CYBER POLITICS OF RUSSIA: SURVEILLANCE, CENSORSHIP AND ACTIVISM

Thesis submitted to Jawaharlal Nehru University

For award of the degree of

MASTER OF PHILOSOPHY

SUDHANSHU KUMAR

Centre for Russian and Central Asian Studies

School of International Studies

JAWAHARLAL NEHRU UNIVERSITY

New Delhi 110067

2022

Date: 25/01/22

DECLARATION

I declare that the dissertation entitled **"Cyber politics of Russia: Surveillance, Censorship and Activism"**, submitted by me for the award of the degree of **Master of Philosophy** of Jawaharlal Nehru University is my own work. The dissertation has not been submitted for any other degree of this University or any other university.

S. Kumar

Sudhanshu Kumar

CERTIFICATE

We recommend that this dissertation be placed before the examiners for evaluation.

A. Upadhyay

Prof. Archana Upadhyay
(Chairperson, CRCAS)

अध्यक्ष/Chairperson
रूसी और मध्य एशियाई अध्ययन केन्द्र
Centre for Russian & Central Asian Studies
अंतर्राष्ट्रीय अध्ययन संस्थान
School of International Studies
जवाहरलाल नेहरू विश्वविद्यालय
Jawaharlal Nehru University
नई दिल्ली/New Delhi - 110 067

A. Upadhyay

Prof. Archana Upadhyay
(Supervisor)

PROFESSOR
Centre for Russian & Central Asian Studies
School of International Studies
Jawaharlal Nehru University
New Delhi - 110 067

Acknowledgement

This project would not have been possible without the support, effort and cooperation of many people.I would like to extend my profound sense of gratitude and respect to my esteemed supervisor Professor Archana Upadhyay for sincere guidance, encouragement, strong motivation and idea oriented discussion, which has enabled me to accomplish this dissertation work. I feel delighted in expressing my sense of thankfulness to the CRCAS staff for the continuous encouragement and help.

I would also like to express my sincere thanks to:

- All the technical and administrative staff of SIS, JNU administration and library for help at every step.
- All research scholars of the centre especially my batchmates for help and valuable suggestions.
- My friends Sheetal, Avinash, Nikhil, Soumya and Pranveer for encouraging and supporting me whenever I needed.

Finally I express my gratitude to my parents and family members for being with me at every moment and providing continuous moral boosting and affection during thesis work.

Contents

Abbreviations

GDP-Gross domestic product

TIN-Tax Information Network

FSB-Federal Security Service

SORM- Sistema Operativno Rozysknih Meropriyativ

DNS-Domain Name System

VOIP-Voice over Internet Protocol

SNS-Social networking sites

ISPs-Internet Service Providers

KGB-Komitet Gosudarstvennoy Bezopasnosti

CIA-Central Intelligence Agency

LGBTQ-Lesbian gay bisexual transgender queer

VPN-Virtual private network

IT- Information Technology

LAN- Local Area Network

RTU- Russian Technological University

DPI-Deep packet inspection

NGO-Non-governmental organisations

RSF-Reporters Without Borders

NATO-North Atlantic Treaty Organization

BRICS-Brazil Russia India China and South Africa

EU-European Union

DDoS-Distributed denial of service

IRA-Internet Research Agency

ECHR-European Court of Human Rights

Chapter 1- Introduction

Background

In the 1950s, the KGB destroyed a state-of- the-art-invention for fear of the chaos it could have on the Soviet Union. The engineer who had designed it, Vlamadir Friedkin, had not created a deadly virus or a nuclear bomb, but what the KGB feared was a photocopier that allowed one to make copies of articles from foreign journals and enabled the free flow of information. Friedkin's photocopier is an indication of the intellect that drives Russia's crackdown on the Internet.

While tracing the history of internet censorship in post-Soviet Russia and how communication technologies have enhanced over time, the central figure is Vlamadir Putin, who has also served as the FSB director (Federal Security service) for a short duration. Putin compelled Russian internet service providers to install an invasive surveillance program into their server networks. This system is called SORM (Sistema Operativno Rozysknikh Meropriyatiy), a backdoor to the country's internet communications. The Soviet-era phone tapping system inspires it. Since his re-election in 2012 was met with mass protests, policymakers in Moscow became increasingly anxious about the Internet as an American instrument to orchestrate colour revolution. Putin and his inner circle of advisory decided to restore national sovereignty in cyberspace just as they had done so with federal television channels a decade ago. Following Russia's seizure and annexation of Crimea in 2013, the government in Moscow asked Twitter to close the accounts of far-right Ukrainian parties, and Twitter complied.

At the same time, Putin turned up the heat on other foreign social media platforms and signed a decree that requires global internet firms to store Russian clients' user data on local servers within the Russian Federation. This relocation would allow the FSB to expose the servers to SORM, giving state bodies the ability to monitor the behaviour of Russians on foreign social media platforms. Similarly, Putin's government has sought to restrict the impact of social media by emitting and filtering. The Federal Service for Communications, Information technology and Mass Media (Roskomnadzor) has blacklisted some websites of political Opposition leaders, including the news portals of Gary Kasparov and Alexei Navalny.

Furthermore, bloggers with more than 3000 followers were required to register themselves in official ledgers.

The Russian political establishment sees the Internet as a disruptive instrument in politics as it gives a mechanism to people for circumventing and passing the traditional media set-ups of the Russian government.
Several advancements in the recent past in Runet(Russian Internet) regulation evolve into a picturisation of the Russian state's intention to capture the digital sphere in the bag of national control. The Internet sovereignty forum organised in May 2016 by the federal administration focuses on aspects related to Big data, Internet of things, artificial intelligence etc.

The whole puzzle revolves around disseminating the idea of developing an isolated and closed network in Internet administration. The Russian political establishment is exchanging this idea with people in response to the twin perils of terrorism and American domination over internet services. However, the complexity of several laws related to the Internet and their incomplete and dysfunctional implementation creates perturbation for Russia's IT industry. The frontline technocrats, developers, bloggers, Internet service providers, journalists, hosting agencies, and others have to mend their daily functioning following these laws. The challenges that emerged from these restrictions moved on simultaneously with new paths to bypass and circumvent these restrictions. Several organisations and hacktivists come together to launch a mass level campaign for Internet freedom through widespread dissemination of information and hacking into restricted networks.

The Russian state is looking forward to copying the Chinese model of the Internet. Beginning in 2014, the government made attempts to develop a "sovereign internet" similar to the Chinese. In May 2019, sovereign internet law was signed by President Putin, giving authority to Roskomnadzor (media regulator) to take control of Runet if cut from the world wide web. This will provide Russia with a similar convenience like the Chinese government to isolate the national Internet from the global one. In the long run, it may create a model for other countries to do the same, which will eventually lead to the dissolution and separation of the global internet structure. Since the Chinese way of developing their own high tech Internet

firewall is challenging to create or replicate, the Russian model of cutting off from the global Internet is very convenient for authoritarian regimes to follow.

The Russian surveillance technology works on using legal and administrative means for controlling and tightening the circulation of information and intimidating top bosses of internet companies and service providers. The removal of the CEO of Vkontakte is an example of how the Russian political establishment undertakes the operation of intimidation in case of conflict.

This study aims to understand the interplay between the several characters in Russian cyberspace, especially digital dissidents and authorities governing the state-centred Internet. The study builds upon observation of how Russian civil society, internet activists, anonymous hackers, and common masses deal with restrictive internet policies by developing and encompassing different individual and collective resistance strategies.

Literature review

In 1991, Russia inherited a broken and dysfunctional communication system with no significant reach outside, but today it stands out in the top ranks of those developing countries with global internet outreach. According to the survey of the Pew Research centre, approx 73 per cent of people in Russia have online access in comparison to 63 per cent in China and 87 percent in the USA. Sibert, Peterson & Schramm (1956) discuss how press freedom and censorship of media has always been a subject of interest in academia concerning the peculiarities of different political systems of Russia at other times.

To explain the nature of the Russian establishment's influence over the Internet, several studies have outlined Russian society's history and its media history. Many research pieces have concluded that censorship and control have been a primary functioning element in the governance of Russian culture and how it has been imbibed into the implicit dimension of lived experiences for its natives. Simons and Strousky (2006) have highlighted this by enumerating examples of how deep-rooted authoritarianism traditions have stepped into the everyday consciousness of the population. These traditions have emerged due to a mix of factors, such as how a large territory with difficult living conditions must be protected from different sides from outside incursions. These all have culminated into a unified Russian populace with its authority residing into a dominant and powerful leader.

Many scholars have drawn coherent comparisons between modern-day state surveillance and the idea of the Panopticon. Mcmullan(2015) comprehends that the parallel between Jeremy Bentham's Panopticon and CCTV may be exact, but it becomes more tricky and confusing when it steps into the world of data surveillance. As a work of architecture, Panopticon allows the watchman to watch the occupants without their awareness and knowledge of whether they are being observed or not. This idea of Panopticon has been revitalised again by French philosopher Michel Foucault in his 1975 book Discipline and Punish. Foucault illustrated very clearly how Panopticon symbolises the predisposition of autocratic societies subjugating their citizenry.

McMullan (2015) argues that The Snowden leaks about the scale of operations of GCHQ(Government Communications Headquarters) in the UK and NSA (National Security Agency) in the USA make the system more panoptic post-Snowden. The relative intangibility of data surveillance, due to the back of the physical sense of exposure in the face of authority, makes surveillance invisible in our imagined reality.

Internet censorship is a typical and standard tool in authoritarian regimes, especially in the context of non-democratic countries. According to the 2009 report of the open net initiative, research in this area has been primarily focussed on China and the Middle east. The Chinese government owns the most Intrusive and advanced Internet filtering technology system today. By using methods like selective blocking of sites, blacklisting of web addresses, scanning for banned keywords in internet traffic, the people's republic of China has been able to restrict the access of online information to its citizens.

Although the internet filtering system is a robust censorship tool, it is just one of the many methods to restrict the content on the Internet. Ziffrain and Palfrey (2008) have identified several other non -filtering ways to limit Internet content access. They are termed as soft means of control. It includes laws, acts, rules and regulations related to media, information technology and communications, internal security or national security, restricting the publication, circulation and access to objectionable content on the Internet.

Since Russia is not engaged in Internet filtering and monitoring efforts at a large scale, it resorts to relying on soft means of control to deal with displeasing online content. Russia presents an interesting case study precisely because it has been triumphant in developing control and influence over the Internet without resorting to content filtering technologies. (Fossato, Lloyd & Verkhously, 2009).

Over the last few years, internet regulation has specifically increased more in Russia than in the rest of the world. Due to a series of progressively restrictive legislation, the powers of the Russian Prosecutor General's office and federal agency Roskomnadzor to block and take down URLs (uniform resource locator) have increased many folds. Legislations like mandatory registration of bloggers with government agencies and increased access of

Russian authorities into user data are continually reshaping the battlefield for freedom of speech and expression and data privacy.

Soldatov & Borogan (2015) highlight that Russia has not entirely broken with its Soviet past; the SORM boxes, invented by the KGB, are still getting updated and are used to curb the political opposition. Though, in other ways, Russia has become an entirely new country of digital activists who have learnt to use the Internet to elude government restrictions and spread uncensored information. This creates unease and regular frustration for government authorities in Russia. They investigate the collision between two great forces of surveillance and control on one side and freedom on the other side. They conclude that it does not yet have a definite ending. The significance of these events are multifaceted as it extends far beyond the region of Russia, and not just because the Russian state has continuously tried to dodge and manipulate the global rules of the Internet to develop and create national boundaries in what today is a wide-open space. The events of the 2016 US election demonstrated that ignoring the cyber operations of the Russian government abroad can not be overlooked. In 2014, Russia allocated a monthly budget of 1.2 million dollars to the internet research agency to create a troll factory that was primarily staffed by students from St. Petersburg State University. The aim was to focus on controversial topics like gun control and racial violence in the US, that would accelerate the polarisation of the political landscape of the United States. They devised algorithms to sow discord on platforms such as Facebook and Twitter and also in the comments section of news outlets like The Guardian.

Sussman (2000) shows how the emergence of the Internet has formulated different types of complexities into the study and policymaking in the field due to its nature of being an unruly and decentralised communication medium. On the surface, media freedom in Russia has improved since the collapse of the Soviet Union, yet in truth, the government in Moscow uses unique methods of internet censorship that is distinct from the surveillance practices of other nations.

Faris, Wang & Palfrey (2008) have highlighted how the new online social media platforms have reshaped the stage for civic participation and dialogue. In an economy dominated by energy companies, domestic brands such as the search engine Yandex, social media platform

Vkontakte, and security software Kaspersky labs are rare achievements. The success of these firms relies on vibrant and free internet access only. But the further attempt to control the Internet is likely to damage Russia's tech Savvy industries.

Shirky (2008) also mentions in a similar way how these channels of web-based social media help in circumventing official channels of information in countries where there exist a certain level of restrictions in respect of the media environment. The Russian government is accustomed to deal with a hierarchical structure, where they go after the bosses of organisations to deal with the crisis. On the Internet, everyone can participate without authorisation.

Tselikov (2014) highlights how Russian internet users, activists, civil rights advocates are bypassing these legislations through different tactics of online and offline protest. Despite government efforts to gain the upper hand over Internet activists, they have found ways to outsmart the Russian agencies' intrusive surveillance. The last two decades of the Internet in Russia is driven by the contradiction of the coexistence of state-centred Internet governance along with a rapidly developing internet populace.

In context to global internet governance, Russia's foreign policy has sought to shift the western narrative over the current international internet governance regime, where the US exists with a considerable advantage and upper hand. In a context where states actively construct a direct link between cyberspace and foreign policy. The Russian foreign policy of the Internet sees the current running model of the Internet as an enterprise of US-led hegemonic set-up which the US government would use to undermine the sovereignty of other States and supplant its world views, values, ideals and ethics. Even though the Russian system of state internet censorship has been gradually increasing in the past few years with its control over foreign and domestic internet companies, the regime of state censorship remains deficient. The tools of mass surveillance of internet users are only sufficient to counter a small number of dissidents and can not put a stop to the spread of information among thousands of users. (Soldatov 2014)

Julien Nocetti (2015) explores Russia's profound involvement in web governance. The divulgence of the US government's mass online surveillance program on monitoring internet traffic by Edward Snowden has formulated a notion of legitimacy for the government to control online activities in the virtual world. Russia seeks to vigorously cultivate coordination over internet governance and cybersecurity policy with en rapport nations. Russia is using both regional forums and international stages like the UN to highlight US dominance over Internet governance and demand a more significant role for other governments too. By presenting its case with issues of national security, prescribing more hierarchy and a more substantial role for governments, Russian foreign policy aims to politicise the problems regarding global cyber governance and attempt to reconfigure the network to make it suitable for its own domestic political, social and technological and strategic interests.

Soldatov and Borogan (2015) argue that intimidation is the tool on which the Russian state takes charge of dissent control. This system is only effective till the time people are confident that the government is in control. In case of a crisis of confidence, on upheaval or an emergency, the dynamic is transformed, and situations can turn upside down for the Russian political establishment. The Internet is not a top-down structure; they are horizontal creatures.

Christopher Hill (British historian of the Civil War in England) described In his work "The World Turned Upside Down" how press liberty in England made it easier for eccentrics to get into the print. 1641-1660 was a time of free press. Before and after that, there was strict censorship. Similarly, the Internet is also playing a significant role in Russia as it's impossible for the Russian establishment to control the mind of every single user. Information runs free like water or air on a network and is not easily captured. Here the content is not generated by the companies that operate websites and social media; they are just platforms where users come and create content. The Internet today is the printing press of today. Once the printing press enabled the free flow of information, today, the same is done by the Internet. Simple tools like Vkontakte and Facebook have created an environment where information cannot be controlled or suppressed completely and outrightly.

Critical Gaps in the Literature

With the above literature in mind, this study attempts to fill some of the following critical gaps. Most studies on Russia's internet system focuses on the different aspects of surveillance and control of the Internet. However, the multifaceted application of the Internet in Russia goes way beyond just surveillance and censorship. For instance on foreign policy, political system or socio-economic dynamics has not been assessed in great detail by the existing literature. Similarly, there has been a lot of focus on what are the implications of the use of technology like SORM for surveillance, but how the SORM works and how it functions to complete its objectives has not been assessed in the present literature.

Regarding Russia's surveillance methods, most works are either comparative studies with countries like China, Iran and North Korea or descriptive studies presenting the research in its origin and impacts. There is no work in great detail, highlighting working and functioning behind the technologies used by government agencies, tech companies and other organisations as to how they use software and hardware tools to fulfil their objectives. Similarly, what type of software tools are used by hacktivists and people on the Internet to bypass the censorship and restrictions on the Internet. The study aims to fill this gap in the literature by focussing on tools, mechanism, working and functioning of surveillance and counter-surveillance.

Definitions, Scope and Rationale

Definitions

The Internet

The Internet is a technical and nuanced concept, and its definition depends on what aspect is taken into consideration. The Internet has varied meanings based on its value orientation regarding the technological, social, commercial, cultural or metaphysical construct. A definition can also be created based on combining two constructs as well. According to Wikipedia: the Internet is a publicly accessible worldwide system of interconnected computer network that transmit data by packet switching using a standardised Internet protocol (IP). It is made up of thousands of smaller commercial, academic, domestic, and government networks. It carries various information and services, such as electronic mail, online chat, and interlinked web pages and other documents as the world wide web.

This research focuses on the political dimension of the Internet. More specifically, it approaches the Internet as a domain of realpolitik, including practices of security, surveillance, governance, authority, dissent, individualism and freedom.

The Runet

Runet, a portmanteau of ru and net/network, is the Russian language community on the Internet and websites. Runet is not entirely synonymous with the Internet in Russia nor Internet sites in Russian, not even with the set of websites in the .ru TLP (Top Level Domain), but more accurately refers to the sphere of Internet sites predominantly visited by Russian-speaking user, which form a part of contemporary Russian culture. (Wikipedia)

Internet censorship

According to webopedia, internet censorship is the practice of controlling, supervising, and restricting the creation, distribution and access of online content. It is done by government or private entities for dual purposes - either to ensure and develop safer and safe practices on the Internet or to suppress free speech and dissent against the government. Internet censorship is a very potent and viable tool for a government or an organisation to manage and control what its citizens and users can view. Though there also exist several set of tools on the Internet to

bypass and circumvent these restrictions. From using VPN (virtual protected network) to Tor browsers, there are different ways to access restricted content in a region.

Internet surveillance

Internet surveillance is the monitoring of Internet traffic and activity by looking into data stored and transferred over computer networks. It is carried out by governments, private organisation, criminal groups or even individuals often covertly. The legality over surveillance is always a question of debate as it depends on location, logic and liability. Several civil rights and privacy groups like the American civil liberties union, Reporters without Borders etc., have expressed concern over the increasing level of surveillance over the Internet, creating less space for political, social, and individual freedom.

Internet activism

Internet activism is the use of Internet technology tools to create social, political and cultural change. The use of these tools is done by a different type of agents like
hackers, culture jammers, journalists, NGOs, social activists, political dissidents etc.
Internet activism presupposes the reflection of ideological struggle or tensions in the real world to its projection in the online or virtual world. The strategies used by the agents of Internet activists involves: networking, publishing, educating, organising and mobilising. Activism, as it is practised in new media, often uses old means. Meikle (2000)

Rationale

In 1991, Russia inherited dysfunctional and broken communication from Soviet times. Still, even after that, it has made itself into one of the top ranks of the developing countries wired to the world. Online access in Russia has increased significantly, and around 77 per cent of people in Russia have access to the Internet today. Russia has built its own tech brands like search engine Yandex and social media website VKontakte instead of giving up its total markets to US tech giants like Google and Facebook. Since the Internet is penetrating deep into Russian society, it poses a continuous challenge to the Russian establishment to control the flow of information and content against the government. The Internet has become a breeding ground for dissenters, activists and NGOs who oppose government policies. In

response to that, the federal government has tried to restrict the content and data on the Internet, which is problematic for the Russian establishment. It has several tools and techniques of surveillance and censorship to fulfil its agenda. Similarly, people are using different mechanisms to bypass restrictions imposed by the government on the Internet to ensure their freedom. The study intends to contribute to the understanding of ideas behind Internet restriction and activism. The study covers several aspects of Russia's censorship and Surveillance efforts, including the dynamics of SORM, internet filtering systems, the role of Roskmnadzor and other federal agencies, and the use of Internet technology tools abroad in different situations. The study's focus is Russia's IT industry and especially its role in the Russian political system.

Scope

The interest in the process of change has translated the choice of historical methods as the fundamental methodology of the research. It should be considered that the relative age of the Internet creates different challenges in terms of methodology. Traditional history goes with usually the event, which can be traced to hundreds and even thousands of years; in comparison to this, the history of the Internet is too recent and short, very brief to become a proper subject for historical analysis. The Internet is a vivid example of accelerated development. The processes that may take longer in other fields and domains of study occur very rapidly when it comes to the Internet. But still, the Internet is worth studying from a historical point of view.

Internet studies or Internet research evolved as a separate study domain in the latter half of the 1990s, when the Internet became widely accessible to the common masses in different parts of the world. Internet research has two aspects: first, it is the practice of using the Internet for doing research in any area. Second, it is research having the Internet as its subject and field of study. Internet studies go along with several phenomena found on the web and take account of technological, cultural, social, psychological, local and global aspects of Internet communications. Internet studies have no particular or specific methodology but traditional methods found in other disciplines from communication theory to sociology, anthropology and cultural studies.

Internet studies use both qualitative and quantitative methods such as content analysis, case studies, surveys, data analysis, conversation analysis, network analysis etc. However, the properties of the new media like intertextuality, non-linearity, textual ephemerality and the use of multimedia etc., makes it tricky to apply traditional methods to the electronic environment.

As this study is on the Russian Internet and its political aspects, it does not cover other dynamics of the Internet related to cultural, social, business, creativity and advanced technological dimensions. The Internet is chosen as it is one of the important stages for political input, opinion formation and mandate building and contributes significantly to the political narrative in Russia. The Internet is an enabling and disabling tool simultaneously, and control over it can change the dynamics of governance and politics in a big way.

Surveillance and counter-surveillance are chosen as a field of study because they will help in understanding both the current and evolving nature of the relationship between the federal government and citizens.

Research problem

The central research problem that this study examines is the architecture of surveillance tools in contemporary Russia besides the role of the Russian state in developing these, distribution of capabilities among different actors like activists and hackers to bypass restrictions, explicitly focussing on IT industry in Russia concerning its role and place in internet censorship and information control over the Internet.

Research questions

1. Why has Russia placed such a great emphasis on internet surveillance and censorship?
2. What has been the role of the Russian establishment in promoting the idea of data surveillance over the Internet? Whether these efforts have helped the Russian establishment in curbing the dissent and political opposition in Russia.?
3. What are the political, economic, social, legal and foreign policy implications of the sovereign Internet law signed in May 2019 by President Vlamadir Putin?
4. What are the challenges faced by the IT industry in Russia due to state policies of surveillance and censorship?
5. What is the role of internet activists, opposition leaders, hackers and NGOs in providing a free flow of right information to the common masses, bypassing and circumventing restrictions imposed by the government?
6. How has the Russian establishment used its local and unique methods of data surveillance in disseminating its agenda overseas. Whether the Russian establishment can use these capabilities in future to change the dynamics of global internet governance?

Hypotheses

1. The Internet and media development in Russia has been witnessing a significant paradigm shift in the last decade, leading to the restructuring of government and politics in Russia.

2- Internet activism can help in regulating the effects of surveillance and censorship over the Internet in Russia.

Research Methods

This study has used the theoretical framework of surveillance, censorship and internet activism to identify the constituents within these systems and their interrelationships.

The study used both primary and secondary sources. Primary sources would include policy documents of the Russian federal government, speeches by Russian leaders in government and opposition, Russian media sources and reports by international organisations. Secondary sources would consist of books, journal articles, newspaper reports, think tank reports by both Russian and western sources.

The study is deductive as it tests the hypothesis based on the data collected. This research has primarily utilised Qualitative methods and descriptive analysis of data, along with some amount of simple statistical analysis of quantitative data.

For this study, the dependent variable is surveillance capabilities, and the independent variable is the state's effort on the Internet in implementing surveillance and censorship. The intervening variable is development in rational and global internet governance.

Chapters-

This study consists of four chapters apart from the Introduction and conclusion.

Chapter 1. Introduction

This chapter defines the context, rationale and background of the research, including the constituent elements, objectives, structure and scope of the thesis.

Chapter 2. Surveillance in the Russian Cyberspace: context and contours

This chapter explores a series of case studies covering the dimension of surveillance and censorship in Russian internet history.

Chapter 3 - Tools of surveillance and censorship : process and functioning of SORM

This chapter focuses on what kind of tools are used by the Russian state to control the flow of content over the Internet, formulating a narrative against the government. It will primarily focus on how the SORM helps in monitoring the dissent over Internet traffic for the Russian establishment.

Chapter 4 - Challenges of censorship and surveillance: Role of civil society and citizenry

This chapter focuses on the role of new online revolutionaries and activists in fighting with dual challenges of censorship and surveillance. This chapter emphasises how political opposition, activists, and NGOs deal with the Russian establishment's policies over the Internet.

