lugovoi law'.[295] In March 2014, the Kremlin complained that the news website lenta.ru is informing about the Ukraine events in favour of the Ukrainian government because it shared an interview with a Ukrainian far right party representative.[296] After having received warnings from Roskomandzor about publishing extremist material, its owner fired the whole editorial team[297] because the editor refused to fire the interview's author.[298] The logic of supressing oppositional voices in the online sphere is particularly visible on the case of ej.ru because it often contained opinions of various liberal commentators that were barred from television and other typical media in the 2000s. When it criticized the wave of patriotism and propaganda related to the annexation of Crimea, it got blocked.[299]

---

[291] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 24

[292] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 271

[293] Kovaleva, "Russina Information Space, Russian Scholarship, and Kremlin Controls.", p. 157

[294] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 263

[295] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 24

[296] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 261

[297] Kovaleva, "Russina Information Space, Russian Scholarship, and Kremlin Controls.", p. 151

[298] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 261

[299] Soldatov and Borogan., p. 262

Following the anti-Western narrative, the Kremlin had built up on the 'Foreign Agent Law' mentioned in the previous section with a new 2015 law that set up a 20% limit for foreign ownership of media enterprises[300] under the rationale that Russians needed to be "protected from foreign influences and values that threaten Russian society."[301] Consequently, many foreign publishers (who were the main proponents of balanced journalism and high standards) left Russian media market, such as German Axel Springer[302] who sold the Russian part of Forbes, or Finnish Sanoma who sold all of its shares of the "influential Russian daily Vedomosti, as well as the English-language platform The Moscow Times."[303] In 2017, Russia passed yet another law on foreign agents. This time it was dealing with media outlets in response to the fact that the US demanded Russia Today to register as a foreign agent on its soil.[304] This law was further amended throughout 2019 and 2020 to legally label individuals as well as digital media outlets as foreign agents. Because of this, in 2021, the Kremlin fined Radio Free Europe/Radio Liberty 150 000 dollars for failing to add the "foreign agent" label to its content.[305]

To further limit the activity of bloggers, in 2014, a new "Bloggers Law" was adopted which required those with more than 3000 daily readers to register with Roskomandzor as mass media outlets and to conform with the same regulations.[306] Effectively, that meant equal treatment and/or prosecution in terms of the "accuracy of information published."[307] Moreover, the law also forbade bloggers' anonymity and required social media companies to have records of all their posts in the past six months.[308] Russia had also started to brand itself as a protector of traditional values as opposed to the "morally corrupt West". One example of this is the adoption of the "so-called 'Gay

[300] Kovaleva, "Russina Information Space, Russian Scholarship, and Kremlin Controls.", p. 152
[301] Katja Lehtisaari, "Formation of Media Policy in Russia: The Case of the Iarovaia Law," in *Freedom of Expression in Russia's New Mediasphere*, ed. Katja Lehtisaari and Mariëlle Wijermars (London: Routledge, 2020), 57–75., p. 61
[302] Litvinenko and Toepfl, "The 'Gardening' of an Authoritarian Public at Large: How Russia's Ruling Elite Transformed the Country's Media Landscape After the 2011/12 Protests 'For Fair Elections.'", p. 233
[303] Kovaleva, "Russina Information Space, Russian Scholarship, and Kremlin Controls.", p. 152
[304] Shaun Walker, "Russian Parliament Votes for Law That Could List CNN as 'Foreign Agent,'" *The Guardian*, accessed August 10, 2022, https://www.theguardian.com/world/2017/nov/15/russia-to-register-international-media-as-foreign-agents.
[305] Justin Sherman and Dylan Myles-Primakoff, "The Kremlin's Latest Target Is Online Media: Why the Russian Government Is Now Equating Digital Journalism with Foreign Espionage.," *Foreign Policy*, 2021, https://foreignpolicy.com/2021/03/02/the-kremlins-latest-target-is-online-media/.
[306] Gainous, Wagner, and Ziegler, "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections.", p. 220
[307] Litvinenko and Toepfl, "The 'Gardening' of an Authoritarian Public at Large: How Russia's Ruling Elite Transformed the Country's Media Landscape After the 2011/12 Protests 'For Fair Elections.'", p. 232
[308] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 215

Propaganda Law' (…) that prohibits the distribution of propaganda on non-traditional sexual relations among minors."[309] Evaluating this new legislative reality in Russia, the Freedom House had changed its evaluation of the Internet freedoms in Russia to "not free".[310]

Russia has not been only reactive on social media. Gunitsky argues that social media can function as an "early-warning system for the government, alerting policy makers when certain policies just are not working or need modification to prevent unrest."[311] To get this intelligence, the Kremlin launched an online platform 'Russian Public Initiative' that allowed Russians to propose policy changes on all levels and if a certain proposal gather enough support (federal level changes required 100 000 votes), it will be debated.[312] Overall, this period marked an increase in the Kremlin's collaboration with various organisation regarding the online environment. Among them were public relations and social media marketing companies that were paid to monitor "the opposition segment of Runet."[313] One of them was an American company Crimson Hexagon that collaborated with the authorities on a system called Mediaimpuls, designed to "figure out consumer data on social networks" and monitor networks such as LiveJournal, Twitter, as well as Russian social media.[314] The rationale behind this was that in order the propaganda to work, the ideological message needed to be disseminated in line with contemporary digital media trends to be able to reach different audiences in an appealing way ("as a story, image, game, video or as merchandise"[315]).

With a more controversial foreign policy that included the annexation of Crimea and the war in eastern Ukraine, the Kremlin needed to visualise itself in the online sphere to get the audience on its side. For that, it strived to build an online visual culture that would attract mass audience[316] and to turn Runet into a tool of "propaganda and counter-propaganda, aimed at users both in Russia and abroad."[317] One example of this was strategy used in the days that followed the annexation of

[309] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 27
[310] Sanja Kelly et al., "Freedom on the Net: Privatizing Censorship, Eroding Privacy" (Freedom House, 2015).
[311] Gunitsky, "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability.", p. 47-48
[312] Gunitsky., p. 48
[313] Zvereva, "State Propaganda and Popular Culture in the Russia-Speaking Internet.", p. 230
[314] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 282 – 283
[315] Zvereva, "State Propaganda and Popular Culture in the Russia-Speaking Internet.", p. 235
[316] Fedor and Fredheim, "'We Need More Clips about Putin, and Lots of Them:' Russia's State-Commissioned Online Visual Culture.", p. 162
[317] Zvereva, "State Propaganda and Popular Culture in the Russia-Speaking Internet.", p. 225

Crimea. Contrary to the expectation that the annexation will be complemented with cyberattacks on Ukrainian infrastructure, the Kremlin orchestrated a propaganda campaign on social media, particularly VKontakte as there were more than 20 million of users in Ukraine.[318]

To increase the effectiveness of the mentioned laws, the Kremlin had found a further use for regime-friendly organisations tied to the state. Violations of these laws were often reported to Roskomnadzor by "pro-government whistle-blowers[319] or "vigilante NGOs"[320] such as 'Cyberguards of the Safe Internet League', created by Orthodox entrepreneurs in 2012 with the support by the minister of communication.[321] Another is called 'Media Guard', a part of the Young Guard of United Russia,[322] that was created in 2013 and by 2015, its roughly 3700 volunteers managed to block 2475 sites. According to Soldatov and Borogan, volunteers competed in who will report the most sites with "extremist content" to Roskomnadzor.[323] According to Kiriya, this form of "digital vigilantism" contributes to user surveillance and relies on collective moral values[324], something that the Kremlin was pushing forward extensively in this period and further on.

Zvereva argues, that these organisations can be perceived as a collective actor to support the regime in "preserving the status quo in the presidency, ensuring stability in the domestic political course, and supporting Russia's foreign policy."[325] This shows that in order to regulate the online sphere, the Kremlin had introduced an equilibrium between more straightforward repressive methods and an atmosphere that encourage users towards pro-regime views.[326] According to Yaykobe and Brannen, the goal of digital authoritarianism is to reshape societies in their

[318] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 280
[319] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 31
[320] Henry and Howells, "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet Governance.", p. 12
[321] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 201
[322] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 31
[323] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 201-202
[324] Kiriya, "From 'Troll Factories' to 'Literring the Information Space': Control Strategies Over the Russian Internet.", p. 20-21
[325] Zvereva, "State Propaganda and Popular Culture in the Russia-Speaking Internet.", p. 227
[326] Kiriya, "From 'Troll Factories' to 'Literring the Information Space': Control Strategies Over the Russian Internet.", p. 21

authoritarian image.[327] By that time, the Kremlin seemed to be aware that the Internet is a useful tool for that, and that especially manipulating search engine results could prove instrumental in this endeavor. Speaking about the necessity that Putin needs to become a brand, Kristina Potupchik from Nashi advocated for creating Putin-related animated content that would be welcomed by school children because they allegedly "disseminate internet links like crazy", clearly referring to the opportunity of generating good search engine results.[328] As such, according to Zveereva, this collective actor "seeks to monopolise the interpretation of reality and employs many creative and innovative methods to propagate its message."[329] Being aware that the Internet trend had been leaning towards video content, it had come up with innovative methods such as the "state-commissioned 'viral video'" (e.g. the famous propagandist piece *I'm a Russian Occupier*).[330]

Following this logic, the Kremlin invested in the news aggregator project mediametrics.ru that collects content from platforms controlled by the state and offers "live" collection of the most popular stories from social media. Instead of fooling third-party algorithms such as Yandex, the Kremlin created its own project while excluding oppositional content all together.[331] According to Kiriya, this "littering of the information space" contributed to the non-organic traffic to pro-regime websites and made the pro-Kremlin discourse to dominate the online public sphere.[332] Another innovative method was also a quasi-news agency ANNA News that was active on both Western and Russian social media where it was posting highly propagandistic videos preaching the Ukrainian separatists. Another agency of this nature, Novorossia, had been daily posting videos on social media and even raising money for the separatists. The same videos were then shared with pro-regime TV stations and pro-regime bloggers.[333] This goes along the argument of Gunitsky who argued that social media can improve regime legitimacy either by "*discourse framing* that

[327] Yayboke and Brannen, "Promote and Build: A Strategic Approach to Digital Authoritarianism.", p. 2
[328] Fedor and Fredheim, "'We Need More Clips about Putin, and Lots of Them:' Russia's State-Commissioned Online Visual Culture.", p. 170-171
[329] Zvereva, "State Propaganda and Popular Culture in the Russia-Speaking Internet.", p. 227
[330] Fedor and Fredheim, "'We Need More Clips about Putin, and Lots of Them:' Russia's State-Commissioned Online Visual Culture.", p. 162
[331] Fedor and Fredheim., p. 163
[332] Kiriya, "From 'Troll Factories' to 'Literring the Information Space': Control Strategies Over the Russian Internet.", p. 23
[333] Soldatov and Borogan, *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*., p. 285

shapes the perceptions of the public at large, and *counter-mobilization* of the regime's support base."[334] As we can see, the Kremlin had been active in both of these activities.

With the increased surveillance of social media, the Russian authorities also started to prosecute its users for their online behaviour such as comments or even likes and reposts without considering the context of such actions. One journalist was fined 1000 rubles for sharing a picture of her childhood house under the Nazi occupation that contained a Nazi flag.[335] In 2016, two year sentence was imposed on VKontakte user Andrey Bubeyev for reposting content that showed Crimea as part of Ukraine.[336] In another case, a liberal blogger had reposted a leaflet of an activist group "calling for the destruction of corrupt officials' property" – without being the author of the leaflet, he was sentenced to "two years and seven months in a colony with a strict regime and prohibited from occupying certain positions for one year and one month", while other users who reposted the same leaflet did not face any of that.[337] According to Pallin, this unsystematic prosecution contributes to an "atmosphere of uncertainty and randomness".[338] Most analyst concur that the main problem with the mentioned laws, especially the one on extremis, is their vague language.[339] Therefore, the logic of blacklist is problematic mainly because it includes all different kinds of information deemed illegal and as such, "arbitrary enforcement becomes possible."[340] Gel'man argues that the legal regime around Internet governance has created an atmosphere of fear, "especially after the state began prosecuting greater number of opponents and ordinary Russians."[341]

[334] Gunitsky, "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability.", p. 42
[335] Freek Van der Vet, "Imprisoned for a 'like': The Criminal Prosecution of Social Media Users under Authoritarianism," in *Freedom of Expression in Russia's New Mediasphere*, ed. Mariëlle Wijermars and Katja Lehtisaari (London: Routledge, 2020), 209–25., p. 213
[336] Sanja Kelly et al., "Silencing the Messenger: Communication Apps Under Pressure," Freedom on the Net (Freedom House, 2016)., p. 8
[337] Van der Vet, "Imprisoned for a 'like': The Criminal Prosecution of Social Media Users under Authoritarianism.", p. 216
[338] Pallin, "Internet Control through Ownership: The Case of Russia.", p. 17
[339] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 21
[340] Sivetc, "The Blacklisting Mechanism: New-School Regulation of Online Expression and Its Technological Challenges.", p. 40
[341] Van der Vet, "Imprisoned for a 'like': The Criminal Prosecution of Social Media Users under Authoritarianism.", p. 211

As shown, a strong confrontative societal narrative had been underpinning Putin's regulative actions since the colour revolutions, be it against offline enemies (such as Western-funded NGOs) or online enemies (Western based companies such as Facebook or Google). Importantly, compared to the previous period, the Kremlin had found a way how to use the Internet to its advantage and influence public perceptions to endorse the regime's foreign policy. With an aggressive societal narrative characterising the Internet as a dangerous tool of Western enemies, it had stirred this risk perception to legitimise the domestic Internet regulations.[342] The Euromaidan revolution and the subsequent annexation of Crimea pushed forward the necessity to further sophisticate this narrative for the online environment. To make citizens see the Internet as a dangerous milieu, it was upgraded with "prolific use of fear metaphors"[343] and that steps need to be done in order to create a "safe" Internet.[344] Nisbet et al. argue that the Kremlin's campaign that the Internet is full of extremists, contributed to a so-called "psychological firewall" that helped define the perception of Russians' attitudes towards the Internet freedom.[345] Indeed, the 2016 information security doctrine stressed "the need to control the Internet and develop domestic information technology."[346]

Thus, after 2016, Internet controls in Russia intensified. The first example of this intensification is the set of Yarovaya laws that was passed in 2016 and took effect in 2018. Until that time, it represented one of the gravest infringements of (digital) privacy rights in Russia. Allegedly, these were supposed to be laws of a counterterrorist nature "in order to defend the Russian population against the global terrorist threat and combat extremism at home."[347] However, as we could see many times by now, most of the legislature that had consequences for Internet freedoms was framed along the lines of "national security", "anti-extremism", "to protect children" etc. Initially, the laws required withholding of communication metadata for ISPs for one year and three years for mobile phone service providers.[348] Copies of communications' content was required to be stored for six months by the ISPs, as well as to allow the FSB to warrantlessly browse the

[342] Nisbet, Kamenchuk, and Dal, "A Psychological Firewall? Rick Perceptions and Public Support for Online Censorship in Russia.", p. 973
[343] Nisbet, Kamenchuk, and Dal., p. 960
[344] Zvereva, "State Propaganda and Popular Culture in the Russia-Speaking Internet.", p. 225
[345] Nisbet, Kamenchuk, and Dal, "A Psychological Firewall? Rick Perceptions and Public Support for Online Censorship in Russia.", p. 962
[346] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 19
[347] Kovaleva, "Russina Information Space, Russian Scholarship, and Kremlin Controls.", p. 159
[348] Lehtisaari, "Formation of Media Policy in Russia: The Case of the Iarovaia Law.", p. 62

content.[349] If the content was encrypted, the companies were required to "decipher requested information as well as keep cryptographic backdoors in all messaging applications."[350] With the amendments that came into effect in 2018, the metadata eventually had to be stored for six months and the content of conversations for one month.[351]

According to Cynthia Wong, the framing of the laws could in fact empower terrorists and their networks. That is why she argues the laws serve a hidden purpose to limit freedom of expression. She argued that the laws would result in weaker security of Internet and telecommunication companies' services as the data would no longer be properly encrypted and thus "leaving Russian users and businesses vulnerable to unauthorized spying, data theft, and other harms."[352] Besides, according to Human Rights Watch, a plethora encryption tools not falling under Russian law "would still be available to bad actors."[353] Moreover, the law suspiciously targeted youth – a social group that is often instrumental in organising anti-regime protests – by lowering the age for criminal liability to 14 years. Together with punishable actions such as "aiding extremist activity"[354], the laws suspiciously looked more like yet another protest-proofing mechanism. This followed the behavioural changes among the youth. According to Levada Centre, "the use of traditional TV as a news source among 18 to 24 years old Russians decreased from 81% in 2013 to 60% in 2016", while at the same time, their reliance on "the use of online news media as sources of information increased from 55% in 2013 to 73% in 2016."[355]

However, this was not the only problem as the requirements set by the laws seemed to be unrealistic. There was not enough infrastructure to store the required data and it would have had to be imported from abroad[356] - something that directly contradicts the notion of digital sovereignty pursued by the Kremlin. Moreover, the laws did not assume any aid of the state in building such domestic infrastructure and thus putting a strain on telecommunications companies with cost that

[349] "Russia: 'Big Brother' Law Harms Security, Rights - Repeal Rushed Counterterrorism Legislation," *Human Rights Watch*, 2016, https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights.
[350] Kovaleva, "Russina Information Space, Russian Scholarship, and Kremlin Controls.", p. 159
[351] Lehtisaari, "Formation of Media Policy in Russia: The Case of the Iarovaia Law.", p. 62
[352] "Russia: 'Big Brother' Law Harms Security, Rights - Repeal Rushed Counterterrorism Legislation."
[353] "Russia: 'Big Brother' Law Harms Security, Rights - Repeal Rushed Counterterrorism Legislation."
[354] "Are Russia's Anti-Terror Laws Designed to Fight Democracy?," *Deutsche Welle*, 2016, https://www.dw.com/en/about-dw/s-30688.
[355] Litvinenko and Toepfl, "The 'Gardening' of an Authoritarian Public at Large: How Russia's Ruling Elite Transformed the Country's Media Landscape After the 2011/12 Protests 'For Fair Elections.'", p. 235
[356] Kovaleva, "Russina Information Space, Russian Scholarship, and Kremlin Controls.", p. 160

could had led to bankruptcy.[357] Overall, the legislation further increased the scope of surveillance in Russia's digital authoritarianism and perhaps more importantly, the legal justification for peeking into users' communication. Arguably, as online communication data was required to be stored for an extensive period, it also further contributed to online self-censorship among casual users out of fear of prosecution[358] which also further supports the notion of psychological firewall.

Further evidence of Kremlin's decisive action against online public sphere was its decision to ban the messaging app Telegram after it refused to follow "anti-terrorism" Yarovaya laws requiring technological companies to provide the FSB with access to encrypted data. Indeed, Telegram could have been detrimental to regime stability as, in 2018, it was used by 28% of smartphone users in Moscow and the most popular channels were those related to politics and news in general.[359] In the aftermath of the ban, after Telegram tried to bypass the blocking, Roskomnadzor initiated a serious witch-hunt campaign that ended up blocking at least 18 million IP addresses ranging from "news sites, smart television sets, and even airline ticketing systems in the process."[360] Ironically, this resulted in an opposite effect than the Kremlin wanted. Pavel Durov's decision not to give up the encryption keys increased the platform's popularity - its "traffic increased by a third in the first month, while the number of app downloads for Android jumped twice."[361] Since the ban failed in reducing the usage of Telegram, Roskomnadzor lifted the restrictions in 2020.[362]

In 2017, Russia started to regulate VPNs that started to be increasingly used to circumvent Roskomandzor's blocking. Initially, with questionable success, the law required for VPN providers to follow Roskomnadzor's blacklist and refrain Russian users from accessing listed pages.[363] Subsequently, websites that were offering VPNs were to be blocked by ISPs. In one instance, the local offices of one foreign VPN provider – Private Internet Access – were raided by

[357] Kovaleva., p. 160
[358] Litvinenko and Toepfl, "The 'Gardening' of an Authoritarian Public at Large: How Russia's Ruling Elite Transformed the Country's Media Landscape After the 2011/12 Protests 'For Fair Elections.'", p. 233
[359] Azadeh Akbari and Rashid Gabdulhakov, "Platform Surveillance and Resistance in Iran and Russia: The Case of Telegram," *Surveillance & Society* 17, no. 1/2 (2019): 223–31., p. 227
[360] Shahbaz, "The Rise of Digital Authoritarianism.", p. 15
[361] Gaufman, "Cybercrime and Punishment: Security, Information War, and the Future of Runet.", p. 119
[362] Henry and Howells, "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet Governance.", p. 11
[363] Litvinenko and Toepfl, "The 'Gardening' of an Authoritarian Public at Large: How Russia's Ruling Elite Transformed the Country's Media Landscape After the 2011/12 Protests 'For Fair Elections.'", p. 233

the authorities and their servers seized.[364] The same regulation also obliged search engines to refrain from displaying blacklisted content.[365] In 2018, after VPNs started to be increasingly used to access officially blocked Telegram, Roskomnadzor blocked 50 VPN providers that were used to access it.[366] This shows, that when the blacklist mechanism was failing, the authorities resorted to traditional offline authoritarian means. In a similar manner, Roskomnadzor requested YouTube several times to block Navalny's video that instigated the 2017 anti-corruption protest, however, with no success.[367] After failing to mitigate this event in the online sphere, the Kremlin resorted to offline means and arrested the editor of Navalny Live.[368]

In the second half of 2010s, the Kremlin increasingly started to propose ideas and legislature that followed the logic of digital sovereignty and demonstrated the perception of Internet alongside physical national borders. The willingness to protect its sovereignty in information domain via independent policy and independent management of its "national system of Russian Internet segment" was demonstrated already in the 2016 Information Security Doctrine. Such national system would lead to a control of the routing infrastructure and the information within.[369]

In 2017, the Security Council tasked the Ministry of Communication to come up with "proposals for the creation and implementation of a state information system to ensure the integrity, stability, and security of the Russian segment of the Internet, as well as replacement root servers for national top-level domain names."[370] Accordingly, the Law on Communications was amended which handed the control of domains .ru and .pф to the government, as well as the control of traffic exchange points – the argument for such amendments was that Runet's infrastructure was threatened with foreign interference. Because of this, in the same vein as with the foreign ownership of media outlets, the amendments set a 20% limit on foreign ownership of the Internet

[364] Sanja Kelly et al., "Manipulating Social Media to Undermine Democracy," Freedom on the Net (Freedom House, 2017)., p. 24
[365] Sivetc, "The Blacklisting Mechanism: New-School Regulation of Online Expression and Its Technological Challenges.", p. 44
[366] "Russia: Growing Internet Isolation, Control, Censorship - Authorities Regulate Infrastructure, Block Content."
[367] Kovaleva, "Russina Information Space, Russian Scholarship, and Kremlin Controls.", p. 158
[368] Andrei Soldatov and Irina Borogan, "The New Iron Curtain Part 3: The Internet Is a Western Plot" (CEPA (Center for European Policy Analysis), 2022), https://cepa.org/the-new-iron-curtain-part-3-the-internet-is-a-western-plot/.
[369] Kerttunen and Tikk, "The Politics of Stability: Cement and Change in Cyber Affairs.", p. 56
[370] Soldatov and Borogan, "The New Iron Curtain Part 3: The Internet Is a Western Plot."

exchange points.[371] Soldatov and Borogan characterised this as "the first systemic effort to control Russian cyberspace."[372]

Throughout 2017, the Kremlin started to build a single control center in Moscow that would be able to monitor and control Internet traffic within Russia with the ability to shut down Internet access regionally "without relying on regional enforcers."[373] During 2018-19, this center was put into action and organised regional isolations as a tool of crisis management. There was a regional unrest in Ingushetia that included cries for separatism – the Kremlin responded with blocking of cellular data service. During disturbances over border disputes with Chechnya, the state security requested network blackout with local mobile service suppliers.[374]

In 2019, the Kremlin's decisive switch towards centralised Internet governance intensified with the so-called 'Sovereign Internet Law'. According to Levada Center, Putin's approval rating was the lowest since the annexation of Crimea. Compared to 2018, when he enjoyed popularity of 80% of Russians, it was now only 64%. Moreover, the whole federal government scored even worse and reached 38% approval rating and 61% disapproval rating.[375] Amid these societal moods, the Kremlin started to further develop legal and technological framework for digital sovereignty, allegedly because of a "new, more aggressive US national cybersecurity strategy.[376]

With this law, the Kremlin wanted to further sophisticate its capacity of online surveillance based on a more centralised approach – Roskomnadzor no longer wanted to rely on ISPs in implementing its requests and to be able to "monitor traffic at its source."[377] With the requirement for the ISPs to install deep packet inspection technology, the Kremlin wanted the users not to be able to access undesired content "by using direct commands, which the authorities have programmed, without the users or ISPs even noticing."[378] While this technology has been used in Russia since the creation of the blacklist mechanism, the ISPs were reluctant in introducing them

[371] Kovaleva, "Russina Information Space, Russian Scholarship, and Kremlin Controls.", p. 145-146
[372] Soldatov and Borogan, "The New Iron Curtain Part 3: The Internet Is a Western Plot."
[373] Soldatov and Borogan.
[374] Henry and Howells, "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet Governance.", p. 9
[375] Dimitri Simes, "Poll: Putin's Popularity Falls from 80% to 64%, Lowest in 5 Years," *CNS News*, 2019, https://www.cnsnews.com/news/article/dimitri-simes/poll-putins-popularity-falls-80-64-lowest-5-years.
[376] David Gilbert, "Russia Is Building Its Own Version of China's Great Firewall," *Vice News*, 2019, https://www.vice.com/en/article/gyakjx/russia-is-building-its-own-version-of-chinas-great-firewall.
[377] Alena Epifanova, "Deciphering Russia's 'Sovereign Internet Law': Tightening and Accelerating the Splinternet" (The German Council on Foreign Relations (DGAP), 2020).
[378] "Russia: Growing Internet Isolation, Control, Censorship - Authorities Regulate Infrastructure, Block Content."

widely due to their high costs. This time, Roskomnadzor was to provide the technology free of charge.[379] Interestingly, the technology was provided from abroad – from China, Israel, as well as the US. While Israeli company provided the DPI technology, the Chinese and American companies provided servers for Roskomnadzor's monitoring center.[380]

The DPI technology was supposed to be disseminated across the country, but crucially, also at the national internet exchange points. As such, Roskomnadtzor made further steps towards the centralisation of control over communication lines crossing Russian borders.[381] The ambition and legal basis for controlling national Internet exchange points (IXP) represent the main novelty of this regulation. Again, the owners of these network were expected to install the DPI technology that would allow more thorough analysis and filtering of Internet traffic, including the state's ability to block digital content without the need of ISP's cooperation.[382] There is over 40 IXPs in Russia and to isolate Runet, all of them would have to be connected to the Moscow IXP. Even though three years have passed since the adoption of the law, according to Cyber Threat Intelligence Platform Flashpoint, due to the high complexity of the task, it is extremely unlikely that Russian infrastructure is ready for this.[383]

Furthermore, it included a plan to build a separate Russian Domain Name System (DNS) – something that no country has achieved so far and "would only make sense if a country opts for a long-term and complete isolation of its internet."[384] However, according to Epifanova, the main goal is not to isolate Russia from the global Internet, "but rather to create a precedent, which other states aspiring to sovereignty over their segments of the Internet could follow."[385] This goes along the notion of "norm regression in global governance" as characterised by Deibert and Crete-

[379] Epifanova, "Deciphering Russia's 'Sovereign Internet Law': Tightening and Accelerating the Splinternet.", p. 4-5
[380] Andrei Soldatov and Irina Borogan, "The New Iron Curtain Part 4: Russia's Sovereign Internet Takes Root" (CEPA (Center for European Policy Analysis), 2022), https://cepa.org/the-new-iron-curtain-part-4-russias-sovereign-internet-takes-root/.
[381] Epifanova, "Deciphering Russia's 'Sovereign Internet Law': Tightening and Accelerating the Splinternet."
[382] Baurzhan Rakhmetov, "The Putin Regime Will Never Tire of Imposing Internet Control: Developments in Digital Legislation in Russia," *Council On Foreign Relations*, 2021, https://www.cfr.org/blog/putin-regime-will-never-tire-imposing-internet-control-developments-digital-legislation-russia.
[383] "Understanding Russia's 'Sovereign Internet': What Happens If Russia Isolates Itself from the Global Internet?" (Flashpoint, 2022), https://flashpoint.io/blog/russian-runet-sovereign-internet/.
[384] Epifanova, "Deciphering Russia's 'Sovereign Internet Law': Tightening and Accelerating the Splinternet.", p. 8
[385] Epifanova., p. 2-3