Chapter 5 - Global internet governance : Foreign policy implications for Russia

This chapter has examined the Imprints of Russian internet capabilities in overseas and foreign countries. This chapter focuses on how Russian internet policies have affected global internet governance, especially regarding its Ukrainian condition and 2016 US elections.

Chapter 6 - Conclusion

The final chapter has recapitulated the research problem, the main findings of the study and concluded the academic and policy implication of these findings.

Chapter 2: Surveillance in the Russian Cyberspace: Context and Contours

Amendments To The Law On Personal Data

As per the Country Commercial Guide of the United States International Trade Administration[1], with a GDP of USD 4.016 trillion in purchasing power parity, Russia is the world's sixth-largest economy by purchasing power parity. More than 140 million people live in the nation, and their spending power is expanding, therefore they need well-known worldwide brands and high-quality service. In context to this eventuality, Internet services are one of the domains where people want easy access to information, entertainment and knowledge. With the advent of the World Wide Web, the world has changed dimensionally in aspects of time and space. This creates both advantages and disadvantages regarding generation, dissemination and control of information from one part of the world to another. Though the internet was basically formed on the fundamental basis of free flow of information it creates difficulties for governments around the world to regulate and control the dissemination of right and wrong information locally. In a similar fashion Russian government's policies and executive actions shows tangible evidence of how it is dealing with challenges associated with free flow and control of information in the background of local contingencies.

In this respect the Russian government uses several tools and techniques for fulfilling its mandate of control of information. It uses both soft and hard means of control for regulation of data and information over webspace. In soft means of control the Russian government passes several legislation regarding data control over the internet. For example, Individuals' personal data is protected by Russian Federal Law No. 152-FZ on Personal Data, which was passed on July 27, 2006, and applies to all organisations that collect, use, or distribute such information. The Law on Personal Data is applicable in all 50 states and the Russian Federation[2].

---

1 United States non-agricultural exports are promoted by the International Trade Administration (ITA), a department of the Commerce Department.

2 On February 28, 1996, the Russian Federation joined the Council of Europe as its 39th member state.

The Federal Law of 30 December 2020 No 519-FZ on Amendments to the Federal Law on Personal Data, which amends the Law on Personal Data, took effect on 1 March 2021 (with the exception of one section, which is set to take effect on 1 July 2021) ("Amendments"). The Amendments were ratified by Kazakhstan's[3] President on 1 March 2021.

When it comes to organisations that desire to disclose personal data on the internet and in print, for example, employers vs their workers, the Amendments make a substantial difference in the legal environment. The amendments effectively provide data subjects greater control over the processing of their personal data for dissemination purposes, as opposed to before.

Russia's Personal Data Law was revised on 1st March 2021 for the processing of publicly available personal data, barring one change: per the Russian protection authority, there was no requirement to re-execute consents for the circulation of personal data. This was in abidance with the law that was already in force before 1 March 2021.

Fundamentally, the new amendments concentrated on shielding published personal data against uncontrolled distribution. In simpler words: the revisions aimed at controlling further dissemination of publicly available personal data by third-party readers.

According to the previous version of the Russian Personal Data Law[4], data operators were empowered to make use of personal data per their will. They could process the vital information to "n" number of people without a data subject's consent. This essentially meant that any published personal data, including the one on the internet, could easily be further distributed by any business.

Fortunately, the present amendments don't give a green signal to such an approach. Per the new rules, a category was decided with the name "personal data made publicly available"-defined as personal data to which congregating individuals may have access to,

[3] 'Kassym-Jomart Kemelevich Tokayev, a Kazakh politician and diplomat, has been the country's president since March 20, 2019.

[4] Data protection legislation in Russia is a fast evolving area of Russian law, with the majority of it being passed in 2005 and 2006.

only after the data subject's specific consent for distribution of their personal deets. The other pivotal things that were essentially the part of the new amendments included the following:

- A data operator is restricted from disseminating vital information if there is no consent available. The operator must imperatively possess a clear statement stating that the user has given his/her permission to share the vitals. Additionally, under no condition, the data subject's silence is to be considered as a nod for agreement.
- Data subjects are licensed to bestow their consent anytime directly to the data operator.
- The right to establish certain restrictions or conditions on their information is given to data subjects. Consequently, the operators must never ignore these important guidelines.
- Data subjects are permitted to give their request to data operators if they wish to avert dissemination of their information. The user can make his/her decision regarding this context at any point. Additionally, the consent terminates as soon as the operator receives the request from the data subject.
- Just in case the operator is reluctant to abide by the terms laid by the data subject even after receiving the request to stop dissemination, the subject is granted to pursue his/her complaint in the honourable court. The body is likely to hear this case on priority and give its verdict at the earliest. Post giving the judgment, the operator needs to act swiftly by stopping the distribution of personal data within a period specified by the court.

Further, the Russian data protection authority also declared a special format of the dissemination consent form that is to be religiously followed by data operators. These came into force on 1st September 2021 possessing the following details:

- The complete name of the data subject including his/her contact details.
- Name, address, registration number, and the TIN of the data operator.
- Furnishing details of the website where all the data related to the data subject shall be published.
- What's the intent of data processing?

- Any restrictions or conditions set up by the data subject.

It is also paramount to highlight here that anyone who does not abide by these amendments necessarily has to pay heavy fines. The nod to such penalties came into effect on 27 March 2021. Also, anyone committed to doing repeated violations had to face the brunt of multiplied fines.

Additionally, the need to take data subject's written consent in certain circumstances was adopted by the State Duma (the lower house of Russian Parliament) on 16 February 2021 in its first reading. The State Duma is one of the houses of the Russian parliament, the Federal Assembly, and it represents the interests of the Russian people. It is a legislative authority of 450 members that are chosen to serve terms of five years. Adoption of federal constitutions and federal laws, supervision of Russian government activities, nomination and dismissal of Central Bank, Accounts Chamber, and High Commissioner for Human Rights officials, declaration of amnesty, and issues relating to international parliamentary cooperation are among its primary responsibilities.

It stressed the urgency of getting a written consensus particularly for processing of sensitive data, sharing the information to third parties, and cross-border transfers of personal data to all those countries that do not furnish sufficient protection of personal data subjects. The current law clearly states that special heed must be paid by everyone involved in the chores related to "data-dealings". Once again, someone ditching these guidelines has to necessarily pay the price of this ignorance.

A new criminal offence, if data of protected persons are shared

Code-based continental civil law is the basis of the legal system of Russia. Both federal and regional laws exist; however, in the event of a dispute, federal legislation takes precedence. In general, data privacy problems are handled at the federal level, and the regions of Russia do not enact any particular legislation or regulations in this regard.

The most recent Russian Constitution, which guarantees each individual the right to privacy and the confidentiality of personal and family secrets, was approved in 1993. Each person has

the right to keep his or her communication private, and any restrictions on this right must be approved by a court. Only with the individual's agreement may information about his or her private life be collected, stored, used, and disseminated. Special laws (for example, on communications) and particular regulations created in regard to these laws govern the preservation of these fundamental rights.

In 2007, Russia passed a substantial data privacy legislation, Federal Law No. 152-FZ on Personal Data, which was enacted on July 27, 2006. (the Personal Data Law). The Personal Data Law addresses nearly every aspect of data protection, including what constitutes personal data and the categories of data to be procured and also processed how and in what circumstances data can be collected and processed, and what technical and organisational safeguards must be implemented by companies or individuals collecting data.

The Personal Data Legislation, unlike European law[5], does not differentiate between data controllers and data processors. As a result, every person or institution that works with personal data is deemed a personal data operator and is therefore subject to the Personal Data Law. There are also other particular rules, which primarily concern the technical aspects of data processing and, to some degree, explain the terms of the Personal Data Law.

Since 2007, data privacy has never been a hotly debated or heavily enforced issue. This, however, changed substantially in 2014. The government's overall stance to privacy became rather protectionist. In 2014, the Russian parliament amended the Personal Data Law (later renamed the Data Localisation Law) to oblige data operators that gather personal data from Russian residents to store and process such data in Russian systems. The Data Localisation Law[6] was heavily criticised by industry and the media, yet it went into effect on September 1, 2015. While this regulation resulted in significant profits for Russian data centres, it also

[5] The GDPR has a "controller" and a "processor," as opposed to the PD operator notion in the 152-FZ. The GDPR states that the controllers are responsible for determining the goals and methods of processing, while the processors acting on their behalf are in charge of actually carrying it out.

[6] The 2015 Russian data localization legislation requires "data operators" to ensure that Russian citizens' personal data is captured and preserved in Russian databases. Essentially, the law requires that personal data of Russian citizens be gathered and stored in a Russian database.

resulted in significant expenditures for regular enterprises that needed to restructure their data storage infrastructure.

A new amendment in the existing criminal code was formulated: leaking out the data of protected persons was a criminal offence in the country. This essentially meant that confidential information related to "protected persons" including employees of the Investigative Committee, FSB, Federal Protective Service, National Guard, Ministry of Internal Affairs, Ministry of Defense Judges, prosecutors, investigators, law enforcement officers, and their relatives was to be concealed. Consequently, the different departments of the Government alongside mobile operators were instructed to assiduously follow the same.

Previously, the law aimed at the temporary restriction of the distribution of data related to "protected persons" of the country. However, with the application of new revisions, it is not permitted to share data of these highbrows by anyone.

Surveillance in the Russian Internet

The potentially destabilizing impact and national security reverberations of information flow within society were concerning factors for the Russian Government. In the calendar year 1995, the country embraced the "Law on Operational Investigations" permitting the FSB[7] authority to envision all private communications of their fellow countrymen, including electronic communications. Consequently, this led to the emergence of the first "System for Operative Investigative Activities" also abbreviated as SORM was built. This was later extended in the year 1998 giving rise to SORM-2 and was primarily designed to meticulously monitor internet traffic. At the onset of the year 1998, Russia was seen putting forward annual resolutions to the United Nations General Assembly in context to "Developments in the field of information and telecommunications". Additionally, the year 1999 saw submission to the UN Secretary-General that covered the topic "principles in international information security". Per these submissions, one thing was crystal clear that the concern

[7] The promotion of international standards for information non-aggression became a consistent theme, with Russia also leading blocks of states in efforts. In 2011 and 2015 it collaborated with other countries from the Shanghai Cooperation Organization to submit joint proposals to the UN General Assembly for an "International Code of Conduct for Information Security," for example.

related as much to international flows of information content as to the flourishing field of cyber security. On September 9th, 2000, just after the massive media coverage of the Kursk submarine tragedy the previous month, the then President Vladimir Putin serving his first year of office passed the new "Information Security Doctrine of the Russian Federation" that had been developed by his own security council. The document demonstrated the indispensability of freedom of speech and the media. And just not this, it also specified supposed perils to natural security due to the flow of information.

In continuation; apart from accomplishing these steps, the Government proactively took part in the global digital economy and made sure the country's domestic internet industry simply flourished [8].Thereon, the Russian Internet became a topic of public discourse. Thankfully, it saw little or no prohibition throughout the 2000s, even after massive restrictions on media and civil society. But at no point, it meant that significant efforts were not taken to oversee the new technology's impact on political stability. The country encountered mass social-media-fueled protests at home.

In the early 2010s, and particularly after the 2011-2012 White Ribbon Protest Movement, the country saw Vladimir Putin regaining his power of the presidency. After this, Russia evolved as the epitome of an innovative and experimental approach to information manipulation. It differed substantially from the often discussed Chinese "Great Firewall" system that continued to remain in highlights for a long time. The ultimate objective was to implement an approach that primarily stressed systemic technical censorship. In simpler words: the country pioneered a quirky model that relies on a blend of less overt, more plausibly deniable (no clear evidence) and legalistic approaches. Moreover, this model for the domestic modulation of information not only proved efficacious for Russia's own political system but emerged beneficial for a plethora of other countries in which a systematic-censorship viewpoint was not technologically or politically feasible.

[8] This included, notably, a widely-recalled December 1999 meeting between then-Prime Minister Putin and members of the Russian Internet community in which, under pressure from the assembled bloggers and ISP-directors, Putin rejected a considered plan for more centralized government control over the Internet and promised that they would be consulted before further policy decisions. But some dynamics of consultation continued throughout the 2000s and beyond. During Dmitriy Medvedev's presidency, 2008- 2012, Internet entrepreneurship was also avidly promoted as part of his economic modernization program. Medvedev toured Silicon Valley, met with young ICT entrepreneurs, and himself utilizing social media.

As a result, since the year 2012, Russia has blacklisted a series of censored websites legitimately. This move was realized as an absolute change in the country as the Internet was essentially uncensored. However, this led to significant pressure on an eclectic number of producers that eventually paved the way for hosts of controversial online content. This increase could easily be felt by the Russian Government post the 2012 period. To handle these pressures in an effective way, new laws and quasi-democratic processes found their way in the legal aspects of the country. The intent of these laws was to create a legal base for the blocking of a wide variety of content during this period. Additionally, these also meant to zero in on the user data, while also ensuring to put a significant burden of liability on content intermediaries.

Let's quickly enlighten you with the monikers of some laws that were discoursed a lot:

- **The 2013 "Anti-Piracy Law"-** There was quite a similarity of this law with SOPA/PIPA[9] legislation in the United States, which eventually was disapproved. All thanks to the massive protests in the country about the impact on internet intermediaries. In the same way, this Anti-Piracy Law was immensely objected to with petitions being filed. Despite these protests, the law was embraced by the Government and went into force.
- **The 2014 "Anti-LGBT Propaganda Law"-** This law primarily aimed at safeguarding children from child pornography and content related to illegal drugs and suicide. It also focused on blocking all such contents that could adversely impact the children of the country. This law was basically the extension of the guidelines that were passed in the year 2012.
- **The 2014 "Law on Pre-Trial Blocking of Websites"-** As soon as this law was successfully implemented in the country, all such websites constituting content in the shape of "incitement to extremism or riots" were blocked at the drop of a hat.
- **A package of "Anti-Terrorist" laws passed in the summer of 2014-** Also termed "Blogger's Law"[10], it primarily intended that all bloggers with a daily audience

[9] Bills called the Stop Online Piracy Act (SOPA) and a bill called the PROTECT IP Act (PIPA) were both brought into the United States House of Representatives and the United States Senate around late 2011.

[10] Russian Internet legislation, called the "blogger's law," enforced website registration, site limitation, and harsh penalties for websites that the authorities deemed to be inciting opposition in the country.

surpassing the figure of 3000 a day must register themselves on a national list. What's more, they were also directed to diligently follow media regulations for fact-examining their posts. Plus, the law also included "anti-encryption", which aimed at furnishing access to the Government related to encrypted services. The package didn't terminate here! It also included a "user data storage requirement", meaning that every platform or website dealing in the collection of subscribers-reaping the benefits of the internet- must store this data for a minimum period of three years. The Government at any point in time might ask for access to this data.

Albeit, the above-discussed laws were never enforced systematically; however, they were enough to create fear in the minds of content producers along with intermediaries, prohibiting them from fabricating something that was not legitimate. In the advent of employing unlawful means by anyone, the laws demanded an investigation on legal grounds.

That said; social media platforms and online media outlets are always sitting ducks to the perils of potential financial takeovers and pressures to see the backside of editors, CEOs, or other indispensable members. This stands to reason: during the occurrences when these members are unable to bow to content restriction pressures, they might see their position swapped.

Delving a bit deeper; the originator of Russia's most popular social network (VKontakte)-Pavel Durov is known to have left the country in April 2014 after he was fired as CEO. Consequently, Durov was pressured to sell all his shares, which were finally possessed by oligarchs in close association with the Russian establishment. The founder without hesitating stated that the conflict had transpired due to his unwillingness to divulge user information or block pages in context to Alexei Navalny's campaign, alongside the conflict in Ukraine.

The Russian government's perspective on information control over the internet, in addition to surveillance, new methods of mass content production, narrative manipulation plays a vital role to sabotage and demean the opposition voices against the Russian establishment and its leaders. Russian content manipulation often pays heed to frame and promote particular narratives. In 2021, the Russian internet and cyber strategy the core concept remains the

"information security"[11]. Plus, Putin's government still continues to launch proposals of "codes of conduct for information security" whilst justifying the internet control in the country and reshaping the internet globally[12]. A key factor for pushing towards RuNet is Russia wants to lessen the foreign-made hardware dependency as well as software equipment which include the DNS (Domain Name System) set up by an alliance of Western companies when the World Wide Web was first developed.

Regulations and directive bills that leads to enhance the development of surveillance in Russia Internet

The Russian government has kept a tight rein on the internet in the country, however, in recent times the Russian government has pugnaciously tried to isolate the RuNet (Russian Internet) from the world wide web- by applying domestic internet law which was signed in May 1, 2019. The same has been put in effect on November 1, 2019[13]; this may impact free speech rights in Russia. If these laws are carried out to in full potential in Russia it may weaken the Russian people to exercise their human rights including freedom of access to information and expression[14]. So-called RuNet i.e. internet isolation in dictatorial countries can also be a national security risk to other countries in the world. Not to mention, the state controlling the internet can also permit the autocratic to federate power. The government in the internet-controlled state may censor the right information and promote only its agenda and campaigns.

The new RuNet developments in internet isolation present a unique security threat in contrast to other cyber hegemony measures, and the Russian establishment is implementing the World Wide Web isolation on a deeper level than any other authoritarian countries have followed to

---

[11] Executive Order approving Basic Principles of State Policy on International Information Security," Russian establishment.ru, April 12, 2021, http://en.Russian establishment.ru/acts/ news/65350.

[12] Executive Order approving Basic Principles of State Policy on International Information Security," Russian establishment.ru, April 12, 2021, http://en.Russian establishment.ru/acts/ news/65350.

[13] M Ristolainen, "Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West," Journal of Information Warfare 16, no. 4 (2017): 113-131

[14] JULIEN NOCETTI, Contest, and conquest: Russia and global internet governance, *International Affairs*, Volume 91, Issue 1, January 2015, Pages 111–130

date. The Russian establishment[15] Internet threat includes extirpation of Western software and hardware from countries' internet architecture and evolution of DNS (Domain Name System).

History of Russia Authorities Controls over Internet

The term “information control” was coined by Ronald Deibert and his team to represent the regulations, policies, practices, and techniques that forcibly impact the availability of computerized information for political, ethical, and social ends[16]. Additionally, information control also includes meanings like filtering, surveillance, electronic means of denial, and regulations like content removal, defamation laws, and media licensing. There are three broad categories for information control for freedom of the Net Index i.e. Violations of user rights (Karlekar & Cook, 2009), Barriers to Access, and Limits to Content. As compared to other authoritarian countries like China, Russia seldom uses Barriers to Access and pay heed to censorship. However, Russia is planning to isolate RuNet from the World Wide Web in case of crisis without describing what crisis calls for isolation. Plus, Russia doesn’t specify its RuNet isolation beyond some modish allusions to the internet shutdowns – no connection with a global network. Besides this, in countries like Egypt and Iran, specific applications like Twitter, Whatsapp, and VOIP are monitored during protests and elections[17]. Historically, the principal mechanisms for information control in Russia are based on censorship and violations of user rights. In 2015 Katherine Ognyanova discovered three primary mechanisms which are employed by the Russian government to exercise information control over media: state control over mainstream media (specifically broadcast), censorship and resulting chilling effects, and the selective applications of unrelated laws[18]. To add, like in most countries in Russia also the physical arrangement of the internet is owned, maintained, and built by the private sector. There are companies like ISPs (Internet Service Providers), search engines, SNS (Social networking sites), and blogging sites which in reality practice private jurisdiction over online activities[19]. This de facto privatization can come into dispute with the

---

[15] Polina Kolozaridi and Dmitry Muravyov, “Contextualizing sovereignty: A critical review of competing explanations of the Internet governance in the (so-called) Russian case,” First Monday 26, no. 5 (May 2021).

[16] Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: understanding Russian Internet policy. Media and Communication, 5(1), 29-41. https://doi.org/10.17645/mac.v5i1.808

[17] DeNardis, L. (2014). The global war for internet governance. New Haven, CT: Yale University Press.

[18] Ognyanova, Katherine & Ball-Rokeach, Sandra. (2015). Political Efficacy on the Internet: A Media System Dependency Approach. 10.1108/S2050-206020150000009001.

[19] MacKinnon, R. (2011). China’s “networked authoritarianism”. Journal of Democracy, 22(2), 32–46.

new law of the country. As there are no potent laws in the country the government can exercise its power to force, push, and even modify information from telecommunication companies. According to Laura DeNardis[20], "state control of internet governance functions via private intermediaries has equipped states with new forms of sometimes unaccountable and nontransparent power over information flows".

In Russia, domestic surveillance foregoes the internet as with censorship. The ongoing surveillance ritual is historically grounded in Russia's Soviet past. The Soviet intelligence agency KGB, now renamed as FSB[21] (Federal'naya sluzhba bezopasnosti, or Federal Security Service) have still had a strong influence. In 1995, SORM (The System of Operational-investigatory Measures) was implemented compelling all the telecommunication providers in the country to utilize only FSB offered hardware permitting the agency to keep an eye on user's content as well as metadata which includes phone calls, internet-based activities, and email-traffic in spite of low internet usage at that time. In addition to this, SORM has been implemented on social networking sites also, a key area of issues with the Russian government. The techniques and tools used to monitor the social site by Russian authorities had some major flaws as stated by Soldatov and Borogan[22].

The Yarovaya laws in 2016 have increased the Russian authority's surveillance powers by amplifying the imperative data retention duration to six months for user's content and metadata retention for three years and in all text applications a mandatory cryptographic[23] backdoors. Also, the "color revolution" in countries likes Georgia, Kyrgyzstan, and Ukraine was alarming for the Russian government, "a narrative of a continuous wave of pro-democracy, pro-reform movements sweeping through the former Soviet Union[24]". Besides this, the Russo-Georgian war in the year 2008[25] raised a huge concern for the Russian

---

[20] DeNardis, L. (2014). The global war for internet governance. New Haven, CT: Yale University Press.

[21] Soldatov, A., & Borogan, I. (2012). The Russian establishment's new internet surveillance plan goes live today. Wired. Retrieved from https://www.wired.com/2012/11/ russia-surveillance

[22] Soldatov, A., & Borogan, I. (2013). Russia's surveillance state. World Policy Journal. Retrieved from http://www.worldpolicy.org/journal/fall2013/Russia -surveillance

[23] Lokshina, T. (2016, July 7). Draconian law rammed through Russian parliament: Outrageous provisions to curb speech, privacy, freedom of conscience. Human Rights Watch. Retrieved from https://www.hrw. org/news/2016/06/23/draconian-law-rammed-through-russian-parliament

[24] Katherine T. Hinkle, Russia's reactions to the color revolutions (Monterey: Naval Postgraduate School, 2017),

[25] Soldatov and Borogan, The Red Web, 110

establishment that the way journalists, as well as individuals, could make use of the World Wide Web to circulate information. The Arab Spring in 2011[26], the freedom of speech on the internet and clandestine views of western online interference were doubled during that period. In 2011 during Putin's[27] election the protest against him was rigging, online criticism was surging for Putin's return to the presidency, the Ukrainian revolution[28], 2013 the Snowden leaks [29] , and 2016 the Panama paper leaks[30] . As the events open out the Putin's government and his Russian establishment counselors become vociferous about the internet risk in their country. Not to mention, in 2014 the Russian president Putin tagged global network aka internet as "CIA project" in St. Petersburg media forum and demand Russian people to "fight for its interests"[31]. Furthermore, the Russian authorities exhibited concern about how Russia's young generation will use the internet and these young people are less persuadable to Russian establishment television advertisement[32]. Thus the Russian government had executed the domestic internet bill along with blocking other countries (especially USA) news websites[33] along with mandating storing local Russian citizen's data with the Russian borders[34]. After Putin's return to the presidency in 2012 the bill

---

[26] See, e.g.: Yulia Nikitina, "The 'Color Revolutions' and 'Arab Spring' in Russian Official Discourse," Connections 14, no. 1 (Winter 2014): 87-104, https://www.jstor. org/stable/26326387, 88; and Soldatov and Borogan, The Red Web, 124, 125, 146.

[27] See, e.g.: Yulia Nikitina, "The 'Color Revolutions' and 'Arab Spring' in Russian Official Discourse," Connections 14, no. 1 (Winter 2014): 87-104, https://www.jstor. org/stable/26326387, 88; and Soldatov and Borogan, The Red Web, 124, 125, 146.

[28] In December 2013, Putin was already blaming "outside actors" for protests in Ukraine. "Ukraine PM Mykola Azarov warns of coup in making," BBC, December 2, 2013, https://www.bbc.com/news/world-europe-25192792.

[29] Putin used the Snowden leaks to criticize the United States, but it also played into his existing worldview of US technologies and, in particular, US social media platforms as tools of Western subversion. See some of Putin's public comments: "Putin says Snowden was wrong to leak secrets but is no traitor," Reuters, June 2, 2017, https://www.reuters.com/article/us-russia-putin-snowden/putin-says-snowden-was-wrong-to-leak-secrets-but-is-no-traitor-idUSKBN18T1T4

[30] Putin called the publication of the Panama Papers a "provocation" and blamed US officials and Goldman Sachs for an attempt to influence Russian elections. "Russia's Putin: Panama papers are a 'provocation'," Reuters, April 14, 2016, https://www.reuters.com/article/us-russia-putin-panamapapers-idUSKCN0XB16D

[31] Noah Rayman, "Putin: The Internet Is a 'CIA Project,'" TIME, April 24, 2014, https://time.com/75484/putin-the-internet-is-a-cia-project/.