Nishihata, because building a national DNS goes directly against the logic of cyberspace as "open commons of information and communication."[386]

The legal codification of national DNS system can be understood as a culmination of the years-long effort of challenging the authority of ICANN in managing the global DNS. Already in 2010, during the ITU meeting in Guadalajara, Russia proposed that governments should be able to veto decisions taken by ICANN, effectively proposing that the UN and its specialised intergovernmental organisation ITU should be able to veto the private sector.[387] Moreover, they proposed that governments ought to be able to decide which international routes will be used for internet traffic leading to their national cyberspace.[388] According to Epifanova, building a national DNS makes sense only in alliance with other countries. In this effort, the main partner is China because it shares the perception of international politics with Russia, stressing the importance of state sovereignty above all. In 2015, a bilateral agreement on "cooperation in the field of international information security" was outlined between Russia and China. They vowed to create mutual means of communication to "jointly respond to threats" but also to cooperate "in the development and promotion of international law standards to ensure national and international information security."[389] Accordingly, the presidents of both countries have been underlining importance of "respecting national sovereignty in information space" in joint statements and China has continuously been supporting Russian proposals regarding cyberspace regulation at the level on UN.[390] In 2018, Chinese government officials invited their Russian counterparts to join their seminars on information management.[391]

In fact, the Kremlin's discussions about Runet's isolation date back to 2014 when the Russian security council discussed for the first time the possibility to disconnect Runet from the global internet in times of crisis or emergency such as war times or serious anti-regime protests.[392] In 2015, Russian officials were conducting experiments "to test the model of Runet isolation, and in

[386] Deibert and Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls.", p. 341
[387] Gregory Francis, "Plutocrats and the Internet," CircleID, October 4, 2010, https://circleid.com/posts/20101004_plutocrats_and_the_internet.
[388] Flonk, Jachtenfuchs, and Obendiek, "Authority Conlifcts in Internet Governance: Liberals vs. Sovereignists?", p. 374
[389] Epifanova, "Deciphering Russia's 'Sovereign Internet Law': Tightening and Accelerating the Splinternet.", p. 9
[390] Epifanova., p. 9
[391] Shahbaz, "The Rise of Digital Authoritarianism.", p. 8
[392] Luke Harding, "Putin Considers Plan to Unplug Russia from the Internet 'in an Emergency,'" *The Guardian*, accessed August 11, 2022, https://www.theguardian.com/world/2014/sep/19/vladimir-putin-plan-unplug-russia-internet-emergency-kremlin-moscow.

March 2018, German Klimenko, advisor to Putin on questions concerning the internet, announced that the country was technically ready for this."[393] In December 2019, the Kremlin announced that a test of Runet's isolation was successful and that similar tests are supposed to take place on a yearly basis.[394] Since then, however, there has been a silence on that matter and according to Sherman, a complete isolation of Runet is unlikely to manifest in the near future mainly because of technical difficulties faced by the ISPs when installing the supportive equipment.[395]

There are also economic constrains. Howells noted that according to Moscow Times, hardware and software that would be necessary for the Runet's isolation would cost around 134 billion rubles per year (calculated in 2019). Considering that only 30.8 billion rubles were assigned to the 2017 Digital Economy project, the plan for Runet's isolation seemed to be too ambitious because, according to Stadnik, many initial goals of the 2019 law gradually disappeared.[396] Initially, the plan was to have this system up and running in 2021, which did not happen, and as of now, according to Epifanova, Russia still lacks the necessary infrastructure to go through with such ambitions.[397] Moreover, she argues that the Russian economy relies on the global Internet and that it might collapse upon Runet's disconnection[398] as international actors were instrumental in building Russia's internet infrastructure since the outset.[399] Nevertheless, according to Soldatov and Borogan, since the beginning of 2021, Russian ISPs followed Roskomnadzor's demands and started to switch to the national DNS – by the end of that year, "the system controlled 73% of overall Internet traffic and 100% of the country's mobile phone traffic."[400]

---

[393] Lonkila, Shpakovskaya, and Torchinsky, "The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.", p. 21

[394] Howells, *Digital Authoritarianism in China and Russia: A Comparative Study*., p. 41-42

[395] Justin Sherman, "Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behaviour," Issue Brief (Atlantic Council (Scowcroft Center for Strategy and Security), 2021), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/., p. 6

[396] Henry and Howells, "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet Governance.", p. 8-9

[397] David Gilbert, "Russia Is Preparing to Cut Itself Off From the Global Internet," *Vice*, accessed August 11, 2022, https://www.vice.com/en/article/88gevb/russia-is-preparing-to-cut-itself-off-from-the-global-internet.

[398] David Meyer, "Russia's Denying That It's about to Cut Itself off from the Global Internet, but It's Acting a Lot like It," *Fortune*, 2022, https://fortune.com/2022/03/07/russia-runet-disconnect-ukraine-dns-chernenko-letter/.

[399] Tom Bateman, "How Russia Could Cut Itself off from the Global Internet, and Why It Probably Won't," *Euro News*, 2022, https://www.euronews.com/next/2022/03/14/how-russia-could-cut-itself-off-from-the-global-internet-and-why-it-probably-won-t.

[400] Soldatov and Borogan, "The New Iron Curtain Part 4: Russia's Sovereign Internet Takes Root."

As discussed, international companies were invited to build even this project, amid the hostile anti-Western narrative propagated by the Kremlin. The fact that international companies, including American ones, were invited to contribute to Russia's increasingly centralised system of Internet governance further supports the argument that complete digital isolation was not intended and that the 2019 law was to further sophisticate Russia's domestic surveillance capability (albeit with foreign technology) instead of isolating it from the global Internet. Nevertheless, once again, the narrative that the Runet needed to be protected from external threats[401] served as a rationale for adopting this new regulation. According to Soldatov, given the fragile standing of the Kremlin at the time, instead of targeting foreign threats, the law was about being able to "cut off certain types of traffic in certain areas during times of civil unrest."[402]

In December 2019, the Kremlin demonstrated again its willingness to shape the society according to its image by adopting amendments to consumer protection law according to which manufacturers would be required to "pre-install Russian apps on certain types of devices sold in Russia."[403] According to Human Rights Watch, by pre-installing apps such as messengers, browsing services, maps, news readers or email providers, the Kremlin economically incentivised the developers to conform to the regulations on the localisation of user data and their retention.[404]

In 2021, the Kremlin had started to throttle social networks such as Twitter during critical times such as anti-regime protests. Roskomnadzor argued, that it had slowed the network because it "failed to remove content related to child pornography, drugs, and suicide."[405] However, according to 2021 Freedom House report, Twitter was throttled because it refused to "remove information related to protests against the detention of opposition leader Aleksey Navalny."[406] The action had unwanted consequences and resulted in over blocking because Twitter's shortened domain name t.co was targeted, which effectively slowed down over 40 000 domains including some governmental websites and big platforms like Yandex and Google.[407] The way this was done was

[401] Epifanova, "Deciphering Russia's 'Sovereign Internet Law': Tightening and Accelerating the Splinternet.", p. 2
[402] Gilbert, "Russia Is Building Its Own Version of China's Great Firewall."
[403] "Russia: Growing Internet Isolation, Control, Censorship - Authorities Regulate Infrastructure, Block Content."
[404] "Russia: Growing Internet Isolation, Control, Censorship - Authorities Regulate Infrastructure, Block Content."
[405] Richard Nieva and Sarah Emerson, "Facebook And Twitter Have Been Blocked In Russia," *BuzzFeed News*, accessed August 8, 2022, https://www.buzzfeednews.com/article/sarahemerson/russia-blocks-facebook-twitter.
[406] Adrian Shahbaz and Allie Funk, "The Global Drive to Control Big Tech," Freedom on the Net (Freedom House, 2021)., p. 14
[407] "The Return of Digital Authoritarianism: Internet Shutdowns in 2021" (Access Now, 2022), https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf., p. 11

again through the cooptation of ISPs that were asked to execute the governmental agenda.[408] The DPI technology was used to execute this operation. According to Sherman, the collateral damage caused by this action had demonstrated that "DPI deployments are still imperfect and incomplete across the domestic Internet sphere" and as such "technical filtering mechanisms were not sufficiently widely deployed to enable precise filtering of Internet traffic."[409] Upon throttling Twitter that seriously complicated functioning of its mobile app, Roskomnadzor announced that Twitter had complied with 91% of its requests.[410] Continuing with the pressure on international companies, the Kremlin forced Apple to switch off its Private Relay service that encrypts data leaving the user's device.[411]

Before the 2021 Duma elections, Russian authorities made a big effort to make Navalny's Smart Voting App inaccessible. The app provided its users with updates and the possibility to monitor the September elections. Initially, the Kremlin demanded Apple and Google to take the app out of their app stores and while doing so, "government agents also personally threatened local staff at these companies"[412] – according to Washington Post, even with a prison sentence.[413] After the companies complied with the pressure, the government came with its own initiative to temporarily block other assets the app was using such as "VPNs, Google Docs, and YouTube videos used by the Smart Voting project, and the disabling of the Smart Voting chatbot on Telegram."[414] Throughout 2021, content supportive of Navalny was the main target of Roskomandzor's blocking requests on Facebook, Twitter, Instagram and YouTube.[415] Subsequently, after trying to mitigate the threat of mass protests in support of Navalny by online censorship, the police then detained more than 3 700 people across the country when the protests

[408] Henry and Howells, "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet Governance.", p. 9
[409] Sherman, "Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behaviour.", p. 5-6
[410] "Russia Says Won't Block Twitter, Will Keep Throttling Speeds," *The Moscow Times*, 2021, https://www.themoscowtimes.com/2021/05/17/twitter-a73926.
[411] Andrei Soldatov and Irina Borogan, "The New Iron Curtain Part 5: Russia's War Against Silicon Valley" (CEPA (Center for European Policy Analysis), 2022), https://cepa.org/the-new-iron-curtain-part-5-russias-war-against-silicon-valley/.
[412] "The Return of Digital Authoritarianism: Internet Shutdowns in 2021.", p. 19
[413] Soldatov and Borogan, "The New Iron Curtain Part 5: Russia's War Against Silicon Valley," 5.
[414] "The Return of Digital Authoritarianism: Internet Shutdowns in 2021.", p. 19
[415] Andrei Zakharov and Ksenia Churmanova, "How Russia Tries to Censor Western Social Media," *BBC*, 2021, https://www.bbc.com/news/blogs-trending-59687496.

manifested.[416] Moreover, the fact that since the beginning of 2022, foreign Internet companies with more than 500 000 daily Russian users are legally required to open an office in Russia[417] further suggests that a physical intimidation, as was the abovementioned case with Google, is a systematic component of Russia's approach towards popular Western Internet companies. This is another example of how digital authoritarianism works on the logic of offline-online nexus.

Overall, it can be argued that throughout this period, the Kremlin had been significantly sophisticating Russia's digital surveillance capabilities and further elaborating on legal formulations that could be used as a reference to prosecute the surveiled users. While it can be argued that increased regulation of the Internet had begun already after the Bolotnaya protests, the events in Ukraine further prompted the Kremlin to step up this endeavour and come up with other restrictive laws to limit the online public sphere for political purposes. With measures such as influencing ownership structures of influential (social) media companies and search engines, laws that made bloggers to register as media companies with Roskomnadzor, or the narrative about digital sovereignty that allowed to frame international companies as a threat to Russians online, the Kremlin managed to further limit coordinative resources for the opposition "while diffusion-proofing their country against external influences."[418] Importantly, this period added the psychological dimension of the Kremlin's approach towards governing the online public sphere, contributing to an increased societal apathy towards politics. Compared to the 2011 Duma elections that proved to be a highly contested event that resulted in mass protests, Levada Centre found out that during 2016 Duma elections "89% of Russian were either not following the elections very closely, or not at all, while only 9% were following the elections very closely."[419]

This psychological dimension along the lines of "psychological firewall" can be supported by survey data. According to Levada Centre, most Russian were not worried about their freedom on the Internet and in October 2014, 54% of them thought "that censorship on the Internet was necessary" and even more surprisingly, "between a third and half of respondents did not express a

[416] "Russia: Police Detain Thousands in Pro-Navalny Protests - Mass Arbitrary Detentions, Police Brutality, Criminal Prosecutions," *Human Rights Watch*, 2021, https://www.hrw.org/news/2021/01/25/russia-police-detain-thousands-pro-navalny-protests.
[417] Justin Sherman, "This Year, Russia's Internet Crackdown Will Be Even Worse" (The Atlantic Council, 2022), https://www.atlanticcouncil.org/blogs/new-atlanticist/this-year-russias-internet-crackdown-will-be-even-worse/.
[418] Gainous, Wagner, and Ziegler, "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections.", p. 210
[419] Gainous, Wagner, and Ziegler., p. 221

strong opinion when asked about this."[420] In 2016, 70.4% of the Russian population older 16 used the Internet. By this time, according to Volkov and Goncharov, these figures "has begun to coincide with the political majority of the country, the electorate that supports Putin and votes for the ruling party in the elections to the state Duma."[421] According to Levada Centre, this degree of support for Putin "may be a highly impactful factor on risk perceptions and influence how individuals interpret and process information from other sources"[422] and thus further contributes to the notion of psychological firewall. The fact that the Pew Research Centre found out in 2015 that "only 29% of Russian believed the Internet had a positive impact on politics in their country"[423] is also supportive of this logic and may suggest that the notion that Russians needed to be protected from the Internet may had worked. Indeed, according to Levada Centre, in December 2016, 91% of Russians watched news on TV "at least once a week or more frequently" as compared to 46% in the case of Internet.[424] Relatedly, this period marked a significant increase in users' suggestions for Roskomandzor to blacklist certain content – "from 95 600 in 2015 to almost 140 000 in 2016."[425] The Kremlin's increased effort to shape the perception of Russians online is also supported by Sivetc's research that shown that the most popular Russian social network VKontakte was the main target of the blacklist mechanism in 2016 where Roskomnadzor had blocked 19 600 websites out of 88 500 in total in that year.[426] According to Human Rights Watch, "between 2014 and 2016, approximately 85% of convictions for 'extremist expression' were made on the basis of online activities."[427] In terms of prosecutions, Gaufman had argued that most of the prosecuted cases of "digital extremism" originated from VKontakte because of its legal obligations "to share private information with the law enforcement agencies."[428]

[420] Pallin, "Internet Control through Ownership: The Case of Russia.", p. 20
[421] Zvereva, "State Propaganda and Popular Culture in the Russia-Speaking Internet.", p. 232
[422] Nisbet, Kamenchuk, and Dal, "A Psychological Firewall? Rick Perceptions and Public Support for Online Censorship in Russia.", p. 963-964
[423] Nisbet, Kamenchuk, and Dal., p. 962
[424] Kovaleva, "Russina Information Space, Russian Scholarship, and Kremlin Controls.", p. 147
[425] Sivetc, "The Blacklisting Mechanism: New-School Regulation of Online Expression and Its Technological Challenges.", p. 43
[426] Sivetc., p. 41
[427] Henry and Howells, "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet Governance.", p. 14-15
[428] Gaufman, "Cybercrime and Punishment: Security, Information War, and the Future of Runet.", p. 120

One aspect of Russian Internet governance is the model of delegation that is based on the principal-agent theory in which the government authorises agents to execute its competencies while maintaining the possibility to cancel this power delegation.[429] In terms of actors that were invited into the Internet regulatory regime, this period marked a further decentralisation. Even before, the Kremlin had worked with third parties in order to manage the online content, typically the ISPs. Feeling the necessity to gather support for its controversial and daring foreign policy, it started to cooperate with yet other third parties such as social media marketing companies or video makers in order to monitor oppositional online sentiment, as well as to counter this sentiment with content supportive of the regime. This initiative was also aimed internationally as the famous I'm a Russian Occupier that was translated into 10 languages[430] had shown.

Most importantly, the Kremlin had further sophisticated its approach to the Internet across all three generations of cyberspace controls. With the introduction of the 2019 sovereign internet law that included the ambition to control key internet chokepoints in order to be able to filter information, it embarked on a path towards the first generations of controls, albeit, for now, only on the legal level. Initiatives such as building a single control center in Moscow and the ambition to build a national DNS can be considered a step in the same direction and importantly, a step towards infrastructural centralisation of Internet governance in Russia. In terms of the second generation of controls the repressive legal framework for online censorship and surveillance was further elaborated. Here the propagated nation-wide initiative to switch towards DPI technology that ISPs were required to install can serve as the best example. The Kremlin was able to draw a lesson from the fact that ISPs such as Rostelecom were refusing targeted blocking "as too expensive to apply" and that blocking on the level of IP address often caused collateral blocking, sometimes even of Roskomnadzor's own website.[431] The initiative to introduce DPI technology more widely was therefore motivated by a more economical form of censorship than blocking certain websites.[432] Actions in the third generation of controls can be demonstrated on the set of

[429] Moritz Weiss and Vytautas Jankauskas, "Securing Cyberspace: How States Design Governance Arrangements," *Governance*, no. 32 (2019): 259–75., p. 263
[430] Fedor and Fredheim, "'We Need More Clips about Putin, and Lots of Them:' Russia's State-Commissioned Online Visual Culture.", p. 161
[431] Sivetc, "The Blacklisting Mechanism: New-School Regulation of Online Expression and Its Technological Challenges.", p. 48, 51
[432] Glen, "Internet Governance: Territorializing Cyberspace?", p. 646

intrusive Yarovaya laws serves as the best example of surveillance and warrantless monitoring that according to Deibert et al. pertain to this generation.[433]

Crucially however, the overall character of Internet as an oppositional space was transformed in this period. By 2020, there were 78% of monthly and 71% of daily Internet users in Russia.[434] However, it cannot be argued that these number would represent a population prone to oppositional views. Here we must keep in mind all the regulations, narratives as well as legal regimes that had been in place since the 2011 protests and especially after the annexation of Crimea. Indeed, the Internet was not the same place as in 2011 when arguably, being an active Internet and social media user might had led to oppositional views. Kiriya has described this change as "mainstreamisation of the Internet space." His research has shown, that due to ownership and editorial changes, increased online presence of big state media such as rt.com or tass.ru, and influencing news aggregation by the search engines, the share of total monthly reach of state-owned media has increased from 51% in 2012 to 95% in 2020.[435] As such, he argues, that "the Internet (and social media) should no longer be regarded as an oppositional or protest space, but as a part of the whole media landscape oriented towards maintaining the status quo."[436]

4.5 Russia's invasion of Ukraine

The final turning point under my analysis is the 2022 Russia's invasion of Ukraine that prompted the Kremlin to further regulate the Internet and online behaviour of its users. While this is an ongoing issue, some of the Kremlin's initiatives to regulate the online sphere and limit access to information go in line with the narrative and logic of authorities' argumentation that I have been presenting until now – this includes for example the "foreign agents" narrative or the usage of the 'extremist' argument.

The very beginning of the war ignited street protests across all Russia. On February 24th, the first day of the invasion, police detained around 2000 people all over the country, often brutally beating the protesters.[437] On TV, The Ministry of Interior had warned Russians to "refrain from

[433] Deibert et al., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*., p. 27
[434] Kiriya, "From 'Troll Factories' to 'Literring the Information Space': Control Strategies Over the Russian Internet.", p. 20
[435] Kiriya., p. 22
[436] Kiriya., p. 24
[437] "Almost 2,000 Russians Arrested on the First Day of Anti-War Protests," *OVD-Info*, 2022, https://ovdinfo.org/articles/2022/02/27/almost-2000-russians-arrested-first-day-anti-war-protests.

unsanctioned protests" because of COVID-19 restrictions and that attendance could lead to prosecution.[438] Sunday February 27th marked the 7th anniversary of the murder of Boris Nemtsov, a vocal critic of Russia's annexation of Crimea – the protests continued and more than 900 more people were arrested across the country.[439] However, besides the streets, Russians were protesting also in the online environment and media, often with the help of famous public figures. Among them was the pop-star singer Valery Meladze who was begging Russia to stop the war in a videopost on Instagram.[440] The head of the state-funded Moscow theatre – Yelena Kovalskaya – said in a Facebook post that she resigns from her position because "it's impossible to work for a killer and get paid by him."[441] The famous rapper Oxxxymiron who enjoys a large online audience (2.2 million followers on Instagram and 1.3 million on Twitter) labeled the invasion as "a crime and a catastrophe" and canceled his upcoming shows in Moscow and St. Petersburg.[442] Importantly, the dissenting voices did not avoid even the state official media. One of the figures was also the editor of Channel 1, Marina Ovsyannikova, who interrupted an evening news broadcast with an anti-war sign "stop the war, no to war" and "do not believe the propaganda, they are lying to you here".[443]

Generally, the end of February represented a wake-up call for the Kremlin in terms how wide-spread the anti-war sentiment has become. Naturally, controlling information is crucial in war times and the Kremlin is aware of that. The Kremlin's take from February, when it seemed that the anti-war protests were relentless and were happening on daily basis, provided the authorities with incentive to mitigate the threat in a systemic manner. Since the war's outset, the Kremlin

---

[438] Alec Luhn, *Twitter* (blog), February 24, 2022, https://web.archive.org/web/20220226130731/https://twitter.com/asluhn/status/1496869020372398080?s=21.
[439] Andrei Khalip, "Police Detain More than 900 People at Anti-War Protests across Russia - Monitoring Group," *Reuters*, 2022, https://web.archive.org/web/20220227160345/https://www.reuters.com/world/europe/police-detain-more-than-900-people-anti-war-protests-across-russia-monitoring-2022-02-27/.
[440] Pjotr Sauer and Andrew Roth, "Thousands Join Anti-War Protests in Russia after Ukraine Invasion," *The Guardian*, 2022, https://www.theguardian.com/world/2022/feb/24/we-dont-want-this-russians-react-to-the-ukraine-invasion.
[441] Xander Richards, "Nicola Sturgeon Praises Russians' Courage as Anti-War Protests Erupt in Moscow," *The National*, 2022, https://www.thenational.scot/news/19950978.nicola-sturgeon-praises-russians-courage-anti-war-protests-erupt-moscow/.
[442] Lila MacLellan, "A Popular Russian Rapper Canceled Shows and Called for an Antiwar Movement," *Quartz*, accessed August 19, 2022, https://qz.com/2133401/a-major-russian-rapper-canceled-shows-and-called-for-war-protests/.
[443] Pjotr Sauer, "'They'Re Lying to You': Russian TV Employee Interrupts News Broadcast," 2022, https://www.theguardian.com/world/2022/mar/14/russian-tv-employee-interrupts-news-broadcast-marina-ovsyannikova.

made serious effort to frame the invasion along the lines of a "special operation" for the domestic population. To support this notion and to sustain this claim, Russian Duma has passed a new "Fake news law" in March 2022 that introduces criminal liability for sharing of unreliable information about Russian army with up to 15 years in prison. It also promises 3 years in jail for calls for sanctions against Russia.[444] Problematically, this law is about liability for sharing knowingly false information. Therefore, according to RBC, there is an offense against this law only if someone knows the information to be fake before sharing it. However, proving whether the information was truly "knowingly false lies within the prosecution."[445] To avoid any confusion, Roskomnadzor appealed to Russian mass media to cover this event only based on information from official Russian sources.[446]

Simultaneously with the "Fake news law", the Russian Criminal Code was also amended with articles that introduce criminal liability for "discrediting" the actions of Russian army, leading to a possible financial penalisation up to 300 000 roubles or even five years of prison in case the action leads to severe consequences (e.g. mass unrest).[447] Even though the amendments were introduced in March, a woman from Karelia got fined 30 000 roubles for her February post in VKontakte in which she said that "she would not have sent them to Ukraine."[448] In another instance, a lawmaker from Pskov got fined 30 000 roubles for sharing sympathies with the action of Marina Ovsyannikova[449], the abovementioned editor of Channel 1.

Actions such as this represent even more incentive for ordinary Russians, but also for proper media to adhere to self-censorship. After passing the law, 60 people were detained in the first three days, mainly journalists.[450] Also, the street protests continued – two days after signing the law, according to OVD-Info, police detained over 5 000 people across the country in a single day during

[444] "Госдума Приняла Закон Об Уголовной Ответственности За Фейки о Российской Армии," *BBC*, accessed August 10, 2022, https://www.bbc.com/russian/news-60615902.
[445] Evgeniya Stogova, "Закон Об Уголовном Наказании За Фейки. Как Он Изменил Работу Журналистов," *RBC*, accessed August 10, 2022, https://www.rbc.ru/technology_and_media/05/03/2022/6223325d9a7947835d28df5d.
[446] "Госдума Приняла Закон Об Уголовной Ответственности За Фейки о Российской Армии."
[447] "Discreditation of Russian Armed Forces May Be Penalized with up to 5 Years in Jail - Legislative Amendments," *Interfax*, 2022, https://interfax.com/newsroom/top-stories/75222/.
[448] Mike Eckel, "'Discrediting' The Armed Forces: The Russians Caught Up In A Draconian Law," *RFE/RL*, 2022, https://www.rferl.org/a/russia-ukraine-war-discrediting-armed-forces-law/31875273.html.
[449] Eckel.
[450] Soldatov and Borogan, "The New Iron Curtain Part 5: Russia's War Against Silicon Valley."

anti-war protests.[451] Facing this new legal reality, the outlets Novaya Gazeta and The Bell decided to stop covering the events in Ukraine in total.[452] Other international media such as CNN or CBS News stopped their activity in Russia, while Bloomberg or BBC provisionally suspended their journalists.[453] The same day the "Fake news law" was adopted, Roskomnadzor began to block foreign media outlets such as Deutsche Welle, Meduza, Voice of America, or Radio Free Europe/Radio Liberty because of the alleged spreading of fake information.[454] Importantly, the increased censorship also led to the closure of the Echo of Moscow - one of the most respected independent Russian media that had enjoyed respect since 1990.[455] Roskomnadzor complained, that the radio station is reporting falsely about the invasion of Ukraine and blocked its website and disconnected its radio station at the beginning of March. In response, its editorial board announced the end of the station and deleted all its social media accounts and shut down its website.[456] On the pretext of "encouraging towards extremist activity and providing knowingly false information" in connection with the invasion of Ukraine, both TV Rain and the Echo of Moscow were added on the list of "foreign agents" and blocked together.[457] Typically, the Kremlin also went after independent NGOs and blocked websites of Amnesty International, or the election watchdog Golos.[458] According to Moscow Times, since the start of the invasion on February 24th until the

[451] "Russia Arrests over 5,000 in Single Day for Protesting Ukraine War," *The Hindu*, 2022, https://www.thehindu.com/news/international/russia-arrests-over-5000-in-single-day-for-protesting-ukraine-war/article65201756.ece.
[452] Georgyi Tadtaev, "«Новая Газета» и The Bell Решили Прекратить Освещать События На Украине," *RBC*, accessed August 10, 2022, https://www.rbc.ru/politics/04/03/2022/622240959a79473a2ec999cd.
[453] James Ellingworth, "Russia Cracks down on Dissenting Media, Blocks Facebook," *AP*, 2022, https://apnews.com/article/russia-ukraine-vladimir-putin-business-europe-germany-d15ca4ed450d9ca67f43d3b1ac27294d.
[454] Maria Xynou and Arturo Filastò, "New Blocks Emerge in Russia amid War in Ukraine: An OONI Network Measurement Analysis" (OONI (Open Observatory of Network Interference), 2022), https://ooni.org/post/2022-russia-blocks-amid-ru-ua-conflict/#blocking-of-news-media-websites.
[455] "Russia's Top Radio Station Shut amid Crackdown on Dissent," *AP News*, 2022, https://apnews.com/article/russia-ukraine-business-europe-media-moscow-203dd09e6318603d09dc1be098021c8e.
[456] "«Эхо Москвы» Удалит Свои Аккаунты в Соцсетях и Отключит Сайт," *Ekho Kavkaza*, 2022, https://www.ekhokavkaza.com/a/eho-moskvy-udalit-svoi-akkaunty-v-sotssetyah-i-otklyuchit-sayt/31736236.html.
[457] "Венедиктов Сообщил, Что 'Эхо Москвы' Отключено От Эфира," *Interfax*, 2022, https://www.interfax.ru/russia/825574.
[458] "Russia: Authorities Block Amnesty International's Russian-Language Website," *Amnesty International*, 2022, https://www.amnesty.org/en/latest/news/2022/03/russia-authorities-block-amnesty-internationals-russian-language-website/.

beginning of June, Roskomnadzor has blocked more than 65 000 websites.[459] Accordingly, by the end of February, the most downloaded apps in Russia on both Google and Apple store were VPN services.[460]

Since the start of the invasion, the state-owned channels RT and Sputnik have been banned on Facebook across the EU countries.[461] In addition, Facebook have been fact-checking and labelling accounts of Russian official media channels such RIA Novosti or lenta.ru. In response, Roskomnadzor accused Facebook for "violating the rights and freedoms of Russian citizens" after the company refused to stop with the practice and subsequently decided to block Facebook[462] as well as Twitter.[463] According to Xynou and Filastò, however, we can observe an innovative censorship approach in the case of Twitter. Their data have shown that Twitter was throttled at first, while during the first week of March, it got blocked overall. Crucially though, "throttling of twitter.com seemed to stop across all ISPs in Russia at the same time" which may suggest that the Kremlin is able to execute this in a centralised way without waiting for the implementation of the ISPs.[464] According to Xue et al., this is related to the DPI technology that allows for more advanced censorship techniques than blocking.[465] This suggest, that even though analysts remain doubtful about the Kremlin's implementation of ambitions that were set in the 2019 'Sovereign Internet Law', it has certainly sophisticated its censorship capabilities at least to some extent and has advanced with the building of the infrastructure enabling more extensive surveillance.