[32] Noah Rayman, "Putin: The Internet Is a 'CIA Project,'" TIME, April 24, 2014, https://time.com/75484/putin-the-internet-is-a-cia-project/.

[33] Nathalie Maréchal, "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy," Media and Communications 5, no. 1 (2017): 29-41, https://www.cogitatiopress.com/mediaandcommunication/article/view/808/808, 32.

[34] Nathalie Maréchal, "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy," Media and Communications 5, no. 1 (2017): 29-41, https://www.cogitatiopress.com/mediaandcommunication/article/view/808/808, 32.

implementation was hasten up, laws to limit as well as supervise individuals online behavior were widening with facts and tactics of dictatorial power merger from physical enforcement to state ownership of resources available on the internet[35]. To add, the Russian Internet policy is made in context with western countries (especially USA) that uses the internet to bring down the government in "countries where the opposition is too weak to mobilize protests"[36]. That said the freedom of speech and digital rights are extra threatening to Putin's government and its Russian establishment counsellors.

The looming conflict between Putin's rule and the open-minded democracies of North America and Europe appears to abyss two disputing paradigms about the role of data and information circulated via the internet in society[37]. The study has covered the approach by the Russian establishment to control the flow of information, domestic surveillance, and the historical approach of Russia in information control, and the amendment to the law of personal data.

What Content Is Censored by the Russian Government?

The majority of censorship in Russia is aimed at suppressing resistance to the existing administration. Even acts against LGBTQ people and pornographic material are used to strengthen Russia's patriotic and conservative narrative.

Censorship in Russia is often focused on:

- Political dissent is being silenced.
- Prohibition of LGBTQ material.
- Influencing public opinion on the Crimean invasion.
- Interfering with the usage of communication software.
- Punishing satire aimed against religious groups or individuals.

---

[35] coercion

[36] Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. International Affairs, 91(1), 111–130

[37] Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30(1), 75–89. doi:10.1057/jit.2015.5

Opposition in politics

The Russian communications regulator, Roskomnadzor, restricted entry to several website. This move was to urge Russian people to get rid of the vote ahead of Russia's parliamentary elections to be held 2016. In Russia, the Russian establishment also continues to suppress information on any type of political dissent.

Roskomnadzor[38] mainly depends on Federal Law No. 398, often known as "Lugovoy's Law," to prohibit access to these sites. This legislation empowers the Prosecutor General's Office to prohibit entry to websites for "extremism" with no monitoring. The ambiguity of Lugovoy's Law allows for the prohibition of opposing political material for vaguely defined offences such as "inciting unlawful behaviour" or "promoting strife."

LGBTQ(Lesbian Gay Bisexual Transgender Queer)

The Russian Parliament proposed a law in the year 2017. It was a step that led to amending the child protection law of Russia. Here, it meant to include a provision prohibiting "the propagation of non-traditional sexual relations among children."

The new legislation change has given the government broad authority to suppress LGBTQ information. Because of these new powers, they were able to ban many organisations that supported homosexual people in Russia. A potrait of President Putin with exaggerated makeup on a government list of prohibited extremist content, because the image implied that

[38] For the Russian government, Roskomnadzor, or the Federal Service for the Supervision of Communications, Information Technology and Mass Media, is in charge of censoring and monitoring Russian media.

Putin had a "non-traditional sexual orientation." In principle, these photographs, marches, and websites are all prohibited since they may be seen by kids, which is a violation of the law.

Ukraine and the Crimean Peninsula

The Russian Federation acquired the Crimean peninsula from Ukraine in 2014. Since the acquisition the federation has been working hard to prevent access to the information of Russia and Ukraine that portrays the invasion as something apart from being authorised.

There was no access to the news websites of Ukraine. Some famous names include Korrespondent, Liga etc.They were restricted because they quoted Refat Chubarov, the head of the Crimean Tatar movement and a vocal opponent of Russia's annexation.

Telegram

The government of Russia tried to put a ban on the telegram application in April 2017. This was after it refused to provide the authorities a backdoor into its users' communications. Throughout 2017, Telegram was extensively used to assist in arranging a series of large-scale anti-government rallies.

Despite widespread condemnation from the international community, major corporations, etc. Roskomnadzor did maintain the ban. This is in addition to increasing the amount of time it spends targeting political and human rights activists and companies who do not agree with its choice to block content.

Zello

The Russian authorities prohibited access to this application which enables cell phones to be made use of as walkie-talkies. This ban was put in April, 2017.

This app was used by the truck drivers in Russia to plan anti-government rallies and strike activities over a contentious road-tax scheme just before it was banned.

Organizations of faith

There are two major conservative religious organisations in Russia namely - The Russian Orthodox Church and Islam's Sunni branch. Both of them forbid offending the religious sensitivities of those who adhere to a religious belief system.

The authorities of Russia continue to put a ban on the data that they find objectionable to certain religious groups.

Methods adopted by the Russian government to impose censorship on the internet

The Russian government, like many oppressive regimes, employs a variety of tactics to filter the internet. The Russian government's censorship strategies are constantly evolving, from attempting to impose an internet belonging to the government. This would further lead to prohibiting permission to VPN websites along with partnering with ISPs. These are some examples:

- Investing in telecoms providers
- Developing a sort of internet that belongs to the government
- VPNs are not permitted to be used.
- Putting regulations in place to assist government agencies in censoring internet information.

Government-owned telecoms

Rostelecom, Russia's state-owned telecommunications provider, controls over half of the country's broadband internet market, which is growing at a rate of 7 percent per year. The Russian establishment[39] can assure that the largest supplier of internet access complies with all of its censorship criteria by controlling a considerable piece of the Russian broadband market.

ISPs all throughout the world collaborate with governments to influence how people use the internet. In Western Europe and North America, for example, ISPs may limit connections used to download torrent files. That is impressive; imagine what they will be capable of under the control of a politically conservative government.

State-owned internet

Vladimir Putin, the President of the Russian Federation, said in 2014 that he wished to establish a Russian-built internet, comparable to the state-controlled internet of China and Iran.

During 2017, the Russian Security Council directed Roskomnadzor to investigate a system of backup internet servers that would be located inside Russia and its allies and would be used solely by them. They developed this approach to counter the "dominance of the United States and certain European Union nations in areas of internet management."

Putin passed legislation to establish an autonomous Russian internet on May 1, 2019, but it has remained in legal limbo since.

Restrictions on the use of virtual private networks (VPNs) and anonymity

[39] The Russian establishment is the executive branch of Russia's or the Soviet Union's government, particularly in matters of foreign policy. Moscow's citadel, which houses the Russian government's and, previously, the Soviet government's main offices.

The Russian Parliament approved a bill in 2017. It mandated ISPs to ban access to VPN providers' platforms and website proxies, which are frequently put to use to get entry into prohibited information and avoid government monitoring.

Another new regulation that was approved during this time compels people with applications like WhatsApp to make a registration with their contact details, enabling their online conversations to be connected to their actual identities and helping in online government monitoring measures.

Regulation

Multiple government agencies in Russia have the unilateral authority to prohibit any call for unannounced public activities or rallies, as well as any LGBTQ material that is "propagandising non-traditional sexual relations among minors."

Localization of data

"Yarovaya Law" mandates Russian Internet service providers and distributors of communication channels or apps to retain all the data of users relating to communication for a maximum of three years. Russian data localization and retention requirements are growing more stringent, making it more difficult for social and human rights advocates, as well as anti-government protests, to use apps like Telegram, which they rely on for communicating.

New anti-terror law, enacted in late 2017, significantly enhances the state's surveillance powers over internet communication, including compelling sites that enable encrypted communication to supply the government with their decryption keys.

New anti-terror law, enacted in late 2017, significantly enhances the state's surveillance powers over internet communication, including compelling sites that enable encrypted communication to supply the government with their decryption keys.

Internet Service Provider Financing (ISPs)

As soon as Roskomnadzor discovers unlawful material, it instructs the hosting provider to put an end to a warning to the website that is in question. If the unlawful material is not deleted, the page is added to the government blacklist, and all Russian ISPs are required to block it within 24 hours. ISPs who fail to block websites on the government's blacklist fear massive penalties and the loss of their operating license.

Conclusion

The development of surveillance in Russia is concentrated on basically identifying the data and information over the internet which is not in synchrony with the views of the Russian establishment. After identification the next step is censorship for which the Russian state uses different means, tools and techniques depending on the nature of data and its publisher. Throughout the history and even during the present times the Russian state has continuously tried to regulate the data and information in such a manner that it remains plausibly deniable.

Chapter 3: Tools of surveillance:process and functioning of SORM

In the contemporary world, the political landscape between democracies and autocracies is being reshaped by the use of digital information technology by authoritarian governments to monitor, suppress, and control domestic and international people. China and Russia have been at the vanguard of this tendency, developing and exporting different technology-driven frameworks for authoritarian governance.

Governments throughout the world are proactively monitoring Internet activity. The Russian government legally intercepts different IT and telecommunications systems via the use of the SORM (Russia's System for Operative Investigative Activities). When the first SORM version was released in 1995, it enabled the FSB to monitor phone conversations and Internet activity even though the Internet was still in its infancy and had limited reach and capability[40]

Russia employs a restrictive legal system. Furthermore, Russia works on the repression of fundamental companies and civil society, a low-cost autonomous model that can be easily transferred to most countries. Moscow's low-cost digital misinformation tactics have effectively stifled domestic opposition and weakened democratic institutions overseas. The Russian government has recently taken legal and technical steps to tighten control, including a law passed in the calendar year 2019 to create a "sovereign Russian internet."[41]

Information systems, telecommunications networks, and systems and networks for the control of technical processes utilised in state defence, healthcare, transportation, communication, energy, fuel, nuclear and aerospace sectors are considered to be important information infrastructure components. All of these sectors must be secured against cyber threats since they are essential to the economy. The Federal Service for Technical and Export Control, which will be in charge of oversight in this area, requires the adoption of protection measures, assignment of the protection category (by bylaws), and registration. Many

[40] Ermoshina, K., Loveluck, B. and Musiani, F. (2021). A market of black boxes: The political economy of Internet surveillance and censorship in Russia. Journal of Information Technology & Politics, pp.1–16.

[41] Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. Policy Brief, Democracy and Disorder Series (Washington, DC: Brookings, 2019), 1-22.

businesses have raised concerns about this rule, which has been designed in such a wide-ranging manner. According to the legislation, even internal LAN networks may be declared important information infrastructure if they fall within its broad standards. The authorities, on the other hand, argue that this is a misinterpretation. Another factor that obscures the picture is the lack of enforcement activity.[42]

VPN services that do not collaborate with the government, for example, in connection to copyright, data protection, or other legal infringements, were also banned under Russian legislation. Russia approved a new law on this topic on November 1, 2017. The bill's primary focus is on well-known variations like Tor. However, the normal business might be disrupted as well. ' The usage of VPNs by enterprises, however, remains unclear, and this remains an important issue that has to be addressed. If an institution utilises a VPN tool, it must identify the users of the tool eg, which workers may use the tool – such as in an internal IT policy and use it solely for business reasons, according to the exception in the law. This exception, if accurate, might be beneficial to the business sector. The legislation has never been applied in reality by the government, thus there are still doubts.[43]

According to numerous projects, big data regulation is also being addressed, as well as efforts to create a unified code for information law and cybersecurity that would codify the present diverse regulations.

Russia is continuously trying to aggravate the surveillance and censorship of the internet and telecommunication within the country. The flow of information, surveillance, and data censorship has been carried out through various agencies and laws for decades. In the recent past, the amendment to Yarovaya law 374-FZ[44] and 375-FZ has extended law enforcement to monitor private communication data. The Russian government permits the lawful interception of mobile and internet service networks using SORM. The term SORM is used

[42] Ermoshina, K. and Musiani, F. (2018). Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era. Media and Communication, 5(1), p.9.
[43] openDemocracy. (n.d.). Surveillance: Zakharov v Russia and what it means for the Investigatory Powers Bill. [online] Available at: https://www.opendemocracy.net/en/zakharov-v-russia-refresher-on-how-far-europe-has-come/ [Accessed 5 November 2021].
[44] Federal Law of July 6, 2016, No. 374-FZ " On Amendments to the Federal Law" On Countering Terrorism "and certain legislative acts of the Russian Federation in terms of establishing additional measures to counter terrorism and ensuring public safety."

as an abbreviation for "Система оперативно-разыскных мероприятий" or "System for Operative Investigative Activities”.[45]

The advent of SORM took place in 1995 to grant lawful authority to Russia's Federal'naya sluzhba bezopasnosti (FSB) or Federal Security Services, which is responsible for counter-intelligence, counter-terrorism, and surveillance to surveil data for national security. The service providers were mandated to install hardware provided by the FSB. This enabled the FSB to monitor the metadata and content of the various communications between the users. At that time, SORM was used to monitor phone calls, emails, and internet surfing data. [46]With time new inventions and technological advancements in telecommunication and the world wide web gain rise to SORM-2 and SORM-3.

However, with the increase in social networking websites, the Russian State is falling short of controlling the internet traffic with the available infrastructure. The bill passed in 2019 known as the "sovereign internet" requires internet service providers to install state-provided devices that can monitor and censor internet activity. As a result, SORM-3 equipped with deep packet inspection technology is implemented as a defensive approach against external threats.

The tools and technologies used by Russia to control the flow of content over the internet did not limit itself to the Russian State only. These technologies are gaining popularity in other countries, such as Uzbekistan, Kazakhstan. Nevertheless, Russia is exporting its tools to the West as well.[47] The current chapter discusses Russia's surveillance tools that are spreading worldwide like wildfire.

[45] A Comprehensive Overview: 2015 Amendments to the Federal Rules of Civil Procedure. (2015). Kansas Law Review.

[46] Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. Media and Communication, 5(1), 29-41.

[47] Russian-made surveillance technologies used in the west”, Andrei Soldatov, https://www.wired.com/2013/05/russian-surveillance-technologies/

Tools and techniques used by Russia to control the content over the internet

SORM

SORM is the permitted telecommunications monitoring equipment that is legally recognized. All internet service providers (ISPs) in Russia are required by law to install an FSB monitoring device called "Punkt Upravlenia," also known as Omega, on their networks, permitting network traffic collection without the service providers' consent or cooperation.[48] Russian Federal Security Service officers can perform direct surveillance using SORM. SORM is Russia's national automated and remote legal interception infrastructure system. In the mid-1980s, a KGB research institute established SORM's tactical and technical fundamentals. However, the concept was not fully implemented until the early 1990s, when SORM was first placed on analogue signal telephones. In 1992, the Ministry of Communications approved the first SORM-related legislation. Operators were required to allow security services to monitor phone calls and surveil mail[49]. The SORM was introduced in Russia in 1998. To get direct access to data on commercial networks, SORM develops an infrastructure through which law enforcement and intelligence organisations may do so. The SORM phenomenon has given birth to novel configurations of sociotechnical actants, which have had long-term consequences for the market for Internet service providers (ISPs). Three generations of SORM measures have been developed and implemented.[50]

SORM is a decentralized object made up of commutators, switches, servers, and software deployed at the operator's and service provider's expense but directly managed by the FSB via a terminal. The internet service providers (ISPs) must share the data on demand by FSB and seven other agencies, including police departments[51]. SORM comprises two elements. The first is a terminal installed at the office of a regional FSB "curator," which allows direct,

[48] "Here's what Putin didn't tell Snowden about Russia Spying", Mark Memmott, 18 April 2014, https://www.npr.org/sections/thetwo-way/2014/04/18/304530695/heres-what-putin-didnt-tell-snowden-about-russias-spying

[49] "Lawful Interception: the Russian Approach", Privacy International, 04 March 2013, https://privacyinternational.org/blog/1296/lawful-interception-russian-approach

[50] Peers, S. (2015). EU Law Analysis: Zakharov v Russia: Mass Surveillance and the European Court of Human Rights. [online] EU Law Analysis. Available at: http://eulawanalysis.blogspot.com/2015/12/zakharov-v-russia-mass-surveillance-and.html [Accessed 5 Nov. 2021].

[51] Ermoshina, K., Loveluck, B., & Musiani, F. (2021). A market of black boxes: The political economy of Internet surveillance and censorship in Russia. Journal of Information Technology & Politics, 1-16.

remote access to the traffic of all ISPs under his geographical jurisdiction. The second component is the traffic storage system deployed in the premises of ISPs[3]. Fundamentally two modes of information transmission are provided by SORM. One is the transmission of statistical information, and the other is complete information.

These systems were created to perform semantic internet analysis by searching structured computer files or databases. The majority of these systems were designed to function with open sources, and therefore are unable to monitor closed accounts like Facebook and Twitter. The FSB understood early on that the only way to tackle the problem was to use SORM. According to the licensing, companies who rent out server space must provide security services access to their servers via SORM without notifying site owners. The FSB has had minimal issues monitoring closed groups and accounts on Russian social networks like Vkontakte and Odnoklassniki because of SORM. Facebook and Twitter, on the other hand, do not conform with Global Internet Network rules and hence are not covered by the SORM in Russia[2].

Surveillance, Storage Systems, and Monitoring

Since 1998, Russia has implemented three primary forms of infrastructure-based Internet control measures: surveillance, data storage, and filtering.

a) The so-called System of Operative Investigative Measures (SORM) is a set of surveillance measures that allows government agencies like the FSB (the former KGB) access to private telephone and internet communications.

b) Limiting the flow of critical data across national boundaries.

c) Filtering procedures, limiting access to a growing list of websites (blacklist) regarded ex-remits. There is a worldwide trend toward balkanization, which is hyper-localization and nation-state control of data and communication flows. These three levels are intertwined[52].

[52] Peers, S. (2015). EU Law Analysis: Zakharov v Russia: Mass Surveillance and the European Court of Human Rights. [online] EU Law Analysis. Available at: http://eulawanalysis.blogspot.com/2015/12/zakharov-v-russia-mass-surveillance-and.html [Accessed 5 Jan. 2022].

The Russian manufacturer of SORM is MFISoft. Beyond the jurisdiction of Russia, MFISoft works with a partner named "ALOE Systems" based in Canada. The products developed by MFISoft under SORM-1 are SORMovich Voice over internet protocol, also known as SORMovich VoIP, SORM for Broadworks, SORM for RTU, SORM for Nortel, SORM for Ericsson, and many others. Among the various surveillance tools, the most preferred tool by FSB is Omega[5]. The SORMovich VoIP is used for data grabbing. The system provides a high-end system for detecting, monitoring, storing, and analysing data going across the internet.

The chronological developments of SORM are as follows:

- In 1995, SORM-1 was set up to control and monitor telephonic traffic with a vision to strengthen national security and counter-terrorism.
- In 1998, SORM-1 underwent advancements and gave birth to SORM-2. This equipment was responsible for surveillance and monitoring internet browsing information[2].
- In 2012, social networking websites such as Facebook and Twitter started gaining popularity. These sites were becoming critical concerns for Russian authorities. Hence, the scope of SORM-2 was extended to the surveillance of social networking websites.
- In 2014, the last update for SORM was launched. It was known as SORM-3, and the equipment had Deep Packet Inspection (DPI) capability. SORM-3 was capable of monitoring metadata such as date, time, location, and details about the sender and receiver of a particular message. SORM-3 was also equipped to monitor and save multimedia attachments.[53] Online resources and activities that may be vulnerable to targeted monitoring have been expanded in SORM-3. Users' phone numbers, media access control addresses, and email addresses obtained from sites like mail.ru, yandex.ru, rambler.ru, and others are examples, but they are not the only ones. Deep Packet Inspection (DPI) is the data processing protocol used by SORM-3, which

[53] Ferreira, E.G., Freitas, M.S. da R., Pinto, J.A. da R. and Sisquini, G.R. (2019). SORM DG - an efficient SORM based on differential geometry. REM - International Engineering Journal, 72(4), pp.589–600.

extensively examines the content of each piece of data (packet) and reroutes it appropriately.

A court order is often required by the government agency in charge of collecting specified data. However, operatives are not obligated to give this information to a party that has been raided. Refusal to provide information without a court order is pointless. Even if a court order is necessary to take a specific piece of content, metadata (the description and supplementary context of the material in issue) may be acquired without it.

In Zakharov v Russia, the European Court of Human Rights questioned the legality of SORM. Since the Russian state had failed to provide adequate safeguards to eliminate SORM's potential arbitrariness and to arrange for appropriate measures to prevent unwarranted scrutiny, the Court concluded that SORM may violate Article 8 of the European Convention on Human Rights (a right to respect for private and family life).

When compared to international Lawful Interception standards, SORM provides surveillance operators with a tremendous deal of scope. In most Western nations, law enforcement authorities first obtain a warrant from a court and then issue an order for a legal interception to a network operator or Internet service provider (ISP), which is then responsible for intercepting and delivering the information required. Because of the SORM's design, the FSB is not required to communicate with the ISP. SORM is composed of two primary components: the "extractor" the equipment—both software and hardware—that executes data extraction and the "remote control station." FSB's regional office hosts the control station, which allows the extractor to be controlled remotely without the provider's knowledge: the provider will not be aware of what data is intercepted, analysed, and sent since the control station is hosted there. It is not essential to get a court order to activate the metadata interception system. However, to get access to the actual telephone recordings, the Federal Bureau of Investigation must first obtain a court order. According to the official statistics published by the Supreme Court, there were 372,144 orders issued during the calendar year 2012.[54]

[54] Anon, (2018). How Russian Internet Surveillance Operates | Cassandra Voices. [online] Available at: https://cassandravoices.com/law/how-russian-internet-surveillance-operates/ [Accessed 5 Nov. 2021].

The circular buffer for data storage, which is the costliest component of SORM, is the most expensive component. Although the technical requirements for SORM measures have changed with each successive generation of SORM measures, they have remained consistent: whereas providers were required to keep all traffic for 12 hours under SORM-2, providers were required to preserve all metadata for three years under SORM-3. As a result, service providers must replace all of their equipment since the installation of SORM systems is entirely reliant on them.

Along with SORM, Russia implemented the "Safe City" video surveillance system in 2015. The system enables the automatic transmission of data to government authorities, including facial and moving object identification. It was developed by a Russian firm called NTechLabs.

Deep Packet Inspection (DPI) Technology

Deep Packet Inspection (DPI) Technology is a transformational technology that creates unprecedented regulatory possibilities for controlling the flow of content online.[55] It is also known as information extraction or complete packet inspection (CPI). Information in the form of text, image, voice, or anything else is transmitted over the internet as packets, small bundles of data that are individually routed from the sender to the receiver, then put back together in the correct order. Deep packet inspection examines the data and header of a packet as it passes through an inspection point, filtering out any protocol violations, bait, malware, breaches, and other set criteria to prevent the packet from getting through the inspection point.[56]

Deep packet inspection examines a packet's contents as it passes through an inspection point. The user, the Internet service provider, or the network or systems administrator can assign rules for the inspection. In real-time, deep packet inspection determines what to do with these packets. Deep packet inspection can examine the contents of these packets and determine where they originated, such as the service or application that sent them. It can also use filters

[55] DeNardis, L. (2014). The global war for Internet governance. New Haven, CT: Yale University Press
[56] "What is Deep Packet Inspection? How It Works, Use Cases for DPI, and More", Chris Brook, December 5, 2018, https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more

to track down and divert network traffic from a specific IP address or an online service like Twitter or Facebook.

DPI is capable of doing large-scale activities like network packet filtering, which entails identifying network weaknesses and threats. Deep Packet Inspection in the advanced form includes sophisticated network management technologies, data packet mining, and internet censorship and interception.

The payload and header portions of internet information are separated by DPI. Unauthorized data packets, such as spam, viruses, and maliciously infected data packets, must be identified and blocked. Additional security elements may be added to DPI to guard against various threats.[57] To avoid DDoS assaults, DPI might use buffer overflows to prevent bogus IP addresses. Most firewalls, it is used to prevent the propagation of viruses and malware over the network. When it comes to intrusion detection and prevention, it's a lifesaver.

How DPI is employed?

Firewalls employ DPI for deep-level certification checks to monitor large-scale traffic and its real-time flow. To meet the most stringent privacy standards, DPI may even undertake secret header and payload inspections.

To identify and validate each data packet, it may automatically produce the address from where they are generated, as well as their IP address. Google, Facebook, and Twitter recognise and reroute all network traffic that originates from IP addresses that have not yet been assigned to a specific domain name.[58]

The ISP may be contacted by any network administrator to find out what each user is doing and to maintain track of their real-time activity for security reasons.

The following are some possible applications:

[57] Fortinet. (n.d.). What Is Deep Packet Inspection (DPI)? [online] Available at: https://www.fortinet.com/resources/cyberglossary/dpi-deep-packet-inspection [Accessed 5 Jan. 2022].
[58] dgap.org. (2021). Deciphering Russia's "Sovereign Internet Law" | DGAP. [online] Available at: https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law [Accessed 28 Nov. 2021].