A week after blocking Facebook, Roskomnadzor has also blocked Instagram after filing a complaint that the owner of Facebook and Instagram, Meta, has decided to allow certain posts of a violent character (e.g. "death to the Russian invaders") that would otherwise be violating its

[459] "Proton VPN Says 'Likely' Blocked in Russia," *The Moscow Times*, 2022, https://www.themoscowtimes.com/2022/06/02/russian-clinics-brace-for-botox-shortage-as-imports-drop-kommersant-a77870.
[460] "Самыми Скачиваемыми в России Приложениями Стали VPN-Сервисы," *Roskomsvoboda*, 2022, https://roskomsvoboda.org/post/vpn-servisy-stali-chashe-kachat/.
[461] Elizabeth Culliford, "Facebook Owner Meta Will Block Access to Russia's RT, Sputnik in EU," *Reuters*, accessed August 8, 2022, https://www.reuters.com/business/media-telecom/facebook-owner-meta-will-block-access-russias-rt-sputnik-eu-2022-02-28/.
[462] Jane Wakefield, "Ukraine Invasion: How the War Is Being Waged Online," *BBC*, accessed August 10, 2022, https://www.bbc.com/news/technology-60559011.
[463] Ellingworth, "Russia Cracks down on Dissenting Media, Blocks Facebook."
[464] Xynou and Filastò, "New Blocks Emerge in Russia amid War in Ukraine: An OONI Network Measurement Analysis."
[465] Diwen Xue et al., "Throttling Twitter: An Emerging Censorship Technique in Russia," *IMC' 21 Virtual Event*, 2021, https://censoredplanet.org/assets/throttling-imc-paper.pdf.

community standards.[466] However, Instagram was also a platform where influential people could voice their anti-war sentiment. This was done by an affluent banker Oleg Tinkov who said that the war is "unthinkable and unacceptable" and that governments should spend money for healing people rather than waging wars.[467] Similarly, after a popular comedian Ivan Urgant shared an anti-war post on his profile, his popular show on Channel 1 was replaced by a news broadcast "because of the current situation."[468] The rationale behind blocking both Facebook and Instagram was the already typical declaration that their parent company, Meta, is extremist.[469]

Another company that decided to pause its actions was TikTok as it was often used by anti-war protesters to stream their cause. Consequently, Russian users of TikTok were not able to post any new content and could consume content originating only from within Russian borders.[470] Most problematically, this decision effectively created a censored version of TikTok in which pro-Kremlin propaganda could thrive. According to Giulia Giorgi, "TikTok went from being considered a serious threat to Putin's national support for the war to becoming another possible conduit for state propaganda."[471] As such, after TikTok adhered to the blocking, "the number of videos protesting the invasion had dropped to zero from hundreds the day before."[472]

I have already spoken about the phenomenon of non-state actors that are supporting the Kremlin on various social media. This time, with TikTok, it was no different. A Vice News report has found out, that since late 2021, there had been a Telegram channel that was supporting the Kremlin's initiatives such as COVID-19 vaccination campaign. When the war broke out, it had begun to recruit TikTok influencers and pay them for posting in a pro-Kremlin way. After TikTok followed the fake news law and forbade Russian new uploads, the channel also provided its recruits

---

[466] Richard Lawler, "Russia Will Ban Instagram on March 14th," *The Verge*, accessed August 10, 2022, https://www.theverge.com/2022/3/11/22972869/instagram-ban-russia-ukraine-facebook-whatsapp-meta.
[467] James Vincent, "Russia Bans Instagram as Promised, Blocking Access for 80 Million Users," *The Verge*, accessed August 10, 2022, https://www.theverge.com/2022/3/14/22976603/russia-bans-instagram-facebook-meta-call-to-violence.
[468] Dasha Litvinova, "Protests in Russia Resume as Government Seeks to Quash Antiwar Voices," *Los Angeles Times*, 2022, https://www.latimes.com/world-nation/story/2022-02-25/protests-resume-as-russia-seeks-to-quash-invasion-critics.
[469] "The Return of Digital Authoritarianism: Internet Shutdowns in 2021.", p. 11
[470] Matt O'Brien, "Netflix, TikTok Block Services in Russia to Avoid Crackdown," *AP*, accessed August 10, 2022, https://apnews.com/article/russia-ukraine-vladimir-putin-technology-business-media-d4a41ac1088a4e14d5342729079bfb2d.
[471] Will Oremus, "TikTok Created an Alternate Universe Just for Russia," *The Washington Post*, accessed August 11, 2022, https://www.washingtonpost.com/technology/2022/04/13/tiktok-russia-censorship-propaganda-tracking-exposed/.
[472] Oremus.

with a step-by-step guide on how to bypass the block.[473] It is important to understand that this is a result of the fake news law, albeit indirectly. The case of TikTok nicely shows how this law affects not only media outlets, social media, and other big companies, but also individual users and their possibility to gather unbiased information. After Facebook, Twitter and Instagram were made unavailable to Russian users, TikTok has converted into an uncontested space where pro-war propaganda can thrive. This is important, especially considering the fact that, together with YouTube, it is the only global platform still accessible. Moreover, the still active League of the Safe Internet mentioned earlier helped the Kremlin patrol the critics of the invasion when they reported an anti-war post by journalist Yury Dud to the Ministry of Justice and asked to label him as a "foreign agent".[474]

Crucially, Russia has been aggressively expanding its Internet governance also to the occupied territories in Ukraine. It has been active in shutting down Internet access in order to limit access to information for the local population. Additionally, it then re-routed the connection to Russian networks, making the Ukrainian population subject to the SORM surveillance technology.[475] By doing so, it has been able to replicate its approach to Internet governance also inside of the occupied territories. As such, in July, Russian occupiers were able to block YouTube and Instagram in the Kherson region.[476] Furthermore, later in July, Google's search engine was blocked in Donetsk, Luhansk, and Kherson "under the pretext of 'openly propagating terrorism and violence against Russians.'"[477] Allegedly, Russian authorities have also claimed Facebook, Twitter, YouTube, and Instagram to be blocked in the occupied parts of Zaporizhzhia region.[478]

The Kremlin has also been sending some signals that imply the willingness for a more digitally independent Russia. In early March, Russian Ministry of Digital Development called on state-owned websites to adopt measures to increase their resilience in case of cyber-attack. However,

---

[473] David Gilbert, "Russian TikTok Influencers Are Being Paid to Spread Kremlin Propaganda," *Vice News*, accessed August 11, 2022, https://www.vice.com/en/article/epxken/russian-tiktok-influencers-paid-propaganda.
[474] Litvinova, "Protests in Russia Resume as Government Seeks to Quash Antiwar Voices."
[475] Ryan Gallagher, "Control of Ukrainian Internet Is New Focus in Russian Invasion," *Bloomberg*, accessed August 8, 2022, https://www.bloomberg.com/news/newsletters/2022-06-08/ukrainian-internet-is-focus-of-new-fight-after-russian-invasion.
[476] "YouTube Blocked in Ukraine's Russian-Occupied Kherson," *The Moscow Times*, 2022, https://www.themoscowtimes.com/2022/07/06/russian-police-chiefs-top-aide-arrested-on-corruption-charges-a78217.
[477] "Updates: Digital Rights in the Russia-Ukraine Conflict," *Access Now*, 2022, https://www.accessnow.org/digital-rights-ukraine-russia-conflict/.
[478] "Updates: Digital Rights in the Russia-Ukraine Conflict."

besides requiring to "remove any reliance on Western technology that could be removed without warning and bring down Russian government websites (…) it also directs websites to begin using Domain Name System (DNS) servers located in Russia."[479] This is potentially a two-dimensional step that could further contribute to the separation of Runet from the global internet. Since June, amid the continued blocking of Western companies, the Kremlin has been contacting regional governors with requests to start using Russian technology instead of services such as Google Docs, WhatsApp, Skype, Zoom etc. – it is planning to build a platform organised by VKontakte that would be used to connect all state officials for state communications by 2023.[480]

In terms of learning, compared to the previous periods under analysis, for the first time, it was Russia who initiated this event and seriously escalated the situation. Therefore, while the invasion of Ukraine represents a turning point because we can indeed observe yet another increase in Internet regulation in Russia, it follows a different logic than those that I have been presenting up until now. Theoretically, it could have given Russia an upper hand for its approach. Nevertheless, it turned out that it was acting reactively again. The scale of dissent in February and March 2022, both offline and online, clearly prompted the Kremlin to take additional steps to "protest-proof" its regime. Arguably, the notion promoted by Gainous et al. that authoritarian regime's stability often hinges "on the ability to control and manipulate information"[481] is even more pertinent at times of war when sustaining a favourable public opinion is of high importance and for that, information management and propaganda are crucial.

Essentially, Ukraine has been Russia's enemy since Euromaidan and both countries have been in war together since 2014. Therefore, there is no reason to expect some sort of change in the logic behind regulating the Internet and the narrative that I was presenting until now. However, due to the fact that conventional war is being waged, there is a reason to expect increased intensity in online censorship. With the escalation of the hostility between the West and Russia amid the invasion of Ukraine, Russia has been sending further signals that it did not abandon the ambition to insulate itself from the influences of the West – both in terms of information and technology.

[479] Gilbert, "Russia Is Preparing to Cut Itself Off From the Global Internet."
[480] Yuliya Tishina and Yurii Litvinenko, "Губернаторов Ведут На Контакт: Чиновников Пересаживают На Мессенджер От VK," *Kommersant*, 2022, https://www.kommersant.ru/doc/5381031.
[481] Gainous, Wagner, and Ziegler, "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections.", p. 209

Throughout this paper, I have demonstrated a few times already that Internet censorship and regulation has not been influencing Putin's approval rating significantly. On the contrary, the Kremlin's hostile narrative that had been intensified by Putin after Snowden's revelations and the annexation of Crimea contributed to the notion of "psychological firewall", implying that Russians were supportive of the Kremlin's regulatory actions because of the Internet's alleged extremist nature. This time, amid all these events, it is no different. According to Levada Center, Putin's approval ratings have been steadily increasing since February 2022 when the invasion has begun (71%) and reaching 83% in March (when the 'Fake News Law' was adopted) – it has stayed on this level until July 2022.[482] However, it should be noted that amid all these new regulations and introduction of criminal liability for discrediting the Russian army and spreading unreliable information, the results of this survey may not be reliable. Facing the possible strict penalisation, Russians may be reluctant to share what they really think. Nevertheless, a different Levada survey has found out that after the invasion of Ukraine, "trust in television has grown, while trust in Internet sources has sunk". While 32% of Russian do support blocking of Facebook and Instagram and 46% do not, the overall majority of respondents (57%) believed that censorship of the Internet is necessary because of the existence of "malicious websites".[483]

[482] "Одобрение Институтов, Рейтинги Партий и Политиков," *Levada Centre*, 2022, https://www.levada.ru/2022/03/30/odobrenie-institutov-rejtingi-partij-i-politikov/.
[483] "Internet, Social Networks and Blocking," *Levada Centre*, 2022, https://www.levada.ru/en/2022/05/27/internet-social-networks-and-blocking/.

Conclusion

This thesis provided a longitudinal analysis of how Internet governance and cyberspace controls has been approached by Putin's Russia. His rise to power gradually resurrected the Soviet tradition of controlling information and tying actors involved in facilitating of information exchange with the state. As such, it was in this period when the Kremlin showed interest in the ISP market for the first time, being aware of their influential role in this process. Importantly, the infrastructural foundation for Internet development were laid still during the 1990s with the help of Western companies. The Soviet tradition of intercepting phone calls was revived with the requirement for ISPs to install SORM technology on their networks. In 1998, when SORM-2 was adopted to encompass the Internet and linked the devices with the security services, it was Putin who was the head of FSB.

Upon taking office, Putin had taken a decisive action against independent media. Their owners were pressured to sell their shares for their freedom and pro-Kremlin figures such as Gleb Pavlovski were also creating the first pro-Kremlin websites. When the Kursk submarine sank and Putin's approach was widely criticized across the independent media, the Kremlin soon after took control of influential channels such as NTV and ORT (Channel 1). After this experience, the first Information Security doctrine was adopted which framed information along the lines of national security. This refers to the trend that the increased centralisation propagated by Putin also involved the management of information. On the international level and in the context of international security, Russia proposed to create a specialised group in the UN (UNGGE) to discuss norms as to how should states behave in cyberspace.

Arguably, at that time, we should not be talking about some comprehensive approach towards Internet governance as it still represented a rather new phenomenon. While the foundations of Russia's digital authoritarianism were laid already in this period by employing the SORM technology, it had taken many more years until the Kremlin sophisticated its online censorship capabilities. The most relevant developments that occurred in this period was the Kremlin's appropriation of traditional media and setting up the tradition of ISP cooptation.

The colour revolutions, particularly in Georgia and Ukraine, seriously alerted the Kremlin. In response, drawing a lesson from the way these revolutions played out, Putin started to tie civil society organisation with the state in ambition to insulate Russia from regime change. This period started the tradition of broadly formulated laws related to extremism and other illicit activities to

encompass all kinds of behaviour, including oppositional activity. This first involved foreign funded NGOs that started to be seen as threatening to Putin's regime. Accordingly, the regime supported the development of pro-regime organisation such as Nashi that were called upon in times of crisis and which soon after began to be active also in the online environment. Together with other pro-regime bloggers, these actors were active in online discussions trying to sway online content's character in regime's favour, for example by influencing Yandex's top-five blog post list.

After the 2007/8 election cycle, the scope of surveillance expanded. When Medvedev became president, the so-called "Center E" was created under the Ministry of Interior in order to report online extremist activity and the scope surveillance under SORM had doubled under his presidency. Overall, the Internet started to be increasingly perceived as an extension of media and therefore prone to governmental interference.

Importantly, in light of these events, this period revived a state-led narrative of sovereign democracy. After the Kremlin started to believe that the West is interested in undermining Russia's position in its near abroad by facilitating regime change, it has started a tradition that arguably lasts until now. On the international level, Russia started to cooperate with China at the level of Shanghai Cooperation Organisation to formulate international norms against regime change and arguing for an unconditional adherence to national sovereignty.

Since the Arab Spring was characterised as a series of revolutions facilitated by Western social networks such as Twitter and Facebook, the Kremlin's fears of regime change facilitated by Western technology were further validated. Indeed, the number of social media users was rising in Russia. Soon, after the 2011 Duma elections, Russia experienced the biggest mass protests since the soviet times. Bloggers like Navalny started to be active on social media (including Facebook and Twitter) because their platform of choice until then, Livejournal, was struggling with DDOS attacks. Importantly, the main demonstration at Bolotnaya Square was propagated on Facebook.

Until the 2011 mass protests in Moscow, apart from some oppositional bloggers, the Kremlin did not experience any significant disturbances threatening its regime stability that would stem from the online environment. Therefore, it was after these protests when the infamous blacklist curated mainly by Roskomnadzor was created. In addition, the scope of SORM was upgraded to include social media as well. Since 2012, politically oriented NGOs were required to officially register as "foreign agents" and label their publication accordingly.

The mass protests also prompted Russia to intensify its international regulatory initiatives. In 2011, the Kremlin started to propagate global Internet governance on the level of ITU. The same year, at the UN, together with SCO member, Russia argued for sovereignty over states' policies regarding the Internet and asked for global cooperation in limiting information undermining countries' political stability (among others). In 2012, SCO members also started to cooperate in countering online opposition.

Snowden's revelations finally provided the Kremlin with an argument to strike against companies such as Facebook, Twitter, or Google because data of Russian users were allegedly in danger on American soil. As such, the notion of digital sovereignty started to emerge that was followed by pressuring these companies to relocate servers and store data of Russians in Russia. A few have complied which led to different responses to different companies. While LinkedIn got banned in 2016 after refusing to relocate servers, Twitter and Facebook were fined financially multiple times but continued their operation.

Even though the annexation of Crimea boosted Putin's popularity, he still needed Russians to share the Kremlin's perception of what is happening in Ukraine and why Russia is supporting the separatist war in Donbass. In other words, the more aggressive foreign policy required a more aggressive approach towards Internet governance in order for the propaganda to work. For these ends, allies of the Kremlin infiltrated ownerships structures of influential domestic companies VKontakte and Yandex and brought them under increased governmental scrutiny. Yandex also started to be legally liable for search results providing links to media that were not registered with Roskomnadzor which effectively eliminated alternative news from its results. Number of websites critical of Russia's actions in Ukraine got blacklisted, including Navalny's blog on Livejournal. More regime-friendly organisations such as League of the Safe Internet got invited to identify online extremism and to patrol the Internet together with Roskomnadzor.

In 2016, the set of Yarovaya laws significantly increased user surveillance in Russia because of the time periods for which data was legally required to be stored, as well as the obligation for the companies to hand in encryption keys to the FSB. With the increased online surveillance, the authorities also increasingly started to prosecute users for their online behaviour, often selectively and unsystematically. All these facts created an atmosphere of randomness and uncertainty among the Internet users which, together with the propagated extremist nature of the Internet, contributed to the so-called psychological firewall and self-censorship.

Then, with 2019 Sovereign Internet law, the Kremlin strived for a more centralised character of Internet governance, without the necessity to rely on ISPs to implement Roskomandzor's blocking. Compared to previous periods, when ISPs often had to bear the cost of newly required technology, this time, the authorities provided the DPI technology. Nevertheless, the fact that it was bought from abroad, including the US, undermines the Kremlin's long-term aim for digital sovereignty and rather hints towards the willingness to further upgrade Russia's surveillance capabilities. The law's ambition to build a national DNS represented a years-long effort to come up with an alternative to ICANN which the Kremlin perceived to be serving American interests. In 2021, the DPI technology was tested when the method of throttling (the case of Twitter) was introduced for the first time and the Kremlin also continued with …..

Amid the street protests after the 2022 invasion of Ukraine, the Kremlin further intensified Internet censorship in Russia. Again, the reason for this is, that it needed the propaganda to work during crucial times. Arguably, when a conventional war is being waged and Russians are being sent to war on a considerable scale, this necessity is even higher. Facing both offline and online opposition, often from influential popular figures, the Kremlin decided to introduce criminal liability for spreading information that would go against the state interpretation of the invasion. This so-called fake news law resulted in departure of popular media companies, both domestic (TV Dozhd or Echo Moskvy) and international (CNN, CBS News). Other media such as for example Deutsche Welle, Meduza or Voice of America were blocked by Roskomnadzor.

Responding to Meta's decision to continue with labeling of Russia's state media accounts on Facebook, Roskomnadzor has blocked Facebook and subsequently also Instagram. This played into Kremlin's hands because it was Instagram, where Russian popular figures often posted anti-war content. Likewise, Twitter got throttled at first and then blocked entirely. Crucially, the installed authorities were replicating these actions also in the occupied territories in Ukraine.

I now turn into answering my research questions. It is important to clarify that the emergence of digital authoritarianism in Russia was a gradual process. Even though Putin showed authoritarian tendencies since the very beginning of his rule (typically by influencing independent media channels), it took a significant amount of time until the stability of his regime began to rely on digital technologies and the control of digital space.

All the events that I have analysed contributed to increased intensity of Russia's approach towards cyberspace regulation. Not all of them contributed equally though – some of them represented a serious red flag for the Kremlin that a change of approach is necessary in order to sustain the regime, whereas some of them represented rather a rhetorical justification for such a change. As such, all of the events represented a source of learning that allowed the Kremlin to observe and evaluate the experience either of similar countries in terms of the style of governance, or its own domestic experience with the Internet. Thus, indeed, a learning process can be identified behind the development of Russia's approach towards regulating the Internet.

The colour revolutions alerted the Kremlin and pointed its attention to the fact that regime change can be influenced by foreign countries and facilitated by foreign funded domestic actors. This was the only time when complex learning can be identified because the colour revolutions ignited a value conflict which resulted in foreign policy alteration and the subsequent adoption of the inward-looking ideology of sovereign democracy. This state-led narrative started to propagate the idea that Russia has external enemies that are trying to undermine its position in the international arena and that those inside of Russia who are cooperating with these external enemies should be approached with suspicion.

While it is true that every state regulates its online environment to some extent, mostly to fight with extremist content, states such as Russia deliberately widen the horizon of what kind of information is considered extremist in order to encompass all kinds of illicit and potentially dangerous information including libel or for example propagation of unsanctioned events. This tradition started after the colour revolutions when the Kremlin started to develop legislature to limit actions of foreign funded NGOs and forbade the registration of those which threatened Russia's "national interests". This further expanded under Medvedev with the creation of the anti-extremism "Center-E" that patrolled the Internet – since then Russian were criminally liable for expressing extremism online which, among other things, included for example criticism of the police.

It was during and after 2011, when the Kremlin understood that the Internet could be detrimental to regime stability, mainly by instigating public unrest and spreading information that could undermine its position. The then-contemporary discourse about Arab Spring being facilitated by Western social media further increased these fears. When Facebook and Twitter helped to facilitate regime change during the Arab Spring uprising, this argument was strengthened

further as the Arab authoritarian leaders did not have any control over these Western networks. When the same networks helped to facilitate the biggest mass protest since the Soviet times during and after the 2011 Duma elections, the argument about hostile Western technology spreading chaos inside Russia's political system resurfaced. Additionally, Snowden's revelations allowed the Kremlin to argue that data of Russian users are not safe on these networks and that they need to be regulated.

As such, the hypothesis that cyberspace regulation in Russia represent a continuation of Russia's repressive policies against the "foreign elements" inside of Russia's political discourse and/or civil society such as NGOs who receive foreign funding proved to be correct. Indeed, after Snowden's revelations and after his international experience with international bodies who were often reluctant to consider Russia's argument Putin concluded that the Internet is a CIA project.

Therefore, in 2011, the Kremlin was alerted by Internet on both international and domestic level and embarked on a path of a stricter Internet governance. Arguably, the domestic experience of 2011 Duma election represented the most threatening event to the Kremlin's stability and thus it can be perceived as the most significant source of learning that intensified the pace of cyberspace regulation in Russia.

Indeed, Roskomnadzor's blacklist started to be used after these events. Henry and Howells have found in 2021, that 81% of contributions to Roskomnadzor's blacklist were added during or after 2011. Out of those, "at least 64% were digital (websites, digital articles, social media videos, audio clips, posts, and comments) (…) and 54% of digital materials were found on social media sites, most (84%) of which are Russia-based platforms, such as VKontakte and Odnoklassniki."[484] Similarly, a BBC analysis uncovered that between 2011 and 2020, the Kremlin has filed 123 606 request to delete content from Google and YouTube – the second country with the highest amount of request was Turkey, however, the number was drastically lower (14 231).[485] While the blacklisting mechanism is often inconsistent and often led to overblocking and "collateral censorship", it is considered effective in terms of accessibility to the respective content – "approximately 90% of Runet users" cannot access it.[486]

[484] Henry and Howells, "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet Governance.", p. 13
[485] Zakharov and Churmanova, "How Russia Tries to Censor Western Social Media."
[486] Henry and Howells, "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet Governance.", p. 10

Following Bunce and Koesel,[487] I hypothesized that sophistication of Russian cyberspace regulation is related to "protest-proofing" in order to increase regime stability. Indeed, the analysis and the abovementioned data have shown that the Internet censorship intensified after the 2011 protests which suggests that Internet regulation is a form of crisis management, often on ad hoc basis, rather than pre-emptive. Tiberiu and Lupu argued that with the help of digital technology, digital authoritarianism can adhere to preventive repression and "reduce the risk that opposition groups threaten government's power, including opposition effort to mobilise and organise public dissent."[488] While until around 2014, the Kremlin's approach can be characterised as reactive, when Russia annexed Crimea in 2014 and started to support the separatist in Donbass, the incentive for preventive actions increased because the military presence needed to be justified by a functional propaganda.

The preventive trajectory continued in 2016 when the new Information Security doctrine highlighted the need to control the Internet and support the development of domestic information technology. Since then, arguably, the authorities have been first drafting laws that set the direction in which cyberspace regulation should go, sometimes without considering the actual technological or infrastructural capabilities of the time (e.g. there was not enough data storage capabilities to store all the required data as set by the Yarovaya laws), and only then building the capabilities set by the legislation.

Since digital surveillance represents the core element of digital authoritarianism, it would be a mistake to characterise Russia's system as digital authoritarianism until about 2016. While Russia has been leaning towards this direction since the employment of SORM technology, it was not until 2016 when the set of Yarovaya laws was adopted which unprecedently increased the scope of such surveillance. Even though the overall character of Putin's governance is rather centralised, for a long time, the character of Internet governance was decentralised (typically by relying on ISPs to implement Roskomnadzor's blocking). Since 2017, however, with the developing of a control center in Moscow, it has been moving towards more centralised approach. This continued with the ambitious 2019 sovereign Internet law which set the goal of creating a national DNS and wide implementation of DPI technology across all Russia that enabled more intrusive surveillance.

[487] Koesel and Bunce, "Diffusion-Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations against Authoritarian Rulers.", p. 755
[488] Dragu and Lupu, "Digital Authoritarianism and the Future of Human Rights.", p. 993

According to Xynou and Filastò, due to the decentralised nature of Internet governance, "different internet users in Russia may experience different blocks, depending on which network they're connected to".[489] However, the style in which Twitter got throttled amid the current invasion of Ukraine was more of centralised nature which, according to Xynou and Filastò, "raises alarms about Russia potentially having centralized censorship capabilities, which would make censorship more effective and harder to circumvent."[490] Therefore, the trend in Russia's digital authoritarianism is arguably moving from a decentralised direction towards a centralised direction. Importantly, by 2020, all the Kremlin's regulative actions taken since 2011 have effectively transformed the oppositional character of online public sphere that was predominant until the 2011 mass protests.

It should be noted that the scope of offline-online nexus attribute of Russia's digital authoritarianism has proved to be much more extensive than initially expected. As demonstrated, to regulate the online sphere, the regime can physically intimidate not only journalists, activists or bloggers, but also high-ranking employees of international technological companies who hold physical offices in the given country, or providers of VPN technologies – this was demonstrated on the physical intimidation of Google's CEO and the raiding of offices of the Private Internet Access company. The new legal obligation for foreign Internet companies with more than 500 000 daily Russian users to open physical offices in Russia can create even bigger leverage for the authorities in this direction.

Internationally, Russia has been engaging with the international forums to push forward policies that reflect its perception of information security as in its national laws.[491] Interestingly, in September 2022, the dominant vision of how the global Internet governance should look will be tested again as the new secretary-general of the ITU is due to be elected. The two scheduled candidates are Doreen Bogdan-Martin from the US and Rashid Ismailov from Russia. Again, the expected battle between multistakeholder model based on a bottom-up approach and the multilateral model based more on governmental decisions is expected to clash.[492] However, considering the way Putin's Russia has been approaching Internet regulation at home, and the now

[489] Xynou and Filastò, "New Blocks Emerge in Russia amid War in Ukraine: An OONI Network Measurement Analysis."
[490] Xynou and Filastò.
[491] Deibert and Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls.", p. 346
[492] Harding Margaret McGill, "U.S. vs Russia for the Future of the Internet," *Axios*, accessed August 10, 2022, https://www.axios.com/2022/03/03/us-russia-internet-international-telecommunication-union.

full-scale online censorship developed after the invasion of Ukraine, it is hardly imaginable for the Russian candidate to gather support.