1. Optimisation of content – It is possible to compress media and documents in case of low network bandwidth to guarantee appropriate and efficient performance using DPI's compression capabilities.
2. Load Distribution – Network servers constantly monitor and distribute data packets to ensure that all servers on the Internet have an equal amount of load.
3. Analysis of User Behaviour – Users' surfing habits is constantly monitored to ensure that all online activity is under control.
4. Personalized Marketing -A user's browsing history may be used to target advertising that is relevant to the user's interests.
5. Enforcement of copyright – Content that may be a copy of the original is removed from the platform as a result of unlawful access to such files, which breaks copyright regulations.[59]
6. Regulations on content- As part of network censorship regulations, it is used to detect, authenticate, and remove access to potentially damaging actions on the network.

Network administrators employ deep packet inspection to enable network traffic flow more smoothly. Deep packet inspection can be used to allow high-priority information to pass through ahead of lower-priority communications in the case of a national emergency. ISPs can also use DPI to improve their ability to prevent IoT devices from being exploited in malicious attacks by preventing harmful requests from devices. Deep packet inspection can also be used for objectives like monitoring and censorship. The Russian government employs SORM-3, equipped with deep packet inspection, to monitor the country's network traffic and restrict certain content and websites harmful to the national interests. Pornography, religious information, political opposition dissents, and even significant websites like Wikipedia, Google, and Facebook have been blocked due to deep packet inspection technology.

[59] Joshi, A., Narayanan, S.N. and Mittal, S. (n.d.). Russians hack home internet connections – here's how to protect yourself. [online] The Conversation. Available at: https://theconversation.com/russians-hack-home-internet-connections-heres-how-to-protect-yourself-95907 [Accessed 5 Jan. 2022].

DPI: What are the issues?

Denial of service attacks, buffer overflow attacks, and even various sorts of system assaults may result from deep packet inspection. By increasing the complexity of the network security settings and the firewall rulesets, deep packet inspection slows down data transfer rates and harms PC performance. Rather than completing the user-specified task as quickly as possible, deep packet inspection uses all of your system resources to hunt down data packets passing over your network.[60]

However, there is an issue with encapsulation in DPI technology. To explain the concept of encapsulation in layman terms, consider a computer with two cables such that one goes into the computer, the other goes out. This computer must examine each incoming packet, that is, a block of data, and decide on it: to pass or not to pass. If the data block matches the prohibited pattern, it is not permitted. However, when encapsulation of the data packet occurs, one data packet is inserted into another. And a packet with suspicious data can be easily encapsulated in a packet with other data, not prohibited. In this way, a targeted data packet can escape surveillance. The messaging app "Telegram" used this encapsulation to dodge the data scrutiny using VPNs.

The connection between DPI and data loss prevention?

A technique known as Deep Packet Inspection (DPI) is an extraction method that allows us to remove malware that isn't needed, hence reducing network congestion. Rather than relying on the user to provide authorization for data to be sent and received over a network, it employs its own set of screening and blocking policies. Payload and header information is stored in the data packet, which is referred to as a "packet".[61] In addition, it has certain powerful algorithms that may even analyse the secret data that may be delivered unintentionally as spam activity.

[60] Novel imaging technique: DPI and 3-D-DPI versus CFI in liver disease. (1995). Gastroenterology, 108(4), p.A1070.
[61] Anon, (n.d.). What is Deep Packet Inspection? How it Works and Why It Is Important | Endpoint Protector. [online] Available at: https://www.endpointprotector.com/blog/what-is-deep-packet-inspection-how-it-works-and-why-it-is-important/ [Accessed 18 Nov. 2021].

Role of SORM in monitoring the dissent for the Russian government over the internet

President Vladimir Putin wields much power in Russia's authoritarian political system. The Russian establishment can rig elections and repress genuine dissent with the help of loyal security forces, a subordinate judiciary, a tightly controlled media environment, and a legislature made up of a ruling party and docile opposition parties.

SORM is frequently used against political opponents and human rights campaigns to monitor and collect information about them. The FSB's power to monitor political opponents, even if they haven't done anything wrong, has been supported by Russian courts[4]. Surveillance by SORM poses no threat to Internet users. Still, it poses a significant threat to bloggers who write about socio-political problems and users who actively stimulate discussion on social media about those matters.

In May 2019, according to RosKomSvoboda, the government was found to be seeking bids for a social media and news media monitoring service that will do "sentiment polarity" of messages on platforms such as Facebook, Telegram, Twitter, and VKontakte. This step was probably taken to see if the users approve or disapprove of the government's viewpoints[62]. It was discovered that government-backed organizations allegedly carried out coordinated attacks on digital media. For example, ahead of massive protests in late January 2021, numerous social media accounts on dissent sites were subjected to massive bot attacks, which rendered them inoperable for a time.[63]

The Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) increased its arsenal for censoring social media with the help of the centralized installation of Deep Packet Inspection (DPI) technology on internet service providers under the 2019 Sovereign Internet Law in Russia. Roskomnadzor, in March 2021, had warned Twitter over persistent non-compliance with content removal demands. In retaliation to the non-compliance, Roskomnadzor limited Twitter's internet loading speeds which had a relatively modest user base in Russia. Through this action, the regulator

[62] "Russia issues new state contract to monitor and categorize social media and news reports", 07 May 2019, https://meduza.io/en/news/2019/05/07/russia-issues-new-state-contract-to-monitor-and-categorize-social-media-and-news-reports, Accessed 17 December 2021.
[63] "Rush at the troll factory", Meduza, 20 January 2021, https://meduza.io/feature/2021/01/20/na-fabrike-trolley-avral, Accessed 17 December 2021.

conveyed a signal to the larger companies, such as Facebook and YouTube[64]. However, this bold action of Roskomnadzor proved technologically inadequate. To throttle Twitter, Roskomnadzor limited all the websites ending with t.co. This caused unwanted shutdown of websites such as Reddit and Microsoft as well. Ultimately, the atrocious actions of the agency revealed the flaws and shortcomings of the DPI technology.[65]

In another case, when people agitated for Navalny's justice, the supporters had to pay a high price for their protest. Navalny's supporters announced a large-scale rally against his criminal prosecution in March 2021. Russians who intended to participate were invited to register on a specific website, Free.navalny.com, to make a preliminary estimate of the number of demonstrators. The database of registered users, on the other hand, was quickly hacked. Registered customers began receiving emails containing their personal information from unknown accounts in April 2021. The attackers may have matched the hacked database's email addresses with other personal information available on Russia's black market. As a result, some of the users' employers dismissed them.[66]

The narrative against the Russian State

Since Vladimir Putin's re-election to the president in May 2012, Russian authorities have been asserting "legal urgency" to tighten their grip over the internet and other digital communications. The Russian establishment is more concerned than ever with the legitimacy of the state, and any attempts to undermine it are relentlessly rejected. After being translated into the digital arena, this "vision" manifests itself as rhetoric that places the internet at the top of a list of risks that the government must address via an avalanche of laws aimed at eventually cutting Russia off from the global infrastructure.[67] Against the backdrop of an international situation in which internet governance is at a crossroads and big internet businesses are coming under increased regulatory pressure from governments, SORM, the technological system utilised by multiple law enforcement organisations to intercept and

[64] "Throttling Twitter traffic in Russia Here's how Moscow's regulators are doing it and why it's not working," Meduza, March 12,2021 ,https://meduza.io/en/cards/throttling-twitter-traffic-in-russia,Accessed 17 December 2021.
[65] Vittoria Elliott, "How the Russian government accidentally blocked its own websites," Rest of World, March 2021.
[66] "We got to the subway", Opposition in Russia, 14 May 2021, https://www.kommersant.ru/doc/4814830
[67] Malyshkin, A.V. (2019). Specialized Courts in the Context of the Differentiation and Integration of Court Jurisdictions. Vestnik Tomskogo gosudarstvennogo universiteta, (446), pp.240–246.

analyse the contents of telecommunications inside Russia, has now been expanded to include surveillance of the internet.

The Internet Freedom index is based on three categories: obstacles to access, limited content, and violation of user rights. The scoring is done on a scale of 0 to 100. Zero indicates the country with the least net freedom, and a hundred implies the most internet freedom. In 2021, Russia's Global freedom score stood at 20, and the internet freedom score was 30[68]. This portrays that Russia is not a free state regarding internet freedom. Russia does not permit anonymous as well as encryption tools. Due to this, the most significant affected criterion is the violation of user rights. Russia scores merely eight out of forty in 2021 for breach of user rights. This implies that people's fundamental rights are under serious threat in Russia.

Although the constitution protects freedom of expression[69], it is subject to a slew of legislative constraints and is frequently disregarded. The constitution expressly prohibits censorship. There are no statutory laws that safeguard internet freedom. Unless their websites are registered as mass media outlets, online reporters do not have the same privileges as traditional media, such as getting permission at official events. However, media outlets have extra responsibilities, such as refraining from using hateful language. If they receive support from outside sources, both publications and individual reporters can be labelled as foreign agents.[70] Russia is a part of the Council of Europe and a party to the European Convention on Human Rights. However, the Russian judiciary is not autonomous. The European Convention on Human Rights works towards safeguarding the people's freedom of speech. But in reality, Russia is found to have violated Human Rights through its restrictive legislation. Since the courts have been found to side with the government in Human Rights matters frequently. The court has often refused to implement constitutional and international treaty provisions that protect Human Rights[14].

Apart from Human Rights violations, the users in Russia are subject to criminal and civil prosecution for various online activities, which are considered unlawful by the government

[68] "Freedom on the Net 2021: Russia", Freedom House, https://freedomhouse.org/country/russia/freedom-net/2021
[69] "Constitution of the Russian Federation," Constitution, Law, and Statutes: Government of the Russian Federation, Accessed June 16, 2021, http://archive.government.ru/eng/gov/base/54.html
[70] "Peter Tolstoy: The law on foreign agents is dust from ants" [in Russian], RosKomSvoboda, January 12, 2019, https://roskomsvoboda.org/35097/

agencies. If a criminal prosecution is filed against someone for "extremist" movements carried out online, the person's details are added to a denylist of the Federal Financial Monitoring Service (RosFinMonitoring). Even if acquitted, those on this list are barred from certain professions, and their bank accounts may be blocked[71].

In the case of surveillance by SORM, though all communication operators must install the equipment, the appropriate agency must first get a court warrant to use the system legally. In some situations, however, authorized state organizations can carry out the interception and merely notify the court within a day. This is permissible if there is a suspicion of severe or grave offences or risk of activities endangering Russia's State, military, economic, information, or environmental security. However, within four days from the start of the action, the authorities must get a warrant. Russian law does not mandate the warrant as an adequate requirement to monitor the information of any person.

Because of this, SORM impacts not only Russians but also those people who travel to Russia. Connecting to a Russian Wi-Fi network may expose a traveller to surveillance. SORM as a surveillance tool is not a concern. The fact that operators are not authorized to see the warrant is the primary source of concern. This means that the operator has no way of knowing if the decision is legal or if each case has a warrant. The operator has no scope in finding out whether the system is being misused or not.

Case of Roman Zakharov v. Russia[72]

On October 20, 2006, a Russian national, Mr Roman Andreyevich Zakharov, filed a complaint against the Russian Federation with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms. The petitioner claimed that the Russian system of undercover monitoring of mobile phone communications infringed his right to privacy and correspondence and that he lacked a sufficient remedy in this regard. As a publisher and the head of an NGO promoting media freedom and journalists' rights, Zakharov challenged the Russian system for allowing monitoring for crime prevention and

[71] Svetlana Prokopyeva, “Pskov journalist Svetlana Prokopyeva was included in the list of extremists and terrorists” [in Russian], MediaZona, July 4, 2019, https://zona.media/news/2019/07/04/prokopieva-spisok
[72] "CASE OF ROMAN ZAKHAROV v. RUSSIA (Application no. 47143/06)". HUDOC – European Court of Human Rights. Retrieved 2021-12-17.

national security. Order No. 70 mandated the installation of equipment that allowed the Russian Federal Security Service to intercept all telephone calls without previous court authorization, which Zakharov said infringed on his privacy.[73]

This allowed for complete surveillance of all mobile phone conversations. At the national level, there have been no successful challenges to ensuring that only authorised people have access to communications. The European Court of Human Rights heard the case. The laws about surveillance, he contended, violated his Article 8 right to privacy, that some sections of the legislation were inaccessible, and that there were no effective remedies available to him (thus also infringing Art. 13 ECHR).[74]

The Judgment

To begin with, it was necessary to determine whether the case was acceptable. Courts rarely decide on matters in the abstract, but rather on the application of rules in a specific case. As a result, it is more difficult to argue against a system's existence than against its usage. Since its inception, the Supreme Court has acknowledged that covert surveillance might have unique characteristics that warrant a separate legal approach. As a result, there were two conflicting lines of case law: one supported the government's position and required the applicant to demonstrate a high probability that security services had intercepted their communication, while the other supported the applicant's position by arguing that a secret surveillance system's threat was sufficient.

Surveillance is employed to address particular risks, and the Court pointed out that there is a lengthy history of precedent about this. According to the Supreme Court's previous decision in Kennedy, 'threats to national security may vary in type and may be unexpected or impossible to characterise in advance'.[75]

---

[73] Fisher, D., Maimon, D. and Berenblum, T. (2021). Examining the crime prevention claims of crime prevention through environmental design on system-trespassing behaviors: a randomized experiment. Security Journal.
[74] Galperin, D.O. and E. (2016). Russia Asks For The Impossible With Its New Surveillance Laws. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws [Accessed 10 Dec. 2021].
[75] https://Secure.gravatar.com/Avatar/?s=32, img A., #038;d=mm, Srcset='https://Secure.gravatar.com/Avatar/?s=64, 038;r=g', #038;d=mm and says, 038;r=g 2x' class='avatar avatar-32 photo avatar-default' height='32' width='32' loading='lazy'/> X. contribuye a la C. de los D. y D.D. para C. (2015). Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's Schrems judgment. [online] Strasbourg Observers. Available at:

Despite the lower-than-normal level of accuracy demanded by national law, the possibility of misuse and arbitrariness is obvious, hence the extent and method of exercising any discretion must be specified by legislation to prevent abuse. It would be detrimental to the rule of law to represent a presidential discretion in the realm of national security as an unconstrained authority, it added. In this case, the Court emphasised the need for previous court authorization. Examples of minimum protections were provided by the Court, including:

- To get an intercepting order, it is necessary to determine the type of the offences that may lead to such an order, as well as the categories of persons who may be subject to such an order, as well as the length of time that such an order may be in effect.
- No monitoring system could identify illegal interceptions since the secret services' equipment did not preserve records of intercepted communications and did not have direct access to them.

As a result, Russia's emergency interception method does not offer enough protection against exploitation. This was followed by an examination of whether the intervention was essential in a democratic society, which highlighted the conflict between protecting society and its repercussions[76]. The Court made it clear that it must be certain that safeguards against misuse are in place.

As long as surveillance is secret and consequently unknown, it is critical to have monitoring procedures in place to defend the rights of those who aren't able to speak out for themselves. As a general rule, the court prefers to provide a judge with supervisory authority over proceedings. It is necessary for those who have been impacted by surveillance to be told about it or have the ability to launch a legal challenge based on a reasonable belief that monitoring has occurred.

---

https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/ [Accessed 5 Jan. 2022].

[76] https://Secure.gravatar.com/Avatar/?s=32, img A., #038;d=mm, Srcset='https://Secure.gravatar.com/Avatar/?s=64, 038;r=g', #038;d=mm and says, 038;r=g 2x' class='avatar avatar-32 photo avatar-default' height='32' width='32' loading='lazy'/> X. contribuye a la C. de los D. y D.D. para C. (2015). Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's Schrems judgment. [online] Strasbourg Observers. Available at: https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/ [Accessed 5 Jan. 2022].

There is a lack of clarity in Russian law when it comes to the kind of persons who may have their phones tapped, in part because witnesses and suspects are seen as interchangeable terms and because the security services have a great deal of latitude. Security services are exempt from the laws governing the cessation of monitoring.[77] Provisions for data storage and deletion enable the preservation of data that is irrelevant, and it is unclear what happens to the material in the case of persons accused of a criminal offence after the trial has concluded.

Notably, the domestic courts do not check to see whether there is a legitimate suspicion against the individual whose communications the security services have asked for interception to be allowed. It's also not clear if the interception is required or justifiable; in reality, it seems that the courts regard a simple reference to national security as adequate.

Furthermore, the authorization does not identify the numbers to be intercepted, therefore authorizations have been obtained without mentioning this information. The Russian system is especially vulnerable to misuse since it permits direct access without the need for authorization from law enforcement or security agencies.[78] The Court of Appeals ruled that the oversight bodies lacked enough independence. Because only those who can confirm interception may use these medicines, their efficacy is weakened.

The court on this matter declared that current Russian laws governing communications interceptions do not provide adequate guarantees against unfairness and the risk of abuse inherent in any secret surveillance system. Such arbitrary chances are exceptionally high in a system where the confidential services and police have direct access to all mobile-telephone communications via technical means. The situations under which public agencies are authorized to use secret surveillance methods, in particular, are not well defined. Discontinuation of private surveillance measures provisions is insufficient to protect against arbitrary intrusion.

---

[77] data.guardint.org. (n.d.). Zakharov v Russia • Page 7 • Surveillance Oversight Database. [online] Available at: https://data.guardint.org/en/entity/hzbmni4o7ie?file=1601043095114mzz103jbfts.pdf&searchTerm=opportun&page=7 [Accessed 5 Jan. 2022].

[78]https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/

The Court further added that domestic legislation allows for the automated preservation of manifestly irrelevant data and leaves the conditions surrounding the storage and destruction of intercept information after a trial unclear. According to the permission procedures, secret monitoring techniques are ordered only when "essential in a democratic society." The current structure of interception oversight does not meet the independence, powers, and competency requirements necessary to exert effective and ongoing control, public scrutiny, and efficacy in practice. The effectiveness of the remedies is harmed by the lack of notice of interceptions at any point or proper access to interceptions-related records. The fact that the flaws mentioned in the legal framework appear to affect the fundamental operation of Russia's covert surveillance system is essential. The government's claim that all interceptions in Russia are legitimate and based on adequate judicial authority did not persuade the court in this case. The court further concludes that Russian law fails to meet the standard of law in terms of limiting interventions compared to democratic countries. As a result, there has been a breach of "Article 8 of the Convention".[79]

Yarovaya law

Law No. 374-FZ was signed into law by Russian President Vladimir Putin on July 6th, 2016. The "Yarovaya" legislation is another name for this statute. Telecom businesses and anyone involved in the provision of communications services must comply with new data retention regulations included in the Yarovaya bill, which is mainly intended to prevent terrorism.

A punishment of up to RUB1 million may be imposed for failure to comply with the Yarovaya law's requirements. Even though it should be considered a violation, in theory, it is possible that the Russian investigation and prosecution authorities could be fined for not providing information or codes when requested. Authorities can make this judgement based on past judicial and administrative precedents for comparable offences, as the new regulations have not yet been put into action. Several communication and internet service companies have also expressed worry about the expenses of such a deployment and the resulting rise in their services' prices.

[79] Council of Europe. (2016). Convention for the Protection of Human Rights and Fundamental Freedoms. In Council of Europe Treaty Series 005. Council of Europe.

The Yarovaya package has received a wide range of criticism from a variety of sources. In their opposition to the bill, technical professionals have come together as a single voice. The law was opposed by Russia's government Internet ombudsman. Human rights chief for Putin, Mikhail Fedotov, urged Russian senators to oppose the measure. Internet-based telecom and information distribution service providers will be affected. They are unable to do so because they cannot fairly comply with all of the requirements of the Yarovaya package, which makes them de facto criminals regardless of their behaviour. Several communication and internet service companies have also expressed worry about the expenses of such a deployment and the resulting rise in their services' prices[80].

When it comes to mandating rootkit for encrypted communications in the United States and other countries, Russian legislators and officials aren't alone. If a law is technically impossible, some technologists have interpreted this to suggest that the legislation is merely impractical, which is no worse than having no law at all. It's clear from Russia's experience that no one can keep up with the requirements[81]. Protests have been planned around Russia by Russians worried about the decline in Internet freedom, notably the Society for the Protection of the Internet (IPI).

Conclusion

Tools of surveillance like SORM and DPI have been very effective in managing the narrative against the Russian establishment. These tools very diligently monitor the information over the internet and help the Russian government in controlling and regulating the flow of content online. Though the SORM is a decentralised machine installed at the service providers

[80] Global Privacy & Security Compliance Law Blog. (2016). “Yarovaya” Law - New Data Retention Obligations for Telecom Providers and Arrangers in Russia. [online] Available at: https://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/.

[81] Global Privacy & Security Compliance Law Blog. (2016). “Yarovaya” Law - New Data Retention Obligations for Telecom Providers and Arrangers in Russia. [online] Available at: https://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/.

expense but remains directly in control of FSB via a terminal. Similarly DPI uses sophisticated network management technologies which helps in interception and censorship.

Chapter 4: Challenges of Censorship and Surveillance: Role of civil society and citizenry

In a society where information transmission has become a continuous thing on a massive scale, with more material being produced every day, censorship and surveillance are becoming more prominent. When you talk about it, this procedure is almost comical; where the internet was meant to provide with it a better sense of individual independence, people now see situations where the authority has delved into it as well. When people talk about censorship and monitoring today, they are almost inextricably linked. Censorship is the purposeful suppression of material in order to prevent it from reaching the general audience.[82]

Quite often, the administration is held accountable for content censorship activities. This can assume the shape of internet censorship, news and recreational media censorship, which are two of the most powerful information sources while also being precisely focused censorship targets.

Surveillance can be thought of as a censorship help. The state would have to monitor one's lines of connection in order to restrict content, unintentionally breaching one's privacy. Surveillance, on the other hand, can exist in the absence of censorship. Although the terms "digital censorship" and "internet censorship" are frequently used interchangeably.[83]

The primary reason for governments to engage in censorship-related acts, in the best interests of their citizenry, is to protect them. The prospect of cyberattacks, such as when a foreign virus penetrates a system and executes malicious software to steal data, passwords, and other sensitive information, has prompted governments to authorise more stringent censorship capabilities. This is especially critical now that more countries are entering the digital world and entrusting the internet with money transfers and the exchange of other important papers.

---

[82] Penney, Jonathon, The Cycles of Global Telecommunication Censorship and Surveillance (2014). Santa Clara Law School - High Tech Law Institute, Internet Law Work-In-Progress Paper Series No.3, March, 2014, University of Pennsylvania Journal of International Law, Vol. 36, No. 3, 2015.

[83] Penney, Jonathon, The Cycles of Global Telecommunication Censorship and Surveillance (2014). Santa Clara Law School - High Tech Law Institute, Internet Law Work-In-Progress Paper Series No.3, March, 2014, University of Pennsylvania Journal of International Law, Vol. 36, No. 3, 2015.

The process is also motivated by a desire to preserve a certain ideal, which they believe would constitute a risk to society if it were to be disrupted. Censoring illegal information and data that could potentially incite the public to violence is a type of national-security defence. [84]

However, these government-imposed criteria may be subject to change at the discretion of the government. For example, what an authority considers damaging to its population may not be so in a more traditional sense. For example, limiting some opinions or remarks that are critical of the governing party could be a violation of the constitution's 'right to freedom of speech' principles. Russia is yet another case of censorship at its most extreme. The nation's Internet Sovereignty Law was recently implemented.

The law works in the same way as China's firewall, with the goal of controlling the internet and cutting off access to international platforms. The legislation was allegedly enacted to safeguard Russia against foreign cyberattacks. Certain technocrats, on the other hand, say it appears to be more of an attempt to restrict knowledge. However, since China's firewall is based on state-run systems, Russia will never be able to achieve the same level of control as China. Russia, on the other hand, has had free-flowing net on a worldwide network for the past thirty years, and reversing this would be exceptionally hard.[85]

However, the extremes to which authorities have gone severely limit the options accessible to citizens, and if implemented in democratic nations, would shatter the constitutional basis of freedom.

Fearing the unrest that it might cause in the Soviet Union, the state-of-the-art innovation was destroyed by the KGB in the 1950s. Vlamadir Friedkin, the scientist who invented it, had not produced a fatal infection or a nuclear weapon, then what the KGB dreaded was just a printer that permitted the free flow of information by allowing people to make photocopies of papers

[84] Akbari, A., & Gabdulhakov, R. (2019). Platform surveillance and resistance in Iran and Russia: The case of Telegram. Surveillance & Society, 17(1/2), 223-231.
[85] Akbari, A., & Gabdulhakov, R. (2019). Platform surveillance and resistance in Iran and Russia: The case of Telegram. Surveillance & Society, 17(1/2), 223-231.

from international periodicals. Friedkin's printer exemplifies the intelligence that underpins the Internet censorship of Russia.[86]

The essential person, Vladimir Putin is keeping a track on the development of online restrictions in the post-Soviet Federation and how communication technologies have improved over time, he has also worked as the FSB chief for a brief period of time. Putin forced Russian broadband providers to deploy an intrusive surveillance tool on their servers.

A back gateway to the internet activity of the country is SORM (Sistema Operativno Rozysknikh Meropriyatiy). It is based on the Russian military telephone hacking method. After his re-election in 2012 was met with widespread demonstrations, Russian leaders have grown more concerned about the Web being used by the United States to arrange a color revolution. Putin and his close circle of advisers agreed, like they had accomplished with government television channels a decade earlier, to re-establish national sovereignty in cyberspace. Following Russia's capture and takeover of Crimea in 2013, the Russian government requested that far-right Ukrainian parties' accounts be banned, which Twitter did.

At the very same time, Putin ratcheted up the pressure on other international social media sites by signing a law requiring worldwide internet companies to keep Russian customers' user information on Russian Government servers[87]. This particular move was taken as it would enable the FSB to disclose the networks to SORM, allowing state agencies to track the behavior of the individuals of Russia on international social networking sites. Similarly, through releasing and censoring information, Putin's administration has attempted to limit the role of social media. The Government Service for Telecommunications, Information Systems, and Mainstream Media (Roskomnadzor)[88] has placed certain political opposition leaders' websites on a blacklist, including Gary Kasparov's and Alexei Navalny's news portals. Bloggers with far more than 3000 subscribers were also forced to register in government databases.

---

[86] Akbari, A., & Gabdulhakov, R. (2019). Platform surveillance and resistance in Iran and Russia: The case of Telegram. Surveillance & Society, 17(1/2), 223-231.

[87] Tanczer, L. M., McConville, R., & Maynard, P. (2016). Censorship and surveillance in the digital age: The technological challenges for academics. Journal of Global Security Studies, 1(4), 346-355.

[88] Radchenko, D. (2020). Roskomnadzor-chan and Other Beings: Performative Practices and Folklore Reaction to the Telegram Lockout. Etnograficheskoe obozrenie, (3), 24-37.

The Russian liberal establishment views the Web as a destructive tool in politics because it allows individuals to bypass and bypass the Russian government's established media structures. Several recent upgrades in Runet (Russian Web) [89]legislation have been seen as a depiction of the ambition of the state of Russia to seize control of the digital world. The central administration's Internet sovereignty forum, held in May 2016, focuses on issues like large datasets, the Internet - Of - things, artificial intelligence, and other related topics.

The entire challenge focuses around spreading the concept of creating a closed and isolated network in Internet management. In reaction to the dual terror threats and American dominance over online services, the Russian political establishment is discussing this notion with the general public. However, the complication of various Internet-related legislation, as well as their inadequate and inefficient execution, cause concern in Russia's IT business[90]. Frontline technocrats, including as developers, bloggers, Internet service providers, journalists, hosting firms, and others, must adhere to these regulations in their everyday operations.

The issues that have arisen as a result of these constraints are being met by new ways to evade and overcome them. Several institutions and malicious hackers join forces to start a mass-scale movement for Internet freedom, which includes massive information dissemination and hacking into prohibited networks.

The Russian government is planning to emulate the Chinese Online model. Beginning in 2014, the government attempted to create a "sovereign internet" in the same vein as the Chinese. President Putin approved a sovereign internet law in May 2019, allowing Roskomnadzor[91] (Russia's media regulator) the right to assume control of Runet if it is shut off from the rest of the internet. This will provide Russia the same convenience as the Chinese authorities in isolating the national Internet from the global Internet.

---

[89] Etling, B., Alexanyan, K., Kelly, J., Faris, R., Palfrey, J. G., & Gasser, U. (2010). Public discourse in the Russian blogosphere: Mapping RuNet politics and mobilization. Berkman Center Research Publication, (2010-11).

[90] Shama, A., & Merrell, M. N. (1997). Russia's true business performance: Inviting to international business?. Journal of World Business, 32(4), 320-332.

[91] Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. Policy Brief, Democracy and Disorder Series (Washington, DC: Brookings, 2019), 1-22.

Russian mass surveillance legislation and Regulations

In the big scheme of things, it may serve as an inspiration for other nations to follow, resulting in the disintegration and fragmentation of the worldwide internet framework[92]. The Russian technique of shutting off from the global Internet is highly straightforward for authoritarian governments to adopt since the Chinese method of establishing their own high-tech Internet firewall is difficult to create or copy. Russian mass surveillance aims to regulate and tighten the flow of information through legal and administrative measures[93], as well as intimidate senior executives of internet firms and network operators. The ouster of Vkontakte's CEO is an instance as to how the Russian liberal elite conducts intimidation operations in the event of a confrontation.

Russia has considerably increased its legislation and regulations in order to tighten the control its holds over the infrastructure of the internet, online content, and communication privacy. If these policies are implemented to their maximum restrictive power, the new regulations will be able to substantially limit Russian citizens' capacity to exercise their rights as human beings online, including freedom of accessing information and freedom of speech[94].

As stated by “Hugh Williamson, Human Rights Watch's Europe and Central Asia director”, The Russian government's approach to the internet is based on two pillars: control and increasing isolation from the internet, hence in order to reign over internet users, information and communications networks, the government has amassed a vast arsenal of instruments[95].

New rules and regulations enacted in the last two years have increased the already existing strong power of authorities to proactively filter and ban internet material, hence it eliminates the need for providers' participation to carry out this block. The "sovereign internet" law of 2019 compels internet providers (ISPs) to deploy technology that permits authorities to

[92] Sivetc, L. (2019). State regulation of online speech in Russia: The role of internet infrastructure owners. International Journal of Law and Information Technology, 27(1), 28-49.
[93] Zharova, A. (2019). Ensuring the Information Security of Information Communication Technology Users in Russia. International Journal of Cyber Criminology, 13(2).
[94] Shcherbovich, A. A. (2021). National Sovereignty, Security, and Internet Governance: Impact on Constitutional Principles and Challenges for the Human Rights of Internet Users. In Virtual Freedoms, Terrorism and the Law (pp. 173-189). Routledge.
[95] Zharova, A. (2020). The protect mobile user data in Russia. International Journal of Electrical and Computer Engineering, 10(3), 3184.

bypass providers and instantly block material that are prohibited by the government authorities and divert the web traffic.

A regulation passed in 2018 imposes penalties on google searches that provide access to bypass services, such as VPNs, that permit users to share and exchange forbidden information or provide directions for doing so. Rules passed in 2019 compel VPNs and web search providers to immediately restrict access to sites on the central administration's informational system's list of legally blacklisted sites, which would be updated on a regular basis[96].

Legislative intrusions into mobile communications privacy have also occurred in the last two years. Telephone and internet companies registered with the government of Russia as "information dissemination organizers," such as messaging services and social networks, must stockpile and start sharing information related to the users without the order of the court, according to legislative changes to already existing anti-terrorism legislation that went into effect in July 2018[97].

The Russian government was concerned about the possibly disruptive influence and national security ramifications of information movement within society. The government adopted the "Law on Operational Investigations" in 1995[98], allowing the FSB authorization to view any private communications, including electronic communications, of their fellow citizens. As a result, the first "System for Operative Investigative Activities," commonly known as SORM, was created. This was then expanded in 1998, giving rise to SORM-2[99], which was primarily meant to monitor online activity attentively. Russia was observed submitting yearly recommendations to the General Assembly of the United Nations in the framework of "Developments in the sphere of information and telecommunications" at the start of 1998. In addition, in 1999, a report on "principles in international information security" was submitted to the UN Secretary-General.

---

[96] Sanovich, S. (2017). Computational propaganda in Russia: the origins of digital misinformation

[97] Marklund, A. (2016). Listening for the state: censoring communications in Scandinavia during World War I. History and Technology, 32(3), 293-314.

[98] Rudnik, A. (2020). Why do bloggers keep silent? Self-censorship in social media: cases of Belarus and Russia.

[99] Lü, Q., & Low, B. K. (2011). Probabilistic analysis of underground rock excavations using response surface method and SORM. Computers and Geotechnics, 38(8), 1008-1021.

One thing was evident from these submissions: the issue was as much about international information content flows as it was about the burgeoning subject of computer security. On September 9th, 2000, shortly after the extensive media coverage of the Kursk submarine disaster the previous month, then-President Vladimir Putin enacted the new "Information Security Doctrine of the Russian Federation,"[100] which had been established by his own security council. The manifesto underlined the importance of freedom of expression and the press. Not only that, but it also listed potential threats to natural security as a result of information flow.

In addition to these efforts, the government actively participated in the global digital economy and ensured that the country's local internet business thrived. The Russian Net had become a matter of public discussion as a result. Thankfully, also after enormous limitations on the media and civil society, it experienced little or no ban during the 2000s. However, this does not imply that major attempts were not made to monitor the influence of new technologies on political stability. At home, the country was rocked by massive social media-fuelled protests[101].

The country witnessed Vladimir Putin reclaim his leadership in the early 2010s, notably during the 2011-2012 White Ribbon Protest Movement. Following this, Russia became the poster child for a creative and innovative approach to information management[102]. It was very different from the much-discussed Chinese "Great Firewall" system, which has been in the news for a long time. The final goal was to develop a strategy that emphasized systematic technical censorship.

To put it another way, the nation pioneered a unique technique that combines less blatant, more logically deniable (no concrete proof) and juridical procedures. Furthermore, this paradigm for domestic information modulation not only proved effective for the political structure of Russia, but also for a slew of other nations where thorough censorship was neither technologically nor politically viable.

---

[100] Federation, R. (2000). Information Security Doctrine of the Russian Federation. United Nations International Telecommunications Union (ITU) Archive.
[101] Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. Policy Brief, Democracy and Disorder Series (Washington, DC: Brookings, 2019), 1-22.
[102] Klyueva, A. (2016). Taming online political engagement in Russia: Disempowered publics, empowered state and challenges of the fully functioning society. International Journal of Communication, 10, 20.

As a consequence, Russia has properly banned a number of blocked websites throughout 2012. Because the Internet was basically unfiltered, this decision was seen as a sea change in the country. However, this puts a lot of pressure on a diverse group of producers, which finally opened the way for a slew of controversial online content presenters. The Russian government might clearly feel this growth after the 2012 era[103].

To effectively deal with these demands, new laws and quasi-democratic mechanisms were enacted in the country's legal system. These rules were intended to provide a legal foundation for the censorship of a wide range of information during this time period. These were similarly intended to focus on user data while also ensuring that content intermediaries bear a large amount of obligation[104].

How Digital Right Activists Are Reverting Back to Internet Surveillance Adopted by Russia's Government.

For viewers in Russia, pictures and videos on Twitter were processed more slowly than normal on March 10, 2021. It wasn't a connection or server failure, but an intentional action by Russia's state internet operator Roskomnadzor to restrict traffic to the social networking site, in what analysts say was the first open use of contentious new technology adopted by the Russian government after 2019. In response for what it claimed as a failure to delete thousands of postings encouraging underage suicide and containing pornographic material and also information about substance use, the regulator slowed the US site. The move came after Russian officials accused Social media and online platforms of failing to remove content encouraging children to participate in anti-government demonstrations in January.

Common Russians are constantly looking for ways to circumvent government Internet censorship. Roskomsvoboda and the Digital Protection Center, both located in Moscow, are among the online rights organizations and campaigners devoting efforts to assisting Russians

[103] Penney, J. W. (2014). The cycles of global telecommunication censorship and surveillance. U. Pa. J. Int'l L., 36, 693.
[104] Stoycheff, E., Burgess, G. S., & Martucci, M. C. (2020). Online censorship and digital surveillance: the relationship between suppression technologies and democratization across countries. Information, Communication & Society, 23(4), 474-490.

in circumventing new limits[105]. The website of Roskomsvoboda contains a list of all online resources restricted in Russia, as well as advice on how to circumvent online restrictions and news on the Internet regulations of the country.

The organization also maintains a publicly accessible list of trustworthy Virtual Private Networks (VPNs), which enables people to access banned websites. The government, on the other hand, has mandated that certain prominent providers restrict access to banned websites. Individual activists also give assistance; for example, IT professional Vladislav Zdolnikov operates a Telegram channel where he discusses the current changes in Russian internet censorship and proposes circumvention tools.

Activists for a free Internet continue to look for new methods to democratize technology. On the 21st and 22nd of March, Roskomsvoboda hosted Demhack 2, a "hackathon" for 15 teams of developers from throughout Russia. According to Natalia Malysheva[106], the hackathon's presenter and Roskomsvoboda's press secretary, their goal was "to identify technical solutions targeted at safeguarding people' rights and achieving their interests in the digital world." There are enough ideas to go around. Each hackathon receives roughly 100 proposals, according to Roskomsvoboba.

On March 22, a panel of digital experts selected two winners for rewards that included the opportunity to pitch their businesses to investors. The first prize went to Security Addon, a programme that helps prevent data from being accessed on a device if it is hacked or stolen[107] .The Deep Silent application, for example, allows users to download information to their smartphones even if their connection is slow, making it a helpful resource if access to the internet is limited.

Roskomsvoboda is developing its own tools in addition to assisting developers with their technological solutions. They released Censor Tracker, a Google Chrome tool that may assist users discover and overcome internet restrictions, last year. The organization made it plain

[105]Herasimenka, A. (2018). Responding to Democratic Decay: Large-Scale Political Campaigning on Social Media in Russia.
[106] Ermoshina, K., Loveluck, B., & Musiani, F. (2021). A market of black boxes: The political economy of Internet surveillance and censorship in Russia. Journal of Information Technology & Politics, 1-16.
[107] Sherman, J. (2021). Digital Authoritarianism and Implications for US National Security. The Cyber Defense Review, 6(1), 107-118.

when they launched the extension tool how high they think the stakes are now. They added, "We're getting ready to fight the impending sovereign Runet."

In May 2017 tens of thousands of people marched through the streets of Moscow and two other towns to protest new internet restrictions, in some of the largest demonstrations in the Nation's capital in decades[108]. Last month, legislators adopted legislation that tightens internet censorship, claiming it is vital to avoid foreign intervention in Russian affairs. However, it has been compared to an online "iron curtain" by certain Russian media, and opponents believe it may be used to suppress dissent. All these protests took place as a result of fear of higher digital restriction and more censorship to be imposed in the future[109].

Protesters crowded in a fenced section of Moscow's Prospekt Sakharova street, made a speech on a platform, and shouted slogans like "hands off the internet" and "stop damaging the Russian internet." According to White Counter, an NGO that counts event attendees, the march drew roughly 15,300 individuals. The number of those killed has been estimated at 6,500 by Moscow police.

"If nothing is done, things will deteriorate. The officials will continue on their path, and the breaking point will be reached," said Dmitry, a 28-year-old protester who did not want to disclose his full name. Officers grabbed 15 individuals just at the Moscow event, taking their flags and balloons, according to opposition activists on Twitter. There have been no arrests announced by the police[110].

Strikes in Moscow, Voronezh in the south, and Khabarovsk from the far east were all officially sanctioned. Without the permission of the authorities, a small group of activists went to the streets in St. Petersburg. Russia has sought to restrict internet freedoms in recent years by restricting access to select websites and messaging applications like Telegram. The Russian legislature passed the law on the first of three readings in February.

---

[108] Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. Media and Communication, 5(1), 29-41.
[109] Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. Media and Communication, 5(1), 29-41.
[110] Ciani, J. (2019). Outside the GDPR: challenges in ensuring an effective protection of personal data: the Russian case. Outside the GDPR: challenges in ensuring an effective protection of personal data: the Russian case, 37-60.

It aims to reroute Russian web traffic and information through state-controlled sites and suggests the establishment of the national Domain Name System to ensure that the internet can continue to function even if Russia is shut off from foreign infrastructure. The law will be presented a second time in March, and if passed, it will be signed by the upper chamber of parliament and subsequently by President Vladimir Putin[111].

The measure is part of a push by Russian officials to expand the country's "sovereignty" over the Internet. In recent years, Russia has enacted stricter internet legislation, mandating search engines to erase some query results, messaging services to exchange private keys with security agencies, and social media platforms to keep Russian users' personal data on Russian servers[112].

The protests in the capital have been dubbed "some of the largest" in years by the media. The national Internet bill, which has been meandering its way throughout the Russian Legislature, was at the centre of demonstrators' protests. Data between users would have to be diverted locally rather than being forwarded to systems in other countries under the policy. The act, lawmakers contend, is required to safeguard the nation from potential invasion.

Critics are divided. "The administration is fighting liberty, including online freedom," campaigner Sergei Boiko told a gathering in Moscow, according to Agence France-Presse. "I can tell you this as someone who spent a month in jail for a tweet." According to NPR's Lucian Kim, police made approximately two dozen arrests and seized balloons they considered to be "unmanned flying vehicles." The rally in downtown Moscow was organized by the Libertarian Party[113].

[111] Feldstein, S. (2019). Artificial intelligence and digital repression: Global challenges to governance. Available at SSRN 3374575.
[112] Sherstoboeva, E. (2020). Regulation of online freedom of expression in Russia in the context of the Council of Europe standards. In Internet in Russia: A study of the runet and its impact on social life (pp. 83-100). Springer.
[113] Rosenberg, W.G., 2014. Reading Soldiers' Moods: Russian Military Censorship and the Configuration of Feeling in World War I. The American Historical Review, 119(3), pp.714-740.

Issues

The first issue to underline is that leaders and censors were both after aggregate feelings: during the Russian conflict, the most important thing was to determine the mood of a military unit as a whole in order to regulate mutinous sentiments and deploy soldiers properly.

According to Reuters, protests too were conducted in St. Petersburg, Voronezh, and Khabarovsk. "Hands off the Internet" and "No to Isolation" were yelled at by protestors. The bill is anticipated to be debated by legislators later in March. President Vladimir Putin will have to sign the bill into law at some point. According to Russian reporter Andrei Soldatov, it "will undoubtedly be accepted." He anticipates just modest amendments to the bill in parliament. "The important point – giving the state the option of isolating a certain area or country in a crisis – needs to be kept, without a doubt."[114]

He goes on to say that the idea has the support of two industry titans, Yandex and Mail.ru. "It's the first legislation that puts the burden of expense on the government rather than the businesses," he argues. The protests are in response to other contentious measures recently enacted by Russia's parliament. The protests are in response to other contentious measures recently enacted by Russia's legislature. The law permits judges to punish civilians upwards to $3,000 or imprison them for up to 15 days if they demonstrate "disrespect" to public officials online. Governments may also order sites to delete the data that they consider to be false news[115].

Some perceive the Internet restricting methods as a method to influence the national discussion, especially because Putin's favorability rating has dropped by more than 20% from 2014 to 2019, according to polls by the Levada Center. Human Rights Watch claims that Roskomnadzor, the Russian communications regulator, "waged a war" against Telegram last year. The corporation failed to cooperate with a court ruling requiring it to hand over

[114] Geybulla, A. (2021). Uncensored journalism in censored times: Challenges of reporting on Azerbaijan. Journalism, 14648849211036872.66

[115] Niaki, A. A., Cho, S., Weinberg, Z., Hoang, N. P., Razaghpanah, A., Christin, N., & Gill, P. (2020, May). ICLab: A Global, Longitudinal Internet Censorship Measurement Platform. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 135-151). IEEE.

encryption keys that would allow police to read users' text messages[116]. Russians rushed to the streets as the government attempted to ban Telegram. They tossed paper aircraft, the Telegram emblem, as part of their protest.

After the mass protest, RSF analyzed this entire situation, to understand who is right and who is wrong, what should be followed and what not and finally came up with the conclusion that. International platforms such as Google, Twitter, and Facebook tend to be very important for the freedom of speech in Russia and restrict all the urges that were made to take a firm stance in the face of a government that routinely abuses press and expression freedoms[117]. According to the study, these corporations must do human rights due diligence and commit to opposing any efforts by governments to restrict the internet or monitor material in a way that violates human rights. This is especially true of the Russian government requests that specific information be removed from exhibition or distribution unless it has been ordered by an independent court of law or the content infringes on human rights.

As stated by RSF opposing the actions of the Russian government "The Russian government is flagrantly breaching human rights such as the right to privacy and freedom of the press by adopting widespread surveillance of the public without justification," said Christian Mihr, Executive Director of Reporters Without Borders Germany, in Berlin. "In this circumstance, international platforms like Google, Facebook, and Twitter must take a strong stance[118]. They must not collaborate with Russian authorities, keep users' personal data in Russia, or block specific material since this would be equivalent to doing the censors' job for them. The German government should do everything it can as the host of this year's Internet Governance Forum to fight Russia's plans to split the internet into more or less distinct state-controlled networks."[119]

Other global powers, such as France, Germany, or Russia, were shaken awake by Britain's use of significant swaths of the global telegraph fiber networks for strategic and military gain

[116] Sliesarieva, A. (2020). The Defender vs. the Censor: CDA Analysis of 2017 Russian Web-Source Ban in Ukraine.
[117] David, M. (2017). Russia's challenge to US hegemony and the implications for Europe. In American hegemony and the rise of emerging powers (pp. 198-215). Routledge.
[118] DeNardis, L. (2013). Multi-stakeholderism: The internet governance challenge to democracy. Harvard International Review, 34(4), 40.
[119] Akbari, A., & Gabdulhakov, R. (2019). Platform surveillance and resistance in Iran and Russia: The case of Telegram. Surveillance & Society, 17(1/2), 223-231.

during the conflict, despite causing widespread disruption of contacts among other neutral governments. This was a critical juncture in the history of the worldwide telegraph system.[120]

With state cyber-policing technologies rapidly increasing and cyberattacks becoming a worry for infrastructure upgrades and sectors, internet censorship and monitoring is on the rise around the world. Commentators have grabbed at historical comparisons to help explain these new threats – and their ramifications for global communications and relationships – with Cold War parallels being highlighted, often with little background or consideration for continuity or historical complexity. In recent years, some more thorough efforts on telecom history have been published, which has been helpful.

Given the transnational nature of telecommunications innovations like the Internet, as well as the inclination for critics to draw historical analogies, more research into communications technology and their past is needed, with an eye toward international developments. Because the practice involves two contradictory rules of international law – rights to data and expression as well as states' sovereign right to enforce their territories – it is commonly assumed that international law has very little to speak about Internet surveillance, and even less to give in constricting or resisting it. However, this is most certainly an oversimplification. To put it another way, if a state censor blocked a telegraph, the sender would eventually be notified when he or she got a reimbursement. Moreover, by "tipping off" senders that they were being surreptitiously monitored, such specific refund notices would defeat the entire strategic goal of secret telegraph eavesdropping. These international legal provisions, taken together, effectively limited telegram communication restriction and surveillance.[121]

Through its prevalent regulation over key telegraph facilities, Britain, for example, took measures to secretly demonstrate an intricate "censorship" framework of telegram monitoring and blocking; however, by the 1890s, British authorities interrogated the system's validity under the 1875 Telegraph Convention and curtailed operations. The 1875 Telegraph

---

[120] Penney, Jonathon, The Cycles of Global Telecommunication Censorship and Surveillance (2014). Santa Clara Law School - High Tech Law Institute, Internet Law Work-In-Progress Paper Series No.3, March, 2014, University of Pennsylvania Journal of International Law, Vol. 36, No. 3, 2015, Available at SSRN: https://ssrn.com/abstract=2398491 or http://dx.doi.org/10.2139/ssrn.2398491

[121] Nizzoli, Leonardo. (2021). LEVERAGING SOCIAL MEDIA AND AI TO FOSTER SECURE SOCIETIES AGAINST ONLINE AND OFFLINE THREATS. 10.13140/RG.2.2.29807.97446.

Convention encouraged the use of code words and dialects in telegram communications and gave several significant guarantees. These rules may have served as forerunners to more current "rights" to utilise encryption for confidentiality and privacy.[122]

Iran and Russia's internet governance

Surveillance techniques, tactics, and actors have all changed as a result of technological advancements. The much-lauded Foucauldian panopticism came short of understanding the fluidity and pervasiveness of surveillance that turns people to data and forces its attention on "groups that were previously exempt from routine surveillance". The term of the surveillant assemblage is used in this research to stress the diverse nature of the things that operate together to enable invasive undemocratic surveillance. Iran and Russia use a variety of agents and strategies to gain state control over data and persons in their attempts to monitor Telegram.[123]

Various agents, like users, civil society, regional and global flows, technological breakthroughs, things, and software, construct other assemblages that connect, merge, and deviate from the surveillant assemblage, in contrast to the state, which creates the hegemonic paradigm. While the language explaining Iran's and Russia's bans on Telegram differs slightly, both regimes want total control over digital and traditional outlets. Iran criticizes Telegram of propagating moral degeneration and reiterates Russian accusations that Telegram aids terrorists by providing anonymity and data security to its customers.

Autocratic governments take steps to silence, limit, suppress, and otherwise eliminate narratives that threaten their rule. The strategies and technology used by Iran's and Russia's surveillance ensembles are highlighted in the next section. It also highlights the shifting barriers between police and civilians, calling into question established theories of state authority and suggesting alternative approaches to monitoring in undemocratic settings.