Bibliography

Akbari, Azadeh, and Rashid Gabdulhakov. "Platform Surveillance and Resistance in Iran and Russia: The Case of Telegram." *Surveillance & Society* 17, no. 1/2 (2019): 223–31.

Alexander, Marcus. "The Internet and Democratization: The Development of Russian Internet Policy." *Demokratizatsiya The Journal of Post-Soviet Democratization* 12, no. 4 (2004): 607–27.

OVD-Info. "Almost 2,000 Russians Arrested on the First Day of Anti-War Protests," 2022. https://ovdinfo.org/articles/2022/02/27/almost-2000-russians-arrested-first-day-anti-war-protests.

Ambrosio, Thomas. *Authoritarian Backlash: Russian Resistance to Democratization in the Former Soviet Union*. 1st ed. Routledge, 2009.

Amrosio, Thomas. "Constructing a Framework of Authoritarian Diffusion: Concepts, Dynamics, and Future Research." *International Studies Perspective* 11 (2010): 375–92.

Deutsche Welle. "Are Russia's Anti-Terror Laws Designed to Fight Democracy?," 2016. https://www.dw.com/en/about-dw/s-30688.

Bank, André, and Mirjam Edel. "Authoritarian Regime Learning: Comparative Insights from the Arab Uprisings." Working Paper. Legitimacy and Efficiency of Political Systems. German Institute for Global and Area Studies (GIGA), 2015.

Bateman, Tom. "How Russia Could Cut Itself off from the Global Internet, and Why It Probably Won't." *Euro News*, 2022. https://www.euronews.com/next/2022/03/14/how-russia-could-cut-itself-off-from-the-global-internet-and-why-it-probably-won-t.

Burnell, Peter, and Oliver Schlumberger. "Promoting Democracy - Promoting Autocracy? International Politics and National Political Regimes." *Contemporary Politics* 16, no. 1 (2010): 1–15.

Carothers, Thomas. *Aiding Democracy Abroad : The Learning Curve*. Washington DC.: Carnegie Endowment for International Peace, 1999.

Crotty, Jo, Sarah Marie Hall, and Sergej Ljubownikow. "Post-Soviet Civil Society Development in the Russian Federation: The Impact of the NGO Law." *Europe-Asia Studies* 66, no. 8 (2014): 1253–69.

Culliford, Elizabeth. “Facebook Owner Meta Will Block Access to Russia’s RT, Sputnik in EU.” *Reuters*. Accessed August 8, 2022. https://www.reuters.com/business/media-telecom/facebook-owner-meta-will-block-access-russias-rt-sputnik-eu-2022-02-28/.

Deibert, Ronald J. “Authoritarianism Goes Global: Cyberspace Under Siege.” *Journal of Democracy* 26, no. 3 (2015): 64–78.

Deibert, Ronald J., and Masashi Crete-Nishihata. “Global Governance and the Spread of Cyberspace Controls.” *Global Governance* 18 (2012): 339–61.

Deibert, Ronald J., John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. London: The MIT Press, 2010.

Deibert, Ronald J., and Rafal Rohozinski. “Control and Subversion in Russian Cyberspace.” In *Access Controlled: The Shaping of Power, RIghts, and Rule in Cyberspace*, 15–33. London: The MIT Press, 2010.

Diamond, Larry. Authoritarian Learning: Lessons from the Coloured Revolutions. Interview by Kenta Tsuda and Barron YoungSmith. Brown Journal of World Affairs, 2006.

Interfax. “Discreditation of Russian Armed Forces May Be Penalized with up to 5 Years in Jail - Legislative Amendments,” 2022. https://interfax.com/newsroom/top-stories/75222/.

Dragu, Tiberiu, and Yonatan Lupu. “Digital Authoritarianism and the Future of Human Rights.” *International Organization* 75 (2021): 991–1017.

Ebert, Hannes, and Tim Maurer. “Contested Cyberspace and Rising Powers.” *Third World Quarterly* 34, no. 6 (2013): 1054–74.

Eckel, Mike. “‘Discrediting’ The Armed Forces: The Russians Caught Up In A Draconian Law.” *RFE/RL*, 2022. https://www.rferl.org/a/russia-ukraine-war-discrediting-armed-forces-law/31875273.html.

Ellingworth, James. “Russia Cracks down on Dissenting Media, Blocks Facebook.” *AP*, 2022. https://apnews.com/article/russia-ukraine-vladimir-putin-business-europe-germany-d15ca4ed450d9ca67f43d3b1ac27294d.

Epifanova, Alena. “Deciphering Russia’s ‘Sovereign Internet Law’: Tightening and Accelerating the Splinternet.” The German Council on Foreign Relations (DGAP), 2020.

Fedor, Julie, and Rolf Fredheim. “‘We Need More Clips about Putin, and Lots of Them:’ Russia’s State-Commissioned Online Visual Culture.” *Nationalities Papers* 45, no. 2 (2017): 161–81.

Finkel, Evgeny, and Yitzhak M. Brudny, eds. *Coloured Revolutions and Authoritarian Reactions*. 1st ed. Routledge, 2015.

Flonk, Daniëlle, Markus Jachtenfuchs, and Anke S. Obendiek. "Authority Conlifcts in Internet Governance: Liberals vs. Sovereignists?" *Global Constitutionalism* 9, no. 2 (2020): 364–86.

Francis, Gregory. "Plutocrats and the Internet." CircleID, October 4, 2010. https://circleid.com/posts/20101004_plutocrats_and_the_internet.

"Freedom on the Net 2011: A Global Assessment of Internet and Digital Media." Freedom House, 2011.

"Freedom on the Net: A Global Assesment of Internet and Digital Media." Freedom House, 2009.

Gainous, Jason, Kevin M. Wagner, and Charles E. Ziegler. "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections." *Democratization* 25, no. 2 (2018): 209–26.

Gallagher, Ryan. "Control of Ukrainian Internet Is New Focus in Russian Invasion." *Bloomberg*. Accessed August 8, 2022. https://www.bloomberg.com/news/newsletters/2022-06-08/ukrainian-internet-is-focus-of-new-fight-after-russian-invasion.

Gaufman, Elizaveta. "Cybercrime and Punishment: Security, Information War, and the Future of Runet." In *The Palgrave Handbook of Digital Russia Studies*, edited by Daria Gritsenko, Mariëlle Wijermars, and Mikhail Kopotev, 115–35. Cham: Palgrave Macmillan, 2021.

Gilbert, David. "Russia Is Building Its Own Version of China's Great Firewall." *Vice News*, 2019. https://www.vice.com/en/article/gyakjx/russia-is-building-its-own-version-of-chinas-great-firewall.

"Russia Is Preparing to Cut Itself Off From the Global Internet." *Vice*. Accessed August 11, 2022. https://www.vice.com/en/article/88gevb/russia-is-preparing-to-cut-itself-off-from-the-global-internet.

"Russian TikTok Influencers Are Being Paid to Spread Kremlin Propaganda." *Vice News*. Accessed August 11, 2022. https://www.vice.com/en/article/epxken/russian-tiktok-influencers-paid-propaganda.

Giles, Keir. *Handbook of Russian Information Warfare: Fellowship Monograph*. NATO Defense College, 2016.

Glen, Carol M. "Internet Governance: Territorializing Cyberspace?" *Politics & Policy* 42, no. 5 (2014): 635–57.

Gunitsky, Seva. “Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability.” *Perspectives on Politics* 13, no. 1 (2015): 42–54.

Harding, Luke. “Putin Considers Plan to Unplug Russia from the Internet ‘in an Emergency.’” *The Guardian*. Accessed August 11, 2022. https://www.theguardian.com/world/2014/sep/19/vladimir-putin-plan-unplug-russia-internet-emergency-kremlin-moscow.

Henry, Laura A., and Laura Howells. “Varieties of Digital Authoritarianism: Analyzing Russia’s Approach to Internet Governance.” *Communist and Post-Communist Studies* 54, no. 4 (2021): 1–27.

Heydemann, Steven, and Reinoud Leenders. “Authoritarian Learning and Authoritarian Resilience: Regime Responses to the ‘Arab Awakening.’” *Globalizations* 8, no. 5 (2011): 647–53.

Horvath, Robert. *Putin’s Preventive Counter-Revolution: Post-Soviet Authoritarianism and the Spectre of Velvet Revolution*. 1. New York: Routledge, 2013.

Howard, Philip N., Sheetal D. Agarwal, and Muzammil M. Hussain. “The Dictator’s Digital Dilemma: When Do States Disconnect Their Digital Networks?” *Issues in Technology Innovation* 13 (2011): 1–11.

Howells, Laura H.C. *Digital Authoritarianism in China and Russia: A Comparative Study*. Vol. 166. Honors Project, 2020.

Levada Centre. “Internet, Social Networks and Blocking,” 2022. https://www.levada.ru/en/2022/05/27/internet-social-networks-and-blocking/.

Kelly, Sanja, Madeline Earp, Laura Reed, Adrian Shahbaz, and Mai Truong. “Freedom on the Net: Privatizing Censorship, Eroding Privacy.” Freedom House, 2015.

Kelly, Sanja, Mai Truong, Adrian Shahbaz, and Madeline Earp. “Silencing the Messenger: Communication Apps Under Pressure.” Freedom on the Net. Freedom House, 2016.

Kelly, Sanja, Mai Truong, Adrian Shahbaz, Madeline Earp, and Jessica White. “Manipulating Social Media to Undermine Democracy.” Freedom on the Net. Freedom House, 2017.

Kerttunen, Mika, and Eneken Tikk. “The Politics of Stability: Cement and Change in Cyber Affairs.” In *Routledge Handbook of International Cybersecurity*, edited by Mika Kerttunen and Eneken Tikk, 52–64. New York: Routledge, 2020.

Khalip, Andrei. “Police Detain More than 900 People at Anti-War Protests across Russia - Monitoring Group.” *Reuters*, 2022. https://web.archive.org/web/20220227160345/https://www.reuters.com/world/europe/police-detain-more-than-900-people-anti-war-protests-across-russia-monitoring-2022-02-27/.

Kiriya, Ilya. “From ‘Troll Factories’ to ‘Literring the Information Space’: Control Strategies Over the Russian Internet.” *Media and Communication* 9, no. 4 (2021): 16–26.

Koesel, Karrie J., and Valerie J. Bunce. “Diffusion-Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations against Authoritarian Rulers.” *Perspectives on Politics* 11, no. 3 (2013): 753–68.

Kovaleva, Natalya. “Russina Information Space, Russian Scholarship, and Kremlin Controls.” *Defense Strategic Communications* 4 (2018): 133–71.

Kravets, Daria, and Florian Toepfl. “Gauging Reference and Source Bias over Time: How Russia’s Partially State-Controlled Search Engine Yandex Mediated an Anti-Regime Protest Event.” *Information, Communication & Society*, 2021, 1–17.

Krutskikh, Andrei V., and Anatoli A. Streltsvo. “International Information Security - Problems and Ways of Solving Them.” In *Routledge Handbook of International Cybersecurity*, edited by Eneken Tikk and Mika Kerttunen, 260–68. New York: Routledge, 2020.

Lan, Tang. “International Governance of/in Cyberspace.” In *Routledge Handbook of International Cybersecurity*, edited by Eneken Tikk and Mika Kerttunen, 79–93. New York: Routledge, 2020.

Lawler, Richard. “Russia Will Ban Instagram on March 14th.” *The Verge*. Accessed August 10, 2022. https://www.theverge.com/2022/3/11/22972869/instagram-ban-russia-ukraine-facebook-whatsapp-meta.

Lehtisaari, Katja. “Formation of Media Policy in Russia: The Case of the Iarovaia Law.” In *Freedom of Expression in Russia’s New Mediasphere*, edited by Katja Lehtisaari and Mariëlle Wijermars, 57–75. London: Routledge, 2020.

Levy, Jack S. “Learnig and Foreign Policy: Sweeping a Conceptual Minefield.” *International Organization* 48, no. 2 (1994): 279–312.

Lewis, James A. “Sovereignty and the Role of Government in Cyberspace.” *The Brown Journal of World Affairs* 16, no. 2 (2010): 55–65.

Litvinenko, Anna, and Florian Toepfl. “The ‘Gardening’ of an Authoritarian Public at Large: How Russia’s Ruling Elite Transformed the Country’s Media Landscape After the 2011/12 Protests ‘For Fair Elections.’” *Publizistik* 64 (2019): 225–40.

Litvinova, Dasha. “Protests in Russia Resume as Government Seeks to Quash Antiwar Voices.” *Los Angeles Times*, 2022. https://www.latimes.com/world-nation/story/2022-02-25/protests-resume-as-russia-seeks-to-quash-invasion-critics.

Lonkila, Markku, Larisa Shpakovskaya, and Philip Torchinsky. “The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet.” In *Freedom of Expression in Russia’s New Mediasphere*, edited by Mariëlle Wijermars and Katja Lehtisaari, 17–39. London: Routledge, 2020.

Luhn, Alec. *Twitter* (blog), February 24, 2022. https://web.archive.org/web/20220226130731/https://twitter.com/asluhn/status/1496869020372398080?s=21.

Luxmoore, Matthew. “The Kursk Catastrophe, A Lesson For Putin, Is Fading From Russia’s Attention 20 Years Later.” *RFE/RL*, 2020. https://www.rferl.org/a/the-kursk-catastrophe-a-lesson-for-putin-is-fading-from-russian-attention-20-years-later/30778500.html.

MacLellan, Lila. “A Popular Russian Rapper Canceled Shows and Called for an Antiwar Movement.” *Quartz*. Accessed August 19, 2022. https://qz.com/2133401/a-major-russian-rapper-canceled-shows-and-called-for-war-protests/.

McGill, Harding Margaret. “U.S. vs Russia for the Future of the Internet.” *Axios*. Accessed August 10, 2022. https://www.axios.com/2022/03/03/us-russia-internet-international-telecommunication-union.

McIntosh Sundstorm, Lisa. *Funding Civil Society: Foreign Assistance and NGO Development in Russia*. 1st ed. Standford University Press, 2006.

Meyer, David. “Russia’s Denying That It’s about to Cut Itself off from the Global Internet, but It’s Acting a Lot like It.” *Fortune*, 2022. https://fortune.com/2022/03/07/russia-runet-disconnect-ukraine-dns-chernenko-letter/.