[122] Sliesarieva, A. (2020). The Defender vs. the Censor: CDA Analysis of 2017 Russian Web-Source Ban in Ukraine.
[123] Sliesarieva, A. (2020). The Defender vs. the Censor: CDA Analysis of 2017 Russian Web-Source Ban in Ukraine (Dissertation)

In contrast to authoritarian and strategic monitoring systems, Telegram arrived on the scene promising freedom, confidentiality, and resistance, all of which are etched into the platform's design. In an atmosphere of intense control and surveillance in Iran, Telegram's guarantee of security and user-friendliness drew a massive following.[124]

In April 2018, an established polling agency said that 59.5 percent of Iranians utilize Telegram (ISPA 2018a). In January 2018, Telegram claimed that the program has 40 million monthly as well as 25 million daily active users in Iran, and also 678 thousand Persian streams with two billion daily visitors. There are 38 percent dedicated to amusement, 10% to information, and 3% with economic goals among these channels. Telegram claims to account for 60% of all internet activity in Iran, with advertising income exceeding $100 million each year. For one of the world's most restricted internet governance structures, these are nearly inconceivable figures.[125]

Reactive techniques were initially sharply reacted to such wide use of a messaging network. Celebrities and public personalities were subjected to the stringent Islamic government's inspection in order to alert the public about the state's pervasive surveillance and the penalties of disseminating what the authorities deemed unsuitable. The government implemented stricter surveillance tactics as the number of customers increased.

Telegram is still one of the top 5 messengers in Russia, and it was strangely utilized by government agencies and officials to communicate with residents.[126]

Iran and Russia negotiate control of existing platforms while confronting developing alternatives that are geared to circumvent such controls. Both countries have attempted to control the boundaries of technological innovation by requiring Telegram to localise its facilities and provide them access to user information.

---

[124] Geybulla, A. (2021). Uncensored journalism in censored times: Challenges of reporting on Azerbaijan. Journalism, 14648849211036872.
[125] Geybulla, A. (2021). Uncensored journalism in censored times: Challenges of reporting on Azerbaijan. Journalism, 14648849211036872.
[126] Sherstoboeva, E. (2020). Regulation of online freedom of expression in Russia in the context of the Council of Europe standards. In Internet in Russia: A study of the runet and its impact on social life (pp. 83-100). Springer.

The Cyber Police in Iran, as well as loyal press, vigilant citizenry, and Roskomnadzor's communication agency in Russia, have relied on diverse players inside their surveillant assemblages to control the users and the material. While multinational behemoths like Google and Facebook appear to have struck up a rapport with the Russian establishment, companies that refuse to tame their servers and comply with these governments' demands are regarded as dangerously renegade. As a result, both governments have banned Telegram, with the goal of completely eliminating a platform that has steadfastly eluded their surveillance.[127]

As Telegram visitors in Iran and Russia developed new abilities and technological solutions to preserve their access to the network, both governments were forced to adapt and deal with these issues in order to maintain their dictatorial control over new public areas. When it comes to a comprehensive platform ban, Russia's ruling government has technological problems and is wary of taking steps that could spark large protests. A new set of legislative proposals aimed at making Russia's network more "sovereign" is being drafted in an attempt to circumvent these constraints (Reuters 2019). Iran's surveillant assemblage is forceful and extensive in its pervasive surveillance and rigorous control, despite similar technology limits.[128]

It aggressively censors material and networks, and it follows the Chinese model of replacing international routes with domestic alternatives.

Aside from their differences, Iran and Russia share a burning ambition to capture citizens' data and establish control over the media by all means available.[129]

At various levels, effective countermeasures to disinformation are required, including official legislative measures and laws, corporate commitments, and civil society engagement. Legislative and executive entities in numerous nations have taken steps to curb the

[127]Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. Media and Communication, 5(1), 29-41

[128]Sherstoboeva, E. (2020). Regulation of online freedom of expression in Russia in the context of the Council of Europe standards. In Internet in Russia: A study of the runet and its impact on social life (pp. 83-100). Springer.

[129] Ciani, J. (2019). Outside the GDPR: challenges in ensuring an effective protection of personal data: the Russian case. Outside the GDPR: challenges in ensuring an effective protection of personal data: the Russian case, 37-60.

dissemination of misinformation. They've done so by developing rules of conduct and guidelines, as well as establishing verification networks to combat misinformation. Some companies have started anti-disinformation campaigns, but most have been hesitant and delayed in their efforts.

Telegram has grown to become one of the most widely used communication programmes in the world, offering its users safety from the watchful eyes of spy agencies.

Around the globe, civil society is gradually being mobilised to combat disinformation, with a primary emphasis on human values and strengthening democratic capacity at the community scale. Fears over foreign influence operations including disinformation have intensified after the participation of Russia's Internet Research Agency (IRA) – dubbed a "troll farm" for disseminating pro-Russian establishment misinformation online under false identities – in US politics was revealed in 2016. However, creating a platform that enables users to avoid official inspection comes with its own set of issues. Telegram has been used by the Islamic State to arrange terrorism plots, broadcast propaganda, and take blame for strikes in recent years.

Despite the fact that Telegram was established by a Russian, Pavel Durov, the messaging platform denies any Russian ties.

(One of Telegram's unique features is its channels, which allow messages to be broadcast to an unlimited number of users.) Mr. Durov or others at Telegram focused on the confidentiality of private messages.[130]

[130] Ciani, J. (2019). Outside the GDPR: challenges in ensuring an effective protection of personal data: the Russian case. Outside the GDPR: challenges in ensuring an effective protection of personal data: the Russian case, 37-60.

Conclusion

The challenges of surveillance and censorship come along with the presence of new online revolutionaries, activists and opposition leaders on the Internet. Surveillance is not a difficult process but censorship is. Due to the presence of these new online activists and hackers it is not very easy for the Russian establishment to stop the information from reaching the people over the internet. These individuals find new and innovative ways to circumvent the censorship and access and propagate the restricted content online. In response to that the Russian government comes with new laws and regulations over time to strengthen the censorship. This fight between the two ideas of censorship and online freedom continues in perpetuity by trying to overpower each other with new tools and techniques.

Chapter 5: Global internet governance: Foreign Policy implications for Russia

The cyberspace has gained importance as a competitive arena for various nations owing to various incidences of international political and security concerns having taken place, these include Edward Snowden's revelation on US government's surveillance programs, the Mandiant report[131]disclosing (and perhaps even confirming a few conspiracy theories) the existence of Chinese cyber-spying units on US and lastly, NATO's Tallinn Manual[132] that defined the legal framework in the event of a cyber warfare. Today, an increasing number of governments around the world are expressing their discontent with the system of internet governance and seek to challenge the digital hegemony of the US in cyberspace. One such prominent dissenter is Russia, who over the years has sought to challenge global unanimity.

Three significant aspects can be highlighted about the increasing change in digital legislation around the globe. The first aspect is how governments worldwide try to apply jurisdiction to the digital world, just like the physical world. Nations are concerned about the dominance of private firms in this complex ecosystem and their citizens' unrestricted access to the internet. Secondly, countries are having trouble keeping up with the speed of technical innovations, with technology evolving faster than legislative efforts; this imbalance is calling into question the Westphalian nation-very state's nature and its ability to adapt to current challenges, resulting in a substantial restructuring of government-to-government and government-to-citizen alliances in the twenty-first century. Lastly, based on demographic factors, there is a growing perception that the online landscape is rapidly becoming more cosmopolitan and perhaps less western-centric. The internet's gravitational center will undergo a paradigm shift towards the eastern and southern parts of the world in the coming generations. Even in 2012, quasi countries accounted for sixty-six percent of internet users,

[131] Mandiant Report: Report by a publicly traded American cybersecurity company that gained eminence in 2013 after releasing a report affirming China's role in cyber spying.

[132]Tallinn Manual: A non-binding study pertaining to international law applicable to conflicts and warfare in the cyberspace.

and the number of users worldwide is predicted to increase from two billion in 2010 to three billion by 2016. However, profoundly political considerations are at play: a growing percentage of governments are becoming dissatisfied with the existing internet governance system and are striving to undermine the United States' historical supremacy in the cyber domain[133].

The Russian establishment has always upheld a traditional understanding of the concept of ‘sovereignty’ and the ‘principle of non-intervention’ in governance and its foreign policy. Therefore, it is only natural for them to envisage the cyber arena as a zone having virtual borders similar to physical State borders with existing international laws extending to the cyber arena. This expectation of the Russian government is clearly reflected in Russia’s active participation to promote international norms and rules as the guiding light to States’ behavior in cyberspace across the globe.

The Russian establishment increasingly sees the internet as politically disruptive, because it allows citizens to bypass government-controlled print and electronic media, such as newspapers and television. However, the game-changer moment in Russian internet policy was in 2011. In 2011, the year of Arab Spring[134]Russian civil society utilized social media to organize parliamentary election protests, about which then-US Secretary of State Hillary Clinton expressed "serious concerns." This year, Putin reclaimed the presidency after four years of sharing it with Dmitri Medvedev. Since Vladimir Putin's return to the Russian establishment in May 2012, the state Duma has debated and passed a series of laws, the most notable of which went into effect on November 1, 2012, created a "single register" of banned websites that contain child pornography, drug abuse, and drug production instructions, and suicide advocacy. According to analysts, blocking individual websites and IP addresses may necessitate service providers acquiring deep-packet inspection technology1[135]. This might

[133] Linvill, D. L., Boatwright, B. C., Grant, W. J., & Warren, P. L. (2019). “THE RUSSIANS ARE HACKING MY BRAIN!” investigating Russia's internet research agency’s Twitter tactics during the 2016 United States presidential campaign. *Computers in Human Behavior*, *99*, 292-300.

[134] Arab Springs: A series of uprisings that took place across much of Arab world between 2010-2012.

[135] Barberá, P., Jost, J. T., Nagler, J., Tucker, J. A., & Bonneau, R. (2015). Tweeting from left to right: Is online political communication more than an echo chamber. Psychological Science, 26, 1531–1542. https://doi.org/10.1177/0956797615594620.

make blocking specific and more prominent applications, such as Skype, or target pages, such as particular Facebook groups, much quicker. Members of both chambers of parliament are pushing for additional legal proposals, and Russia's most potent leaders frequently speak out in favor of increased government surveillance and more well-organized policing. The Russian authorities believe that regulating 'their' national internet poses a dual threat to governance and political sovereignty, as seen by the 2012 law[136].

The BRICS Cable Project & Russia

In September 2013, the then president of Brazil, Dilma Roussef had announced the beginning of an ambitious project, 'BRICS Cable' whose objective was to create a 34,000 km network of submarine cables connecting Brazil with Vladivostok through Cape Town, south India and the Taiwan Strait. The goal of this project was to create an independent internet outside the surveillance of America's National Security Agency, whose extent of surveillance had just been revealed to the whole world by the Snowden affair.

The BRICS cable project gave the country an opportunity act as an heavyweight in the cyberspace, as evidenced by representations and positions of Putin's rhetoric's, taking the form of patriotism based on state power and sovereignty[137].

The Sovereign Internet: A Russian Perspective

Russia first started its discussion on the concept of 'sovereign internet' around 2011-12, as cyber borne revolutions wreaked havoc upon authoritarian regimes (the Arab springs). Convinced of the role played by the Western States in the incitement of these revolutions, Russia sought to put an end to any possible disruptive influences that may lead to a situation of unrest in the country. While Russia does not seek to transform itself into a corporate

[136] Contest and Conquest: Russia and Global Internet Governance https://www.chathamhouse.org/sites/default/files/field/field_publication_docs/INTA91_1_07_Nocetti.pdf

[137] Andrei Soldatov and Irina Borogan, 'The Russian establishment's new internet surveillance plan go live today', Wired, 1 Nov. 2012.

internet, however it also has its sights set on DNS, a national DNS. For this purpose, Russia has spent years enacting statutes that have forced social media giants and various international companies to store data of the Russian citizens having access to them, while those who refuse to abide by this condition such as LinkedIn, are blocked for their non-compliant behavior[138].

Russia's traditional political approach toward cyberspace is also influenced by certain individuals whose perceptions made a strong impression and helped in shaping up the Russian leadership's views on the Internet. One such individual is Alexei Chadayev, an erstwhile ideologist of United Russia, he played a crucial role in promotion of 'direct internet democracy' in the country; leading IT businessman, Igor Ashmanov has been promoting a 'national search engine' and advancement of 'information sovereignty' within the country and at global level. Further, Ashmanov's wife, Natalya Kasperskaya[139] (formerly the wife of computer security expert Yevgeny Kaspersky) has also been actively engaged in promoting the Russian government's initiatives to strengthen its control over cyberspace.

However, the idea of a 'sovereign internet' is utopian in nature, as cannot be completely cut yourself off from the global internet and North Korea is an accurate example of this, where a single cable connects the country to the entire world through the cyberspace. This once again reminds us that it's its impossible to control the cyberspace, or divide it into territories having defined boundaries[140].

Impact of Russian internet governance on Russia and Ukraine conflict

Ukraine is sandwiched between Russia and Europe. It was a member of the Soviet Union until 1991. Since then, it has been an imperfect democracy with a wretched economy and a

[138] Bloomberg (2018) Russians Staged Rallies For and Against Trump to Promote Discord, Indictment Says. Fortune, February 17, http://fortune:com/2018/02/17/russian-organized-rallies-election-meddling/.

[139] Julien Nocetti, '"Digital Russian establishment": power and the internet in Russia', Russie.NEI.Visions, no. 59 (Paris: Institut français des relations internationales, April 2011), p. 9.

[140]"Everything you need to know about Ukraine crisis", Max Fisher, 3 September 2014, https://www.vox.com/2014/9/3/18088560/ukraine-everything-you-need-to-know

foreign policy oscillating between pro-Russian and pro-European positions[141]. The Ukrainian crisis began in 2013 when President Viktor Yanukovych rejected a proposal that would have allowed Ukraine to become more integrated with the European Union. This led to enormous protests that Yanukovych tried to put down forcefully. In this crisis, Russia backed Yanukovych, while the US and Europe backed the protests. Since then, the situation between Russia and Ukraine is not merry[142].

Along with military forces, Russia also implements social media strategies to spread misinformation among the Ukrainians. This has led to information war between the both. Information wars are not new, but the means to cause distress in a country through misleading information has changed. Earlier the electronic media and the newspaper were used to spread disinformation. Now, this is done using social networks, which creates humongous reach. In the age of social media and the internet, there is no need to throw leaflets outside the enemy line. Instead, now the purpose is served by hiring thousands of internet trolls. Many experts have tried to examine the information war between Russia and Ukraine.

One such attempt was made by Aliaksandrau and Womack (2014) to investigate the new information war between Russia and Ukraine. Russians back President Vladimir Putin and consider Ukrainians to be Nazis. As a result, there has been a significant increase in anti-Russian sentiment in Ukraine because Ukrainian people believe Russia is the intruder. In the recent past, Ukraine saw the emergence of several innovative and interesting media projects[143]. Stopfake.com and other online publications were created to expose the fabricated stories, images, and general lies about events in Ukraine that were shared on the internet and disseminated through Russian media, according to them. This was after Russian media created fake propaganda by spreading images of bloodshed and dead people through social media, which did not actually belong to Ukraine. The photos belonged to some past event or

---

[141] Golovchenko, Y., Buntain, C., Eady, G., Brown, M. A., & Tucker, J. A. (2020). Cross-platform state propaganda: Russian trolls on Twitter and YouTube during the 2016 US presidential election. *The International Journal of Press/Politics*, *25*(3), 357-389.

[142] Aliaksandrau, A. (2014). Brave new war: The information war between Russia and Ukraine. *Index on censorship*, *43*(4), 54-60.

[143] Mejias, U. A., & Vokuev, N. E. (2017). Disinformation and the media: the case of Russia and Ukraine. *Media, culture & society*, *39*(7), 1027-1042.

other location during conflicts or natural disasters. Bloggers, social media activists, and journalists in Ukraine are now making attempts to make their audiences aware of fake propaganda. This information war violates the ethics of internet governance and affects the other neighbouring nations[144].

The continuing crisis between Russia and Ukraine can be seen as an example of how the internet has bolstered political actors' ability to spread misinformation. However, propaganda is no longer produced and disseminated solely by the state-owned media monopoly[145]. Now citizens also deliberately contribute to their alienation by utilizing social media to manufacture, consume, or transmit false information, contributing to a new system of disinformation increasing authority.

Russia also used cyber espionage operations against Ukrainian journalists' systems and networks and Ukrainian, NATO, and EU officials. Some cyberattacks had already begun before the violence erupted. The Sandworm espionage operation started in 2009 and continued through 2014, targeting EU and NATO telecoms infrastructure. During September 2014, Sandworm's malware ramped up and attacked Ukrainian government networks, coinciding with the NATO summit in Wales. Other espionage efforts began in the run-up to the war[146]. In mid-2013, Operation Armageddon was launched to target the Ukrainian government, law enforcement, and military officials. As anti-government protests erupted in Ukraine, sophisticated spyware called 'Snake' infiltrated the Ukrainian prime minister's office and several diplomats working abroad. Moreover, Operation Potao began when Russia started its intrusion of Crimea, attacking Ukrainian officials' computers and mobile devices[147].

---

[144] "Russian Cyber Espionage Campaign – Sandworm Team."

[145] Yin L, Roscher F, Bonneau R, Nagler J and Tucker JA (2018) Your friendly neighborhood troll: The internet research agency's use of local and fake news in the 2016 us presidential election.

[146] David E. Sanger and Steven Erlanger, "Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government," New York Times, March 8, 2014, http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html.

[147] Stewart, L. G., Arif, A., & Starbird, K. (2018). Examining trolls and polarization with a retweet network. In: Proc. ACM WSDM, workshop on misinformation and misbehaviour mining on the web

In Ukraine, Russia carried out a series of cyberattacks to disrupt or destroy targets. Pro-Russian hacker groups out of the Russian state carried out a range of cyberattacks, similar to the earlier espionage. Cyber Berkut, a Ukrainian organization, was particularly well-known for this. Cyber Berkut launched DDoS assaults and defacements against Ukrainian and NATO websites, obtained US-Ukraine military cooperation documents, and disrupted Ukraine's Central Election Commission network in an attempt to sway the Ukrainian parliamentary election[148]. While it is possible that the Russian government secretly aided these groups, the crude and indiscriminate nature of the attacks suggests little coordination or cooperation with the Russian establishment. However, it was found that these non-state attackers caused only minor harm. But concluding that the attempt of these hacking groups was not significant would be wrong. Because these hacking organizations are likely to have caused confusion and chaos among their targets, harmed the confidence of the Ukrainian state among its citizens, and terrified Ukraine's connections[149].

The corpus of online communications broadcast by Russian authorities, reporters, and news organizations to foster a pro-Russian perspective of the crisis was a significant component in Russia's information war on Ukraine[150]. This policy is a continuation of Russian media policies at home. Because television is almost entirely controlled by the government and a powerful platform for the Putin government, the internet is one of the few viable channels for expressing popular discontent in Russia. As a result, the Russian government spends a significant amount of money researching and controlling online media pipelines. Russia-backed reporters, bloggers, and people on social media to spread pro-Russian narratives against Ukraine.

[148] (Limonier, 2014) Russia in Cyberspace: Issues and Representations https://www.cairn-int.info/article-E_HER_152_0140--russia-in-cyberspace-issues.htm?contenu=article

[149] Robert Lipovsky and Anton Cherepanov, “Operation Potao Express,” ESET Report (July 2015): 9-13.

[150] Petro Zamakis, “Cyber Wars: The Invisible Front,” Ukraine Investigation, April 24, 2014, http://ukraineinvestigation.com/cyber-wars-invisible-front/.

Influence of Russian Internet policies on the 2016 US Elections

Experts, government leaders, and the public debate whether the 45th president of the United States, Donald Trump, owes his electoral success in the 2016 US election to the intelligent disinformation campaign orchestrated by the Russian establishment. The Internet Research Agency (IRA) of Russia reached millions of people in the United States, according to the testimony given to Congress by Google, Twitter, and Facebook. The US Department of Justice indicted 13 members of the IRA in 2018 as being part of a Russian group attempting to sway US elections11[151].

Nathalie Maréchal (2017) did a comprehensive study on Russian internet policy to explore the aftermath of this significant event. This study analyzed the networked authoritarian and the geopolitics of information in detail. Accusations made of Russian meddling in Western elections, including the 2016 presidential election in the United States, would certainly be a pattern of "information assault." Russia could be trying to give its rivals a taste of their own medicine, or it could be teaching the world about the perils of unrestricted information flow[152] . However, it is also plausible that, after failing to secure an agreement for a norm prohibiting informational abuses of state sovereignty, Russia opted to utilize that potent weapon to restructure the international system better to suit its authoritarian, Western democratic perspective 1.

In another study, Linvill et al. (2019) tried to examine Russian internet research agency Twitter strategies during the US Elections of 2016. This study examined tweets from accounts linked to the Russian Internet Research Agency to better understand the approach used by that group on Twitter to sway American political discussion and the results of the 2016 presidential election. They took a sample of tweets from the month leading up to the election[153]. They examined them to learn more about the qualitative character of the tweets

[151] CyberBerkut, http://cyber-berkut.org/en/

[152] "Hackers Target Ukraine's Election Website," Agence France-Presse, October 25, 2014, http://www.securityweek.com/hackers-target-ukraines-election-website.

[153] Jen Weedon and Laura Galante, "Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not So Fast." FireEye Blogs, March 12, 2014, https://www.fireeye.com/blog/executive-perspective/2014/03/intel-analysts-dissect-the-headlines-russia-hackers-cyberwar-not-so-fast.html.

and the quantitative disparities between the different types of IRA Twitter accounts. Attack left, support right, attack right, defend left, attack media, attack civic institutions, and camouflage were the seven categories of Twitter behavior found. While camouflage was the most popular type of tweet, the descriptive analysis revealed that attack left and support right was the next most popular[154]. There were several quantifiable discrepancies between how different account types behaved. Their findings shed light on how a foreign disinformation operation worked in practice. Their data implied that the activity of IRA tweets might be an attempt to cause unrest and instability in the US as well as help Trump in the election. The IRA worked to disseminate distrust in institutions and radical ideas in the run-up to the 2016 US Presidential election but did in a balanced way such that it benefitted Donald Trump. On social media, political divisiveness is rampant. Users with the same political ideas were found to form echo chambers from the literature. Steward, Arif, and Starbird (2018) conducted a network analysis of confirmed Russian Twitter accounts. He discovered that the coordinated attempt to bring numerous topics into the public eye characterized a high degree of polarization. In this context, our findings revealed that Russian troll accounts that posted content attacking the left/supporting the right produced more tweets than those who attacked the right/supporting the left. Furthermore, tweets attacking the left and defending the right were more likely to be about candidate Clinton than tweets attacking the right and supporting the left were about candidate Trump[155].

Allcott and Gentzkow (2017) studied the impact of disinformation on social media on the users during the 2016 US elections. The study examined how users were exposed to fake and misleading information. Before the elections, the general public had more exposure to posts promoting Trump than Clinton posts on Twitter. Thus, they found that an average social media user in the US remembered more pro-Trump-related posts and less pro-Clinton-related

---

[154] Jill Dougherty, “Everyone Lies: The Ukraine Conflict and Russia’s Media Transformation,” Discussion Paper Series, Shorenstein Center on Media, Politics, and Public Policy (July 2014): 2-29.

[155] Max Cherney, “Pro-Russian Hackers Took Down Three NATO Websites,” Motherboard, March 16, 2014, http://motherboard.vice.com/blog/pro-russia-ukranians-hack-nato-websites; and Thomas Barrabi, “NATO Not Responsible For Ukraine's Security From Russia, Should Focus On Member Nations, Latvian Envoy Says,” International Business Times, May 6, 2015, http://www.ibtimes.com/nato-not-responsible-ukraines-security-russia-should-focus-member-nations-latvian-1910551.

posts. Their results supported a wider concept that social media significantly impacted how topics rose to greater importance during the election. They claimed that the Russian government systematically used this concept to disrupt the democratic process in the United States.

Golovchenko et al. (2020) also tried to investigate the digital propaganda strategies of the Internet Research Agency during the 2016 US elections. There were two points of view towards the actions of Russian in the 2016 elections. The US government debated whether the Russian IRA "trolls" backed Trump because he assured to aggravate the relationship of the US and Russia. Furthermore, the Russian establishment tried to tarnish the image of Clinton because she insisted on barring Russia for military indulgence in Ukraine. While other experts have suggested that the Russian establishment was not exclusively trying to support one candidate over another, but rather it tried to create political discord by backing liberals and conservatives simultaneously. Golovchenko et al. (2020), in their study, attempted to assess the evidence supporting these techniques. The politically social media platform, Twitter, was chosen to evaluate the content circulation during and after the election period. For this purpose, the tweets of IRA "trolls," which are human-operated Twitter accounts but run by fake identities, were studied[156]. The two outlooks were explored by evaluating the activity and favoritism of 1,052 Russian establishment-linked IRA "troll" Twitter accounts. The researchers have concluded a mixed outcome from this study. The activity of Twitter accounts of the Russian IRA was consistent but multidimensional. The tweets of IRA were most probably designed to account for various possible outcomes and applications12. This outcome is parallel to Linvill et al.'s (2019) results[157].

The concept of propaganda itself can be further distinguished as "white propaganda" and "black propaganda." Russian IRA trolls used the black propaganda strategy. In this propaganda, misleading and fake information is spread on purpose while keeping the reality hidden from the general public. However, the implication of Russia's IRA using black

[156] Sacha Dov Bachmann and Hakan Gunneriusson, “Russia’s Hybrid Warfare in the East: The Integral Nature of the Information Sphere,” Georgetown Journal of International Affairs: International Engagement on Cyber V (2015): 199-200.