Morgus, Robert. “The Spread of Russia’s Digital Authoritarianism.” Artificial Intelligence, China, Russia, and the Global Order. Air University Press, 2019.

Moyson, Stéphanie, and Peter Scholten. “Theories on Policy Learning: Existing Approaches and Future Challenges.” In *Knowledge, Policymaking and Learning for European Cities and Regions. From Research to Practice*, edited by N. F. Dotti. Cheltenham (UK): Edward Elgar Publishing, n.d.

Nieva, Richard, and Sarah Emerson. “Facebook And Twitter Have Been Blocked In Russia.” *BuzzFeed News*. Accessed August 8, 2022. https://www.buzzfeednews.com/article/sarahemerson/russia-blocks-facebook-twitter.

Nisbet, Erik C., Olga Kamenchuk, and Aysenur Dal. “A Psychological Firewall? Rick Perceptions and Public Support for Online Censorship in Russia.” *Social Science Quarterly* 98, no. 3 (2017): 954–75.

O’Brien, Matt. “Netflix, TikTok Block Services in Russia to Avoid Crackdown.” *AP*. Accessed August 10, 2022. https://apnews.com/article/russia-ukraine-vladimir-putin-technology-business-media-d4a41ac1088a4e14d5342729079bfb2d.

Oremus, Will. “TikTok Created an Alternate Universe Just for Russia.” *The Washington Post*. Accessed August 11, 2022. https://www.washingtonpost.com/technology/2022/04/13/tiktok-russia-censorship-propaganda-tracking-exposed/.

Pallin, Carolina Vendill. “Internet Control through Ownership: The Case of Russia.” *Post-Soviet Affairs* 33, no. 1 (2017): 16–33.

Polyakova, Alina, and Chris Meserole. “Exporting Digital Authoritarianism: The Russian and Chinese Models.” Policy Brief. Democracy & Disorder. The Brookings Institution, 2019.

The Moscow Times. “Proton VPN Says ‘Likely’ Blocked in Russia,” 2022. https://www.themoscowtimes.com/2022/06/02/russian-clinics-brace-for-botox-shortage-as-imports-drop-kommersant-a77870.

Rakhmetov, Baurzhan. “The Putin Regime Will Never Tire of Imposing Internet Control: Developments in Digital Legislation in Russia.” *Council On Foreign Relations*, 2021. https://www.cfr.org/blog/putin-regime-will-never-tire-imposing-internet-control-developments-digital-legislation-russia.

Richards, Xander. “Nicola Sturgeon Praises Russians’ Courage as Anti-War Protests Erupt in Moscow.” *The National*, 2022. https://www.thenational.scot/news/19950978.nicola-sturgeon-praises-russians-courage-anti-war-protests-erupt-moscow/.

Roache, Madeline. “How Russia Is Stepping Up Its Campaign to Control the Internet.” *Time*, 2021. https://time.com/5951834/russia-control-internet/.

Rose, Richard. “What Is Lesson-Drawing?” *Journal of Public Policy* 11, no. 1 (1991): 3–30.

The Hindu. “Russia Arrests over 5,000 in Single Day for Protesting Ukraine War,” 2022. https://www.thehindu.com/news/international/russia-arrests-over-5000-in-single-day-for-protesting-ukraine-war/article65201756.ece.

Amnesty International. “Russia: Authorities Block Amnesty International’s Russian-Language Website,” 2022. https://www.amnesty.org/en/latest/news/2022/03/russia-authorities-block-amnesty-internationals-russian-language-website/.

Human Rights Watch. “Russia: ‘Big Brother’ Law Harms Security, Rights - Repeal Rushed Counterterrorism Legislation,” 2016. https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights.

Human Rights Watch. “Russia: Growing Internet Isolation, Control, Censorship - Authorities Regulate Infrastructure, Block Content,” 2020. https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship#_ftn2.

Human Rights Watch. “Russia: Police Detain Thousands in Pro-Navalny Protests - Mass Arbitrary Detentions, Police Brutality, Criminal Prosecutions,” 2021. https://www.hrw.org/news/2021/01/25/russia-police-detain-thousands-pro-navalny-protests.

The Moscow Times. “Russia Says Won’t Block Twitter, Will Keep Throttling Speeds,” 2021. https://www.themoscowtimes.com/2021/05/17/twitter-a73926.

AP News. “Russia’s Top Radio Station Shut amid Crackdown on Dissent,” 2022. https://apnews.com/article/russia-ukraine-business-europe-media-moscow-203dd09e6318603d09dc1be098021c8e.

Sauer, Pjotr. “‘They’Re Lying to You’: Russian TV Employee Interrupts News Broadcast,” 2022. https://www.theguardian.com/world/2022/mar/14/russian-tv-employee-interrupts-news-broadcast-marina-ovsyannikova.

Sauer, Pjotr, and Andrew Roth. “Thousands Join Anti-War Protests in Russia after Ukraine Invasion.” *The Guardian*, 2022. https://www.theguardian.com/world/2022/feb/24/we-dont-want-this-russians-react-to-the-ukraine-invasion.

Shahbaz, Adrian. “The Rise of Digital Authoritarianism.” Freedom on the Net. Freedom House, 2018.

Shahbaz, Adrian, and Allie Funk. “The Global Drive to Control Big Tech.” Freedom on the Net. Freedom House, 2021.

Sharafutdinova, Gulnaz. “The Limits of the Matrix - Ideas and Power in Russian Politic of the 2000s.” *Problems of Post-Communism* 59, no. 3 (2012): 17–30.

Sherman, Justin. “Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behaviour.” Issue Brief. Atlantic Council (Scowcroft Center for Strategy and Security), 2021. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/.

"This Year, Russia's Internet Crackdown Will Be Even Worse." The Atlantic Council, 2022. https://www.atlanticcouncil.org/blogs/new-atlanticist/this-year-russias-internet-crackdown-will-be-even-worse/.

Sherman, Justin, and Dylan Myles-Primakoff. "The Kremlin's Latest Target Is Online Media: Why the Russian Government Is Now Equating Digital Journalism with Foreign Espionage." *Foreign Policy*, 2021. https://foreignpolicy.com/2021/03/02/the-kremlins-latest-target-is-online-media/.

Simes, Dimitri. "Poll: Putin's Popularity Falls from 80% to 64%, Lowest in 5 Years." *CNS News*, 2019. https://www.cnsnews.com/news/article/dimitri-simes/poll-putins-popularity-falls-80-64-lowest-5-years.

Sivetc, Ludmila. "The Blacklisting Mechanism: New-School Regulation of Online Expression and Its Technological Challenges." In *Freedom of Expression in Russia's New Mediasphere*, edited by Mariëlle Wijermars and Katja Lehtisaari. London: Routledge, 2020.

Soest, Christian von. "Democracy Prevention: The International Collaboration of Authoritarian Regimes." *European Journal of Political Research* 54 (2015): 623–38.

Soldatov, Andrei, and Irina Borogan. "The New Iron Curtain Part 1: Putin Wakes Up to the Danger of a Free Internet." CEPA (Center for European Policy Analysis). Accessed August 11, 2022. https://cepa.org/the-new-iron-curtain-part-1-putin-wakes-up-to-the-danger-of-a-free-internet/.

Soldatov, Andrei, and Irina Borogan. "The New Iron Curtain Part 3: The Internet Is a Western Plot." CEPA (Center for European Policy Analysis), 2022. https://cepa.org/the-new-iron-curtain-part-3-the-internet-is-a-western-plot/.

Soldatov, Andrei, and Irina Borogan. "The New Iron Curtain Part 4: Russia's Sovereign Internet Takes Root." CEPA (Center for European Policy Analysis), 2022. https://cepa.org/the-new-iron-curtain-part-4-russias-sovereign-internet-takes-root/.

Soldatov, Andrei, and Irina Borogan. "The New Iron Curtain Part 5: Russia's War Against Silicon Valley." CEPA (Center for European Policy Analysis), 2022. https://cepa.org/the-new-iron-curtain-part-5-russias-war-against-silicon-valley/.

Soldatov, Andrei, and Irina Borogan. *The Red Web - The Struggle Between Russia's Digital Dictators And The New Online Revolutionaries*. PublicAffairs, 2015.

Solingen, Etel. "Of Dominoes and Firewalls: The Domestic, Regional, and Global Politics of International Diffusion." *International Studies Quarterly* 56 (2012): 631–44.

Stogova, Evgeniya. “Закон Об Уголовном Наказании За Фейки. Как Он Изменил Работу Журналистов.” *RBC*. Accessed August 10, 2022. https://www.rbc.ru/technology_and_media/05/03/2022/6223325d9a7947835d28df5d.

Tadtaev, Georgyi. “«Новая Газета» и The Bell Решили Прекратить Освещать События На Украине.” *RBC*. Accessed August 10, 2022. https://www.rbc.ru/politics/04/03/2022/622240959a79473a2ec999cd.

“The Return of Digital Authoritarianism: Internet Shutdowns in 2021.” Access Now, 2022. https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf.

Tishina, Yuliya, and Yurii Litvinenko. “Губернаторов Ведут На Контакт: Чиновников Пересаживают На Мессенджер От VK.” *Kommersant*, 2022. https://www.kommersant.ru/doc/5381031.

Tosun, Jale, and Aurel Croissant. “Policy Diffusion: A Regime-Sensitive Conceptual Framework.” *Global Policy* 7, no. 4 (2016): 534–40.

Traynor, Ian. “Putin Aims Kursk Fury at Media.” *The Guardian*, 2000. https://www.theguardian.com/world/2000/aug/25/kursk.russia2.

“Understanding Russia’s ‘Sovereign Internet’: What Happens If Russia Isolates Itself from the Global Internet?” Flashpoint, 2022. https://flashpoint.io/blog/russian-runet-sovereign-internet/.

Access Now. “Updates: Digital Rights in the Russia-Ukraine Conflict,” 2022. https://www.accessnow.org/digital-rights-ukraine-russia-conflict/.

Van der Vet, Freek. “Imprisoned for a ‘like’: The Criminal Prosecution of Social Media Users under Authoritarianism.” In *Freedom of Expression in Russia’s New Mediasphere*, edited by Mariëlle Wijermars and Katja Lehtisaari, 209–25. London: Routledge, 2020.

Vincent, James. “Russia Bans Instagram as Promised, Blocking Access for 80 Million Users.” *The Verge*. Accessed August 10, 2022. https://www.theverge.com/2022/3/14/22976603/russia-bans-instagram-facebook-meta-call-to-violence.

Wakefield, Jane. “Ukraine Invasion: How the War Is Being Waged Online.” *BBC*. Accessed August 10, 2022. https://www.bbc.com/news/technology-60559011.

Walker, Shaun. “Russian Parliament Votes for Law That Could List CNN as ‘Foreign Agent.’” *The Guardian*. Accessed August 10, 2022. https://www.theguardian.com/world/2017/nov/15/russia-to-register-international-media-as-foreign-agents.

Weber, Valentin. “The Worldwide Web of Chinese and Russian Information Controls.” Centre for Technology and Global Affairs, 2019.

Weiss, Moritz, and Vytautas Jankauskas. “Securing Cyberspace: How States Design Governance Arrangements.” *Governance*, no. 32 (2019): 259–75.

White, Stephen, and Ian McAllister. “Did Russia (Nearly) Have a Facebook Revolution in 2011? Social Media’s Challenge to Authoritarianism.” *Politics* 34, no. 1 (2014): 72–84.

Wijermars, Mariëlle, and Katja Lehtisaari. “Introduction: Freedom of Expression in Russia’s New Mediasphere.” In *Freedom of Expression in Russia’s New Mediasphere*, edited by Mariëlle Wijermars and Katja Lehtisaari, 1–15. London: Routledge, 2020.

Xu, Xu. “To Repress or to Co-Opt? Authoritarian Control in the Age of Digital Surveillance.” *American Journal of Political Science* 65, no. 2 (2021): 309–25.

Xue, Diwen, Leonid Evdokimov, Eric Wustrow, Reethika Ramesh, Andrey Viktorov, Simone Basso, ValdikSS, Arham Jain, and Roya Ensafi. “Throttling Twitter: An Emerging Censorship Technique in Russia.” *IMC’ 21 Virtual Event*, 2021. https://censoredplanet.org/assets/throttling-imc-paper.pdf.

Xynou, Maria, and Arturo Filastò. “New Blocks Emerge in Russia amid War in Ukraine: An OONI Network Measurement Analysis.” OONI (Open Observatory of Network Interference), 2022. https://ooni.org/post/2022-russia-blocks-amid-ru-ua-conflict/#blocking-of-news-media-websites.

Yayboke, Erol, and Sam Brannen. “Promote and Build: A Strategic Approach to Digital Authoritarianism.” Policy Brief. Center for Strategic and International Studies, October 2020.

The Moscow Times. “YouTube Blocked in Ukraine’s Russian-Occupied Kherson,” 2022. https://www.themoscowtimes.com/2022/07/06/russian-police-chiefs-top-aide-arrested-on-corruption-charges-a78217.

Zakharov, Andrei, and Ksenia Churmanova. “How Russia Tries to Censor Western Social Media.” *BBC*, 2021. https://www.bbc.com/news/blogs-trending-59687496.

Zvereva, Vera. “State Propaganda and Popular Culture in the Russia-Speaking Internet.” In *Freedom of Expression in Russia’s New Mediasphere*, edited by Mariëlle Wijermars and Katja Lehtisaari. London: Routledge, 2020.

Interfax. “Венедиктов Сообщил, Что ‘Эхо Москвы’ Отключено От Эфира,” 2022. https://www.interfax.ru/russia/825574.

BBC. “Госдума Приняла Закон Об Уголовной Ответственности За Фейки о Российской Армии.” Accessed August 10, 2022. https://www.bbc.com/russian/news-60615902.

Levada Centre. “Одобрение Институтов, Рейтинги Партий и Политиков,” 2022. https://www.levada.ru/2022/03/30/odobrenie-institutov-rejtingi-partij-i-politikov/.

Roskomsvoboda. “Самыми Скачиваемыми в России Приложениями Стали VPN-Сервисы,” 2022. https://roskomsvoboda.org/post/vpn-servisy-stali-chashe-kachat/.

Ekho Kavkaza. “«Эхо Москвы» Удалит Свои Аккаунты в Соцсетях и Отключит Сайт,” 2022. https://www.ekhokavkaza.com/a/eho-moskvy-udalit-svoi-akkaunty-v-sotssetyah-i-otklyuchit-sayt/31736236.html.