[157] Council on Foreign Relations (2017) Clinton on the issues: Russia. https://www:cfr:org/interactives/campaign2016/Hillary-clinton/on-russia.

propaganda strategy could not be justified. Because while IRA Twitter accounts shared half as much content from deceptive websites as ordinary Twitter users, they only accounted for 6% of all links shared, according to Yin et al. (2018). From the literature, it can be concluded that the goal of the Russian government during the 2016 US Presidential Elections was to disseminate discord and dissatisfaction among the general public. To do this, the Russian establishment made strategic use of the information or misinformation, causing information warfare. It can be implied that the vision behind such actions might be to achieve military and political goals. But it might be intentional, or unintentional, that this discord was so disseminated that it favored the republican government[158].

Where Does Russia Stand Today?

At present, more than 50 million Russians are acquainted with the internet. In terms of quality, the Russian network is one of the fastest running networks in the world. With around 40 percent of these connections being fiber optic ones, the speed of the network enables Russian internet users to be active online. In addition to this, Russia is also one of the foremost producers of digital data in Europe, possessing technical knowledge higher than that of other developed countries, and proving to be a direct contender against America's hegemony over the World Wide Web. The Russian Yandex is in wider use than Google and the Russians prefer their Vkontakte over Facebook[159].

[158] Sacha Dov Bachmann and Hakan Gunneriusson, "Russia's Hybrid Warfare in the East: The Integral Nature of the Information Sphere," Georgetown Journal of International Affairs: International Engagement on Cyber V (2015): 199-200.

[159] (Nocetti, 2014) The Global Internet is Disintegrating. What comes next? https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next

Conclusion

Russia has used its internet capabilities very effectively in order to subdue its adversaries. It has been well shown in the cases of Ukraine and USA as how Russia has been able to create internal dissatisfaction in these countries without getting itself directly involved. These tools of surveillance, censorship and intrusive programs are very practical in contrast to the Great Firewall of China. It has led to the development of a market for Russia in global cyberspace, in which authoritarian countries that don't possess such internet capabilities buy these technologies or consult Russia for managing the information over their local internet. In contrast to these developments in Russia there is an increasing change in digital legislation around the globe in order to protect their inter sovereignty.

Chapter 6- Conclusion

From the aforementioned chapters, it can be concluded that the development of Surveillance in the Russian Internet concentrated on shielding published data that derived through personal data against uncontrolled distribution. It has also highlighted a new criminal offense related with the temporary restriction of the distribution of the data related to the “protected persons” of the country. Surveillance in the Russian Internet promoted a global digital economy that simply flourished in the Russian Internet Market as well as outside Russia.

The politics of cyber control in Russia promotes several advancements in the Russian state's capabilities to capture the digital sphere in the bag of national control. The Regulation and directive bill also aims to enhance the development of surveillance in the Russian Internet that presents a unique security threat in contrast to other cyber hegemony measures. The Russian establishment Internet threat includes hardware from other countries' internet architecture and extirpation of western software. The History of Russian Authorities also represents ongoing surveillance rituals that sourced out with the grounded forces in Russia’s Soviet past.

The study has covered the approach by the Russian establishment to control the flow of information, domestic surveillance, and the historical approach of Russia in information control, and the amendment to the law of personal data.

The tools of surveillance involve SORM and Deep Packet Inspection (DPI) Technology. SORM is a decentralized object made up of commutators, servers, switches and software deployed at the service providers expense but directly managed by the FSB via a terminal. SORM was first placed on analog signal telephones. Besides that, Deep Packet Inspection (DPI) Technology is a formational technology that creates possibilities for controlling the regulatory flow of content online. It also represents the narrative against the Russian State that portrays Russia is not a free state regarding internet freedom.

Challenges of censorship and surveillance present the new online revolutionaries and activists in fighting with different legislative intrusions into mobile communications that have occurred in the last two years. The government adopted the "Law on Operational Investigations" in 1995, allowing the FSB authorization to view any private communications, including electronic communications, of their fellow citizens. The law will be presented a second time in the near future, and if passed, it will be signed by the upper chamber of parliament and subsequently by President Vladimir Putin.

International platforms such as Google, Twitter, and Facebook tend to be very important for the freedom of speech in Russia and restricts all the urges that were made to take a firm stance in the face of a government that routinely abuses press and expression freedoms.

The Russian and global internet governance highlighted the increasing change in the digital legislation around the globe. In 2011, the year of the Arab Spring, Russian civil society utilized social media to organize parliamentary election protests, about which then-US Secretary of State Hillary Clinton expressed "serious concerns." It also had a huge impact upon Ukraine that led to protests of Russia backed Yanukovych, while the US and Europe backed the protests.

As it is very evident that not every country like China can develop its own giant firewall system which helps in blocking all the data coming from outside as it requires enormous level sophisticated tools and technologies. But the Russian model of internet censorship with tools like SORM which only requires installation of hardware at some specific points in local cyberspace, has become very attractive for authoritarian regimes across the world to buy or develop these types of technology. It makes authoritarian regimes less prone to fall due to the development of events like the Arab Spring.

Thus, Russia has evolved itself as the paragon of an innovative, experimental and technical system design to information manipulation. It is considerably dissimilar from the widely known Chinese "Great Firewall" system that continued to remain in discussion for a long period. The ultimate aim was to devise a method that primarily concentrated on systemic technical censorship. In general: the country developed a quirky system that stands on a mix of less overt, more plausibly deniable (no clear evidence) and legalistic

approaches.Furthermore, this method for the domestic modulation of information not only resulted efficacious for Russia's own political system but resulted favourable for a number of other countries in which a systematic-censorship capability was not technologically or politically viable.

To unravel the nature of the Russian government, as to why it places such great emphasis on surveillance and censorship, lies in its history. The history of surveillance and censorship is not new in Russia. Vast boundary, huge geographical area and difficult terrain has always created vulnerabilities for the Russian state from different sides. In order to ensure its sovereignty over its territories, tools of surveillance and censorship of information have always been used by the Russian state in the past. Today the nature of surveillance and censorship may have changed including the developing domains of cyberspace, the idea still remains the same. Protection of sovereignty, ascendancy and autonomy over its territories and subjects is paramount for the Russian government.

In order to understand the scepticism of the Russian government over the internet it is necessary to mention that most of the internet technologies has been developed by American and European nations. The rivalry with West is not just based on power projection or bipolarity but also a cynicism in approaches towards each other. One can not discount the fact that if the internet were to emerge and develop in Russia, the western countries may have the same level of wariness about the internet. Thus Russia in order to protect its influence regionally and globally will have a mixed modus operandi, attitude and strategy towards global and local internet governance. And in episodes like Snowden affairs it has been already corroborated that US establishment and intelligence agencies are no less undemocratic and authoritarian when it comes to regulation of data over the internet. With its unprecedented capabilities over internet technologies, the US has all the potential to harm the interest of any nation states if it gets unwarranted entry into someone’s cyberspace without effective control mechanisms. Thus the Russian government is developing all its mechanisms to develop long lasting and effective control over its cyberspace.

With this idea of realism Russia has played well over the internet in order to protect its sovereign interests. Like, the corpus of online communications broadcast by Russian authorities, reporters, and news organizations to foster a pro-Russian perspective of the crisis was a significant component in Russia's information war on Ukraine. From the literature studied in the chapters, it can be concluded that the goal of the Russian government during the 2016 US Presidential Elections was to disseminate discord and dissatisfaction among the general public. Along with military forces, Russia also implements social media strategies to spread misinformation among the Ukrainians. This has led to information war between the both.

The Russian government in the last decade has played a great role in promoting the idea of data surveillance over the internet. It has not only used soft means of control like legislations, policies and executive orders but also devised hard means of control like tightening the flow of information through internet and internet service providers by coercion and compulsion. Tools like SORM and DPI have also given new ways to keep a check on dissemination of free flow of information creating robust mechanisms for easy access of Russian authorities into public data. These efforts have not only helped the Russian government in controlling foreign influences but also curbing the dissent and political oppositions in Russia itself. The current establishment of Russia has done everything in its sphere to check the development of any strong political opponent in Russian political space creating enough space for Vlamadir Putin to remain as a sole strong leader in Russia.

To handle the uncontrolled flow of information in an effective way, new laws and quasi-democratic processes found their entry in the legal arena of the state machinery. The objective of these legislations was to formulate a legal base for the blocking of a major variety of content during this period.In addition to this, these also meant to zero in on the user data, while also taking care to create a substantial load of liability on content and information intermediaries.

But due to the continuous efforts of internet activists, opposition leaders, and NGOs in order to provide the right information to the common masses has been able to circumvent the Russian surveillance and censorship protocols. The Russian civil society has played a great role by using all the available technological tools and techniques to put forward its interests.

This opposition in the form of internet and cyber activism will benefit Russian democracy and its development in future by forming a systematic tool for proliferation of a credible level of opposition in Russian politics.

In giving thought to this idea of inextricably linked surveillance and censorship mechanisms, the further strengthening of its control over data by the government is not going to help either the people or the current establishment of Russia. It will only further deteriorate the relationship between citizenry and state. These undemocratic tools are obstacles in the formation of a full fledged democracy in Russia. Though it would be eventually wrong to pull off all the control from internet for any government considering its ramifications in form of cyber terrorism and foreign intervention but eliminating spaces of free speech and expression over internet will be detrimental for government itself. This may result in subversion of essential information for effective governance and administration too. History tells us that due to fear of Joseph Stalin and his policies during the great purge soviet officials provided wrong data and information over production of food grains and essential commodities which resulted in massive famine across Russia.

Along with this the coercive surveillance and censorship over the internet will result in decline of growth of Russian internet giants and their capabilities. Russian internet giants like Yandex and Vkontakte have provided tremendous competition to global giants like Google and Facebook. The unnecessary intimidation and arm-twisting from Russian authorities to its operatives will result in brain drain from Russia. This will not help the Russian state but its adversaries only. By allowing free flow of information and data over the internet and less censorship these local internet giants can turn into global giants creating greater room for Russian soft power build up.

It will also create room for development of other upcoming advanced technologies like artificial intelligence, machine learning, data analytics, neural networks, quantum computing, edge computing, blockchain, virtual reality, augmented reality, internet of things ,etc. These technologies have multifaceted applications in fields of governance, administration, military and space. The countries who will control these technologies will rule the world in future. Russia can harness these technologies by developing them through both state sponsored and private partnerships mechanisms and can create new paradigms in geopolitics. It can happen

only when the unnecessary censorship over public data will reduce and give more space to talented technocrats to further augment the Russian internet capabilities.

The future of global internet governance requires the assimilation of every human being on the planet. The democratisation of technology is essential for its better development. Restrictions and censorships in any part of the world will only hamper the prospects of technology. In order to get the virtues and fringe benefits of technological development it is essential for every race on the planet to participate and contribute. It's essential because technology is a double edged sword, it comes along with both positive and negative applications. The larger participation of people across the world will make technology more humane and benign. Thus creating bubbles of isolated cyberspace with undemocratic leadership will not help the future generations and the possibilities of mankind.

References

Chapter 2-

*****Executive Order approving Basic Principles of State Policy on International Information Security," Russian establishment.ru, April 12, 2021, http://en.Russian establishment.ru/acts/news/65350.

Executive Order approving Basic Principles of State Policy on International Information Security," Russian establishment.ru, April 12, 2021, http://en.Russian establishment.ru/acts/news/65350.

M Ristolainen, "Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West," Journal of Information Warfare 16, no. 4 (2017): 113-131

JULIEN NOCETTI, Contest, and conquest: Russia and global internet governance, International Affairs, Volume 91, Issue 1, January 2015, Pages 111–130

Polina Kolozaridi and Dmitry Muravyov, "Contextualizing sovereignty: A critical review of competing explanations of the Internet governance in the (so-called) Russian case," First Monday 26, no. 5 (May 2021).

Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: understanding Russian Internet policy. Media and Communication, 5(1), 29-41. https://doi.org/10.17645/mac.v5i1.808

DeNardis, L. (2014). The global war for internet governance. New Haven, CT: Yale University Press.

MacKinnon, R. (2011). China's "networked authoritarianism". Journal of Democracy, 22(2), 32–46.

Soldatov, A., & Borogan, I. (2012). The Russian establishment's new internet surveillance plan goes live today. Wired. Retrieved from https://www.wired.com/2012/11/russia-surveillance

*Lokshina, T. (2016, July 7). Draconian law rammed through Russian parliament: Outrageous provisions to curb speech, privacy, freedom of conscience. Human Rights Watch. Retrieved from https://www.hrw.org/news/2016/06/23/draconian-law-rammed-through-russian-parliament

See, e.g.: Yulia Nikitina, "The 'Color Revolutions' and 'Arab Spring' in Russian Official Discourse," Connections 14, no. 1 (Winter 2014): 87-104, https://www.jstor.org/stable/26326387, 88; and Soldatov and Borogan, The Red Web, 124, 125, 146.

See, e.g.: Yulia Nikitina, "The 'Color Revolutions' and 'Arab Spring' in Russian Official Discourse," Connections 14, no. 1 (Winter 2014): 87-104, https://www.jstor.org/stable/26326387, 88; and Soldatov and Borogan, The Red Web, 124, 125, 146.

*See some of Putin's public comments: "Putin says Snowden was wrong to leak secrets but is no traitor," Reuters, June 2, 2017, https://www.reuters.com/article/us-russia-putin-snowden/putin-says-snowden-was-wrong-to-leak-secrets-but-is-no-traitor-idUSKBN18T1T4

Noah Rayman, "Putin: The Internet Is a 'CIA Project,'" TIME, April 24, 2014, https://time.com/75484/putin-the-internet-is-a-cia-project/.

Nathalie Maréchal, "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy," Media and Communications 5, no. 1 (2017): 29-41, https://www.cogitatiopress.com/mediaandcommunication/article/view/808/808, 32.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30(1), 75–89. doi:10.1057/jit.2015.5

Chapter 3-

[1] Ermoshina, K., Loveluck, B. and Musiani, F. (2021). A market of black boxes: The political economy of Internet surveillance and censorship in Russia. Journal of Information Technology & Politics, pp.1–16.

*[2]Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. *Policy Brief, Democracy and Disorder Series (Washington, DC: Brookings, 2019)*, 1-22.

[3] Ermoshina, K. and Musiani, F. (2018). Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era. Media and Communication, 5(1), p.9.

[4] openDemocracy. (n.d.). Surveillance: Zakharov v Russia and what it means for the Investigatory Powers Bill. [online] Available at: https://www.opendemocracy.net/en/zakharov-v-russia-refresher-on-how-far-europe-has-come/ [Accessed 5 Jan. 2022].

*[5] Federal Law of July 6, 2016, No. 374-FZ " On Amendments to the Federal Law" On Countering Terrorism "and certain legislative acts of the Russian Federation in terms of establishing additional measures to counter terrorism and ensuring public safety."

*[7] A Comprehensive Overview: 2015 Amendments to the Federal Rules of Civil Procedure. (2015). Kansas Law Review.

[8] Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. *Media and Communication*, *5*(1), 29-41.

[9]“ Russian-made surveillance technologies used in the west”, Andrei Soldatov, https://www.wired.com/2013/05/russian-surveillance-technologies/

[10] “Here’s what Putin didn’t tell Snowden about Russia Spying”, Mark Memmott, 18 April 2014, https://www.npr.org/sections/thetwo-way/2014/04/18/304530695/heres-what-putin-didnt-tell-snowden-about-russias-spying

[11] “Lawful Interception: the Russian Approach”, Privacy International, 04 March 2013, https://privacyinternational.org/blog/1296/lawful-interception-russian-approach

[12] Peers, S. (2015). EU Law Analysis: Zakharov v Russia: Mass Surveillance and the European Court of Human Rights. [online] EU Law Analysis. Available at: http://eulawanalysis.blogspot.com/2015/12/zakharov-v-russia-mass-surveillance-and.html [Accessed 5 Jan. 2022].

[13] Ermoshina, K., Loveluck, B., & Musiani, F. (2021). A market of black boxes: The political economy of Internet surveillance and censorship in Russia. *Journal of Information Technology & Politics*, 1-16.

[14] Peers, S. (2015). EU Law Analysis: Zakharov v Russia: Mass Surveillance and the European Court of Human Rights. [online] EU Law Analysis. Available at: http://eulawanalysis.blogspot.com/2015/12/zakharov-v-russia-mass-surveillance-and.html [Accessed 5 Jan. 2022].

[15] Ferreira, E.G., Freitas, M.S. da R., Pinto, J.A. da R. and Sisquini, G.R. (2019). SORM DG - an efficient SORM based on differential geometry. REM - International Engineering Journal, 72(4), pp.589–600.

[16] Anon, (2018). How Russian Internet Surveillance Operates | Cassandra Voices. [online] Available at: https://cassandravoices.com/law/how-russian-internet-surveillance-operates/ [Accessed 5 Jan. 2022].

[17] DeNardis, L. (2014). *The global war for Internet governance*. New Haven, CT: Yale University Press

***[18]** “What is Deep Packet Inspection? How It Works, Use Cases for DPI, and More”, Chris Brook, December 5, 2018, https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more

*[19] Fortinet. (n.d.). What Is Deep Packet Inspection (DPI)? [online] Available at: https://www.fortinet.com/resources/cyberglossary/dpi-deep-packet-inspection [Accessed 5 Jan. 2022].

*[20] dgap.org. (2021). Deciphering Russia's "Sovereign Internet Law" | DGAP. [online] Available at: https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law [Accessed 28 Mar. 2021].

[21] Joshi, A., Narayanan, S.N. and Mittal, S. (n.d.). Russians hack home internet connections – here's how to protect yourself. [online] The Conversation. Available at: https://theconversation.com/russians-hack-home-internet-connections-heres-how-to-protect-yourself-95907 [Accessed 5 Jan. 2022].

*[22] Novel imaging technique: DPI and 3-D-DPI versus CFI in liver disease. (1995). Gastroenterology, 108(4), p.A1070.

*[23] Anon, (n.d.). What is Deep Packet Inspection? How it Works and Why It Is Important | Endpoint Protector. [online] Available at: https://www.endpointprotector.com/blog/what-is-deep-packet-inspection-how-it-works-and-why-it-is-important/ [Accessed 18 Mar. 2021].

[24] "Russia issues new state contract to monitor and categorize social media and news reports", 07 May 2019, https://meduza.io/en/news/2019/05/07/russia-issues-new-state-contract-to-monitor-and-categorize-social-media-and-news-reports, Accessed 17 December 2021.

[25] "Rush at the troll factory", Meduza, 20 January 2021, https://meduza.io/feature/2021/01/20/na-fabrike-trolley-avral, Accessed 17 December 2021.

[26] "Throttling Twitter traffic in Russia Here's how Moscow's regulators are doing it and why it's not working," Meduza, March 12, 2021, https://meduza.io/en/cards/throttling-twitter-traffic-in-russia,Accessed 17 December 2021.

[27] Vittoria Elliott, “How the Russian government accidentally blocked its own websites,” Rest of World, March l2021. https://restofworld.org/2021/how-the-russian-government-accidentally-bl…

[28] “We got to the subway”, Opposition in Russia, 14 May 2021, https://www.kommersant.ru/doc/4814830

*[29] Malyshkin, A.V. (2019). Specialized Courts in the Context of the Differentiation and Integration of Court Jurisdictions. Vestnik Tomskogo gosudarstvennogo universiteta, (446), pp.240–246.

*[30] “Freedom on the Net 2021: Russia”, Freedom House, https://freedomhouse.org/country/russia/freedom-net/2021#footnote2_sb1qn13

*[31] “Constitution of the Russian Federation,” Constitution, Law, and Statutes: Government of the Russian Federation, Accessed June 16, 2021, http://archive.government.ru/eng/gov/base/54.html

*[32] “Peter Tolstoy: The law on foreign agents is dust from ants” [in Russian], RosKomSvoboda, January 12, 2019, https://roskomsvoboda.org/35097/

[33] Svetlana Prokopyeva, “Pskov journalist Svetlana Prokopyeva was included in the list of extremists and terrorists” [in Russian], MediaZona, July 4, 2019, https://zona.media/news/2019/07/04/prokopieva-spisok

*[34] "CASE OF ROMAN ZAKHAROV v. RUSSIA (Application no. 47143/06)". *HUDOC – European Court of Human Rights*. Retrieved 2021-12-17.

[35] Fisher, D., Maimon, D. and Berenblum, T. (2021). Examining the crime prevention claims of crime prevention through environmental design on system-trespassing behaviors: a randomized experiment. Security Journal.

[36] Galperin, D.O. and E. (2016). Russia Asks For The Impossible With Its New Surveillance Laws. [online] Electronic Frontier Foundation. Available at:

https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws [Accessed 10 Dec. 2021].

[37] Src='https://Secure.gravatar.com/Avatar/?s=32, img A., #038;d=mm, Srcset='https://Secure.gravatar.com/Avatar/?s=64, 038;r=g', #038;d=mm and says, 038;r=g 2x' class='avatar avatar-32 photo avatar-default' height='32' width='32' loading='lazy'/> X. contribuye a la C. de los D. y D.D. para C. (2015). Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's Schrems judgment. [online] Strasbourg Observers. Available at: https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/ [Accessed 5 Jan. 2022].

[38] Src='https://Secure.gravatar.com/Avatar/?s=32, img A., #038;d=mm, Srcset='https://Secure.gravatar.com/Avatar/?s=64, 038;r=g', #038;d=mm and says, 038;r=g 2x' class='avatar avatar-32 photo avatar-default' height='32' width='32' loading='lazy'/> X. contribuye a la C. de los D. y D.D. para C. (2015). Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's Schrems judgment. [online] Strasbourg Observers. Available at: https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/ [Accessed 5 Jan. 2022].

[39] data.guardint.org. (n.d.). Zakharov v Russia • Page 7 • Surveillance Oversight Database. [online] Available at: https://data.guardint.org/en/entity/hzbmni4o7ie?file=1601043095114mzz103jbfts.pdf&searchTerm=opportun&page=7 [Accessed 5 Jan. 2022].

[40] https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/

*[41] Council of Europe. (2016). Convention for the Protection of Human Rights and Fundamental Freedoms. In *Council of Europe Treaty Series 005*. Council of Europe.

[42] Global Privacy & Security Compliance Law Blog. (2016). “Yarovaya” Law - New Data Retention Obligations for Telecom Providers and Arrangers in Russia. [online] Available at: https://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/.

[43] Global Privacy & Security Compliance Law Blog. (2016). “Yarovaya” Law - New Data Retention Obligations for Telecom Providers and Arrangers in Russia. [online] Available at: https://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/.

Chapter 4-

[1] Penney, Jonathon, The Cycles of Global Telecommunication Censorship and Surveillance (2014). Santa Clara Law School - High Tech Law Institute, Internet Law Work-In-Progress Paper Series No.3, March, 2014, University of Pennsylvania Journal of International Law, Vol. 36, No. 3, 2015.

[2] Penney, Jonathon, The Cycles of Global Telecommunication Censorship and Surveillance (2014). Santa Clara Law School - High Tech Law Institute, Internet Law Work-In-Progress Paper Series No.3, March, 2014, University of Pennsylvania Journal of International Law, Vol. 36, No. 3, 2015.

[3] Akbari, A., & Gabdulhakov, R. (2019). Platform surveillance and resistance in Iran and Russia: The case of Telegram. *Surveillance & Society*, *17*(1/2), 223-231.

[4] Akbari, A., & Gabdulhakov, R. (2019). Platform surveillance and resistance in Iran and Russia: The case of Telegram. *Surveillance & Society*, *17*(1/2), 223-231.

[5] Akbari, A., & Gabdulhakov, R. (2019). Platform surveillance and resistance in Iran and Russia: The case of Telegram. *Surveillance & Society*, *17*(1/2), 223-231.

[6] Tanczer, L. M., McConville, R., & Maynard, P. (2016). Censorship and surveillance in the digital age: The technological challenges for academics. *Journal of Global Security Studies*, *1*(4), 346-355.

[7] Radchenko, D. (2020). Roskomnadzor-chan and Other Beings: Performative Practices and Folklore Reaction to the Telegram Lockout. *Etnograficheskoe obozrenie*, (3), 24-37.

*[8] Etling, B., Alexanyan, K., Kelly, J., Faris, R., Palfrey, J. G., & Gasser, U. (2010). Public discourse in the Russian blogosphere: Mapping RuNet politics and mobilization. *Berkman Center Research Publication*, (2010-11).

[9] Shama, A., & Merrell, M. N. (1997). Russia's true business performance: Inviting to international business?. *Journal of World Business*, *32*(4), 320-332.

*[10] Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. *Policy Brief, Democracy and Disorder Series (Washington, DC: Brookings, 2019)*, 1-22.

[11] Sivetc, L. (2019). State regulation of online speech in Russia: The role of internet infrastructure owners. *International Journal of Law and Information Technology*, *27*(1), 28-49.

[12] Zharova, A. (2019). Ensuring the Information Security of Information Communication Technology Users in Russia. *International Journal of Cyber Criminology*, *13*(2).

[13] Shcherbovich, A. A. (2021). National Sovereignty, Security, and Internet Governance: Impact on Constitutional Principles and Challenges for the Human Rights of Internet Users. In *Virtual Freedoms, Terrorism and the Law* (pp. 173-189). Routledge.

[14] Zharova, A. (2020). The protect mobile user data in Russia. *International Journal of Electrical and Computer Engineering*, *10*(3), 3184.

[15] Sanovich, S. (2017). Computational propaganda in Russia: the origins of digital misinformation.

[16] Marklund, A. (2016). Listening for the state: censoring communications in Scandinavia during World War I. *History and Technology*, *32*(3), 293-314.

[17] Rudnik, A. (2020). Why do bloggers keep silent? Self-censorship in social media: cases of Belarus and Russia.

[18] Lü, Q., & Low, B. K. (2011). Probabilistic analysis of underground rock excavations using response surface method and SORM. *Computers and Geotechnics*, *38*(8), 1008-1021.

*[19] Federation, R. (2000). Information Security Doctrine of the Russian Federation. United Nations International Telecommunications Union (ITU) Archive.

[20] Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. *Policy Brief, Democracy and Disorder Series (Washington, DC: Brookings, 2019)*, 1-22.

[21] Klyueva, A. (2016). Taming online political engagement in Russia: Disempowered publics, empowered state and challenges of the fully functioning society. *International Journal of Communication*, *10*, 20.

[22] Penney, J. W. (2014). The cycles of global telecommunication censorship and surveillance. *U. Pa. J. Int'l L.*, *36*, 693.

[23] Stoycheff, E., Burgess, G. S., & Martucci, M. C. (2020). Online censorship and digital surveillance: the relationship between suppression technologies and democratization across countries. *Information, Communication & Society*, *23*(4), 474-490.

[24] Herasimenka, A. (2018). Responding to Democratic Decay: Large-Scale Political Campaigning on Social Media in Russia.

[25] Ermoshina, K., Loveluck, B., & Musiani, F. (2021). A market of black boxes: The political economy of Internet surveillance and censorship in Russia. *Journal of Information Technology & Politics*, 1-16.

*[26] Sherman, J. (2021). Digital Authoritarianism and Implications for US National Security. *The Cyber Defense Review*, *6*(1), 107-118.

[27] Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. *Media and Communication*, *5*(1), 29-41.

[28] Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. *Media and Communication*, *5*(1), 29-41.

[29] Ciani, J. (2019). Outside the GDPR: challenges in ensuring an effective protection of personal data: the Russian case. *Outside the GDPR: challenges in ensuring an effective protection of personal data: the Russian case*, 37-60.

[30] Feldstein, S. (2019). Artificial intelligence and digital repression: Global challenges to governance. *Available at SSRN 3374575*.

[31] Sherstoboeva, E. (2020). Regulation of online freedom of expression in Russia in the context of the Council of Europe standards. In *Internet in Russia: A study of the runet and its impact on social life* (pp. 83-100). Springer.

[32] Rosenberg, W.G., 2014. Reading Soldiers' Moods: Russian Military Censorship and the Configuration of Feeling in World War I. *The American Historical Review*, *119*(3), pp.714-740.

[33] Etling, B., Alexanyan, K., Kelly, J., Faris, R., Palfrey, J. G., & Gasser, U. (2010). Public discourse in the Russian blogosphere: Mapping RuNet politics and mobilization. *Berkman Center Research Publication*, (2010-11).

[34] Herasimenka, A. (2018). Responding to Democratic Decay: Large-Scale Political Campaigning on Social Media in Russia.

[35] Feldstein, S. (2019). Artificial intelligence and digital repression: Global challenges to governance. *Available at SSRN 3374575*.

[36] Geybulla, A. (2021). Uncensored journalism in censored times: Challenges of reporting on Azerbaijan. *Journalism*, 14648849211036872.

[37] Niaki, A. A., Cho, S., Weinberg, Z., Hoang, N. P., Razaghpanah, A., Christin, N., & Gill, P. (2020, May). ICLab: A Global, Longitudinal Internet Censorship Measurement Platform. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 135-151). IEEE.

*[38] Sliesarieva, A. (2020). The Defender vs. the Censor: CDA Analysis of 2017 Russian Web-Source Ban in Ukraine.

[39] David, M. (2017). Russia's challenge to US hegemony and the implications for Europe. In *American hegemony and the rise of emerging powers* (pp. 198-215). Routledge.

[40] DeNardis, L. (2013). Multi-stakeholderism: The internet governance challenge to democracy. *Harvard International Review*, *34*(4), 40.

[41] Akbari, A., & Gabdulhakov, R. (2019). Platform surveillance and resistance in Iran and Russia: The case of Telegram. *Surveillance & Society*, *17*(1/2), 223-231.

[42] Penney, Jonathon, The Cycles of Global Telecommunication Censorship and Surveillance (2014). Santa Clara Law School - High Tech Law Institute, Internet Law Work-In-Progress Paper Series No.3, March, 2014, University of Pennsylvania Journal of International Law, Vol. 36, No. 3, 2015, Available at SSRN: https://ssrn.com/abstract=2398491 or http://dx.doi.org/10.2139/ssrn.2398491

[43] Nizzoli, Leonardo. (2021). LEVERAGING SOCIAL MEDIA AND AI TO FOSTER SECURE SOCIETIES AGAINST ONLINE AND OFFLINE THREATS. 10.13140/RG.2.2.29807.97446.

[44] Sliesarieva, A. (2020). The Defender vs. the Censor: CDA Analysis of 2017 Russian Web-Source Ban in Ukraine.

[45] Sliesarieva, A. (2020). The Defender vs. the Censor: CDA Analysis of 2017 Russian Web-Source Ban in Ukraine (Dissertation)

[46] Geybulla, A. (2021). Uncensored journalism in censored times: Challenges of reporting on Azerbaijan. *Journalism*, 14648849211036872.

[47] Geybulla, A. (2021). Uncensored journalism in censored times: Challenges of reporting on Azerbaijan. *Journalism*, 14648849211036872.

[48] Sherstoboeva, E. (2020). Regulation of online freedom of expression in Russia in the context of the Council of Europe standards. In *Internet in Russia: A study of the runet and its impact on social life* (pp. 83-100). Springer.

[49] Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. *Media and Communication*, *5*(1), 29-41

[50] Sherstoboeva, E. (2020). Regulation of online freedom of expression in Russia in the context of the Council of Europe standards. In *Internet in Russia: A study of the runet and its impact on social life* (pp. 83-100). Springer.

[51] Ciani, J. (2019). Outside the GDPR: challenges in ensuring an effective protection of personal data: the Russian case. *Outside the GDPR: challenges in ensuring an effective protection of personal data: the Russian case*, 37-60.

[52] Ciani, J. (2019). Outside the GDPR: challenges in ensuring an effective protection of personal data: the Russian case. *Outside the GDPR: challenges in ensuring an effective protection of personal data: the Russian case*, 37-60.

Chapter 5

[1] Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, *91*(1), 111-130.

*[2] Data collected on http://www.internetworldstats.com (as of 15 Feb. 2014), accessed 20 Dec. 2021. See also David Dean, Sebastian Digrande, Dominic Field, Andreas Lundmark, James O'Day, John Pineda and Paul Zwillenberg, The $4.2 trillion opportunities: the internet economy in the G-20 (Boston: Boston Consulting Group, March 2012).

[3] Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. *Media and Communication*, *5*(1), 29-41.

*[4] Andrei Soldatov and Irina Borogan, ‘The Russian establishment’s new internet surveillance plan go live today’, Wired, 1 Nov. 2012.

[5] Julien Nocetti, ‘“Digital Russian establishment”: power and the internet in Russia’, Russie.NEI.Visions, no. 59 (Paris: Institut français des relations internationales, April 2011), p. 9.

[6]“Everything you need to know about Ukraine crisis”, Max Fisher, 3 September 2014, https://www.vox.com/2014/9/3/18088560/ukraine-everything-you-need-to-know

*[7]Aliaksandrau, A. (2014). Brave new war: The information war between Russia and Ukraine. *Index on censorship*, *43*(4), 54-60.

[8] Mejias, U. A., & Vokuev, N. E. (2017). Disinformation and the media: the case of Russia and Ukraine. *Media, culture & society*, *39*(7), 1027-1042.

*[9] “Russian Cyber Espionage Campaign – Sandworm Team.”

[10] David E. Sanger and Steven Erlanger, “Suspicion Falls on Russia as ‘Snake’ Cyberattacks Target Ukraine’s Government,” New York Times, March 8, 2014, http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html.

[11] Robert Lipovsky and Anton Cherepanov, “Operation Potao Express,” ESET Report (July 2015): 9-13.

[12] Petro Zamakis, “Cyber Wars: The Invisible Front,” Ukraine Investigation, April 24, 2014, http://ukraineinvestigation.com/cyber-wars-invisible-front/.

[13] CyberBerkut, http://cyber-berkut.org/en/.

[14] “Hackers Target Ukraine’s Election Website,” Agence France-Presse, October 25, 2014, http://www.securityweek.com/hackers-target-ukraines-election-website.

[15] Jen Weedon and Laura Galante, “Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not So Fast.” FireEye Blogs, March 12, 2014,

https://www.fireeye.com/blog/executive-perspective/2014/03/intel-analysts-dissect-the-headlines-russia-hackers-cyberwar-not-so-fast.html.

[16] Max Cherney, “Pro-Russian Hackers Took Down Three NATO Websites,” Motherboard, March 16, 2014, http://motherboard.vice.com/blog/pro-russia-ukranians-hack-nato-websites; and Thomas Barrabi, “NATO Not Responsible For Ukraine's Security From Russia, Should Focus On Member Nations, Latvian Envoy Says,” International Business Times, May 6, 2015, http://www.ibtimes.com/nato-not-responsible-ukraines-security-russia-should-focus-member-nations-latvian-1910551.

*[17] Sacha Dov Bachmann and Hakan Gunneriusson, “Russia’s Hybrid Warfare in the East: The Integral Nature of the Information Sphere,” Georgetown Journal of International Affairs: International Engagement on Cyber V (2015): 199-200.

[18] Sacha Dov Bachmann and Hakan Gunneriusson, “Russia’s Hybrid Warfare in the East: The Integral Nature of the Information Sphere,” Georgetown Journal of International Affairs: International Engagement on Cyber V (2015): 199-200.

[19] Jill Dougherty, “Everyone Lies: The Ukraine Conflict and Russia’s Media Transformation,” Discussion Paper Series, Shorenstein Center on Media, Politics, and Public Policy (July 2014): 2-29.

[20] Linvill, D. L., Boatwright, B. C., Grant, W. J., & Warren, P. L. (2019). “THE RUSSIANS ARE HACKING MY BRAIN!” investigating Russia's internet research agency’s Twitter tactics during the 2016 United States presidential campaign. *Computers in Human Behavior*, *99*, 292-300.

[21] Barberá, P., Jost, J. T., Nagler, J., Tucker, J. A., & Bonneau, R. (2015). Tweeting from left to right: Is online political communication more than an echo chamber. Psychological Science, 26, 1531–1542. https://doi.org/10.1177/0956797615594620.

[22] Stewart, L. G., Arif, A., & Starbird, K. (2018). Examining trolls and polarization with a retweet network. In: Proc. ACM WSDM, workshop on misinformation and misbehaviour mining on the web

[23] Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. The Journal of Economic Perspectives, 31, 211–236. https://doi.org/10.1257/jep.31.2.211.

*[24] Council on Foreign Relations (2017) Clinton on the issues: Russia. https://www:cfr:org/interactives/campaign2016/Hillary-clinton/on-russia.

*[25] (Nocetti, 2014) The Global Internet is Disintegrating. What comes next? https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next

*[26] Contest and Conquest: Russia and Global Internet Governance https://www.chathamhouse.org/sites/default/files/field/field_publication_docs/INTA91_1_07_Nocetti.pdf

*[25] Bloomberg (2018) Russians Staged Rallies For and Against Trump to Promote Discord, Indictment Says. Fortune, February 17, http://fortune:com/2018/02/17/russian-organized-rallies-election-meddling/.

[26] Golovchenko, Y., Buntain, C., Eady, G., Brown, M. A., & Tucker, J. A. (2020). Cross-platform state propaganda: Russian trolls on Twitter and YouTube during the 2016 US presidential election. *The International Journal of Press/Politics*, *25*(3), 357-389.

[27] Yin L, Roscher F, Bonneau R, Nagler J and Tucker JA (2018) Your friendly neighborhood troll: The internet research agency's use of local and fake news in the 2016 us presidential election.

[28] (Limonier, 2014) Russia in Cyberspace: Issues and Representations https://www.cairn-int.info/article-E_HER_152_0140--russia-in-cyberspace-issues.htm?contenu=article

Other references

Anderson, Robert, Tora Bikson, Sally Ann Law and Bridger Mitchell (1995), "Uni versal Access to E-mail: Feasibility and Societal Implications." Rand Corporations Paper.
Arendt, Hannah (1960), "Freedom and Politics." Chicago Review 14(1):18–46. Reprinted in Liberty, edited by David Miller (Oxford: Oxford University Press, 1991).

Arnold, R. Douglas (1992), The Logic of Congressional Action. New Haven: Yale University Press.

Bimber, Bruce (1998), "The Internet and Political Transformation: Populism, Community and Accelerated Pluralism." Polity 31(1):133–160.

Bimber, Bruce (2000), "Measuring the Gender Gap on the Internet." Social Science Quaterly 81:868–876.

Boreiko, Aleksander and Pavel Nefedov (2000), "Cabinet Approves E-Russia Plan." The Moscow Times . July 2001.

Boreiko, Alexander (2001), "Law Change May Put RuNet Names in Peril." The Moscow Times . December 19.

Brown, Archie (2001), "From Democratisation to 'Guided Democracy'." Journal of Democracy 12(4):35–41. Part of the symposium" Ten Years After the Soviet Breakup".
Brown, Nancy and Jeff Wright. 1997. "Information Technology in the Russian Federation." www.american.edu/initeb/nb2224a/russia.html .

Brzezinski, Zbignew (2001),“The Primacy of History and Culture.” Journal of Democracy 12(4):20–26. Part of the symposium "Ten Years After the Soviet Breakup".
Bucy, Erik. 2000. "Social Access to the Internet." Harvard International Journal

of Press and Politics 5:50–61.

Diamond, Larry, Juan J. Linz and Seymour Martin Lipset (1990), Politics in Developing Countries: Comparing Experiences with Democracy. Boulder, Colo.: Lynne Rienner Publishers.

DiMaggio, Paul, Eszter Hargittai, W. Russell Neuman and John P. Robinson (2001), "Social Implications of the Internet." Annual Review of Sociology 27:307–336.
Doctrine of Information Security of the Russian Federation (2000), Doktrina Infor macionnoy bezopasnosti Rossiyskoi Federacii. Adopted September 9, 2000. Refered to as the Information Security Doctrine. Published in Rossiskaya Gazeta, September 8, 2000. Reprinted in Russian Media Challenge, edited by Kaarle Nordenstreng, Elena Vartanova, and Yassen Zassoursky, Helsinki: Kikimora Publications, 2001

Dunlop, John B (2001) Sifting through the Rubble of the Yeltsin Years. In Con temporary Russian Politics: A Reader, ed. Archie Brown address =. Oxford University Press.
Dutton, William H (1999), Society on the Line: Information Politics in the Digital Age. Oxford: Oxford University Press.

Ellis, Frank(1999), From Glasnost to the Internet: Russia's New Infosphere. Lon don: Macmillan.

Federal Law Concerning Communications (1995), Federalnyy zakon o svyazi. Adopted February 20, 1995. Refered to as the Law on Communications.
Fishkin, James (1991), Democracy and Deliberation: New Directions for Democratic Reform. New Haven: Yale University Press.

Foster, Frances H (1996), "Information and the Problem of Democracy: The Rus sian Experience." American Journal of Comparative Law 44:243. Reprinted in Russian Media Law and Policy in the Yeltsin Decade: Essays and Documents, edited by Monroe E. Price, Andrei Richter and Peter K. Yu (The Hague: Kluwer Law International, 2002), pp 95-118.

Hindman, Matthew (2002), "The Liberal Medium? The Political Correlates of Web Use.". Paper prepared for delivery at the 2002 Annual Meeting of the American Political Science Association, Boston, August 29-September 1, 2002.

Hoffman, Donna L., Thomas P. Novak and Ann E. Schlosser (2002), "The Evolution of the Digital Divide: How Gaps in Internet Access May Impact Electronic Commerce." Journal of Computer-Mediated Communication .

Dunlop, John B (2001), Sifting through the Rubble of the Yeltsin Years. In Con temporary Russian Politics: A Reader, ed. Archie Brown address =. Oxford University Press.
Dutton, William H (1999), Society on the Line: Information Politics in the Digital Age. Oxford: Oxford University Press.

Ellis, Frank (1999), From Glasnost to the Internet: Russia's New Infosphere. Lon don: Macmillan.

Federal Law Concerning Communications (1995), Federalnyy zakon o svyazi. Adopted February 20, 1995. Refered to as the Law on Communications.

Fishkin, James (1991), Democracy and Deliberation: New Directions for Democratic Reform. New Haven: Yale University Press.

Foster, Frances H (1996), "Information and the Problem of Democracy: The Rus sian Experience." American Journal of Comparative Law 44:243. Reprinted in Russian Media Law and Policy in the Yeltsin Decade: Essays and Documents, edited by Monroe E. Price, Andrei Richter and Peter K. Yu (The Hague: Kluwer Law International, 2002), pp 95-118.

Hindman, Matthew (2002), "The Liberal Medium? The Political Correlates of Web Use.". Paper prepared for delivery at the 2002 Annual Meeting of the American Political Science Association, Boston, August 29-September 1, 2002.

Hoffman, Donna L., Thomas P. Novak and Ann E. Schlosser (2002), "The Evolution of the Digital Divide: How Gaps in Internet Access May Impact Electronic Commerce." Journal of Computer-Mediated Communication

Horkeimer, Max and Theodor W. Adorno (1972), The Cutlture Industry: Englight enment as Mass Deception. In Dialectic of Enlightenment, ed. Max Horkeimer and Theodor W. Adorno. New York: Seabury Press. Translated by John Cumming.

Hughes, James (2001), From Federlisation to Recentralisation. In Developments in Russian Politics 5, ed. Stephen White, Alex Pravda and Zvi Gitelman. Carnegie Endowment for International Peace.

Huntington, Samuel P (1991), The Third Wave: Democratisation in the Late Twen tieth Century. Norman: University of Oklahoma Press.

Huskey, Eugene (2001), Overcoming the Yeltsin Legacy: Vladimir Putin and Rus sian Political Reform. In Contemporary Russian Politics: A Reader, ed. Archie Brown. Oxford: Oxford University Press.

Law of the Russian Federation Concerning the Legal Storage of Computer Programs and Data Bases (1992), Zakon Rossiyskoy Federatsii o pravovoy okhrane program dlya elektronnykh vychislitel'nykh mashin i baz dannykh. Adopted September 23, 1992. Reffered to as the Law on Databases.

Mansbridge, Jane J (1980), Beyond Adversary Democracy. New York: Basic Books.
Margolis, Michael and David Resnick (2000), Politics as Usual: The Cyberspace "Revolution". Thousand Oaks: Sage Publications.

Martin Malia, Jack Matlock Jr., Jerry Hough Geoffrey Hosking Alexey Pushkov Robert Legvold and Henry Trofimenko (2002), “Odom’s Russia: A Forum.” The National Interest (66):114. Winter.

McFaul, Michael (2001), Russia's Unfinished Revolution: Political Change from Gorbachev to Putin. Ithaca and London: Cornell University Press.

MMLPC, Moscow Media Law Policy Center (2000), "CEC Waffles on Whether Internet is Mass Media." Commentary by the Moscow Media Law and Policy Center . March.
MMLPC, Moscow Media Law Policy Center (2000), "Is the Internet Independent of the Law on Elections?" Commentary by the Moscow Media Law and Policy Center . February.

Mulvey, Stephen (2001), "Russian Internet Politics." BBC News . March 5, news.bbc.co.uk

Norris, Pippa (1999), Who Surfs? New Technology, Old Voters and Virtual Democ racy. In democracy.com: Governance in a Networked World, ed. Elaine Ciulla Kamarck and Jr. Joseph S. Nye. Hollis, NH:: Hollis Publishing.

Norris, Pippa (2001), Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide. Cambrdige: Cambrdige University Press.

NTIA (2000), Falling Through the Net: Toward Digital Inclusion. Washington, D.C.: U.S. Department of Commerce.

NTIA (2002), A Nation Online: How Amercians are Expanding Their Use of the Internet. Washington, D.C.: U.S. Department of Commerce.

NYT, The New York Times (2000), "Reforms Russia Needs." The New York Times . Editorial. January 7.

Odom, William E (2001), "Realism about Russia." The National Interest (65):56. Fall.

Ognev, Maxim (2001), "Site of the Week: State-Sponsored Web Site Takes War on Drugs Online." The Moscow Times . October 3.

Palma, Giuseppe Di (1990), To Craft Democracies: An Essay on Democratic Tran sitions. Berkeley: University of California Press.

Price, Monroe E (1995), "Law, Force, and the Russian Media." Cardozo Arts & Entertainment Law Journal 13:795. Reprinted in Russian Media Law and Policy in the Yeltsin Decade: Essays and Documents, edited by Monroe E. Price, Andrei Richter and Peter K. Yu (The Hague: Kluwer Law International, 2002), pp 31-46.

Price, Monroe E. and Peter Krug (2000), Enabling Environment for Free and Independent Media. University of Oxford: Programme in Comparative Media Law & Policy.

Przeworski, Adam (1991), Democracy and the Market: Political and Economic Re forms in Eastern Europe and Latin America. Cambridge: Cambridge University Press.

Przeworski, Adam (1999), Minimalist Conception of Democracy: A Defence. In Democracy's Value, ed. Ian Shapiro and Casiano Hacker-Cordon. Cambridge: Cambridge University Press.

Putnam, Robert D (1993), Making Democracy Work: Civic Traditions in Modern Italy. Princeton: Princeton University Press

Putnam, Robert D (2000), Bowling Alone: The Collapse and Rivaval of American Community. New York: Simon and Schuster.

Rheingold, Howard (1993), The Virtual Community: Homesteading on the Elec tronic Frontier. Reading, Mass.: Addison Wesley.

ROCIT, Russian Non-Profit Center For Internet Technologies (1999), "How many on line.".

Rozumilowicz, Beata (2002), Democratic Change: A Theoretical Perspective.
In Media Reform: Democratising the Media, Democratising the State, ed. Monore E. Price, Beata Rozumilowicz and Stefaan G. Verhulst. London and New York: Routledge pp. 9–26.
Schumpeter, Joseph (1942), Capitalism, Socialism, and Democracy. New York: Harper.

Selnow, Gary W (1998), Electronic Whistle-Stops: The Impact of the Internet on American Politics. Westport, Conn.: Praeger Publishers.

Seregina, Yelena (2001), "Reiman Wrestles With Communication Goals." The Moscow Times . May 15.

Shanetskaya, Natasha (2001), "Duma to Mull Over 15 Internet Bills." The Moscow Times . January 31.

Shevtsova, Lilia (2001), Conclusion. In Gorbachev, Yeltsin, and Putin, ed. Archie Brown and Lilia Shevtsova. Carnegie Endowment for International Peace.

Shlapentokh, Vladimir (2001), "Putin's First Year in Office: The New Regime's Uniqueness in Russian History." Communist and Post-Communist Studies 34:371–399.
Smetko, Holli A. and Natalya Krasnoboka. Forthcoming. "The Political Role of the Internet in Societies in Transition." Party Politics . Draft copy of the paper on file with the authors.

Statute Concerning the Committee Attached to the Presidential Office on the Pol icy of Informatization (1994), Polozhenie o Komitete pri Prezidente Rossiyskoy Federatsii po politike informatizatsii. Adopted February 17, 1994. Refered to as the Roskominform Statute.

The Federal Law Concerning Information, Informatization and the Protection of Information (1995), Federalnyy zakon ob informatsii, informatizatsii I zashchite informatsii. Adopted January 25, 1995. Refered to as the Law on Information.

The Federal Law Concerning Participation in the International Information Ex
change (1996), Federalnyy zakon ob uchastii v mezhdunarodnom informatsionnom obmene. Adopted June 5, 1996. Refered to as the Law on Information Exchange.

Tracy, Jen and Matt Bivens (2000), "Profile: Putin's Patronage Lifts Ex-Dissident Persecutor." The Moscow Times . February 24.

Warren, Marcus (1998), "Connected: Russian Spies Target Web." The Daily Tele
graph . August 6.

Wilhelm, Anthony G (2000), Democracy in the Digital Age: Challenges to Political Life in Cyberspace. Oxford: Routledge.

Wines, Michael (2000), "Path to Power: A Political Profile: Putin Steering to Reforms, But with Soviet Discipline." The New York Times . February 20.

Wolfe, Elizabeth(2001), "Ministries Vie for E-Russia Control." The Moscow Times . September.

Wresch, William (1996), Disconnected: Haves and Have-Nots in the Information Age. Rutgers: Rutgers University Press.

Yurchak, Alexi (1997), "The Cynical Reason of Late Socialism: Power, Pretense, and the Ankdot." Public Culture 9(2):161–188