From Analog to Digital Control: A Study of the Russian Experience with Communications Technologies

THESIS

Presented in Partial Fulfillment of the Requirements for the Degree Master of Arts in the Graduate School of The Ohio State University

By

Kathryn E. Johnson

Graduate Program in Slavic and East European Studies

The Ohio State University

2014

Master's Examination Committee:

Jessie Labov, Advisor

Jennifer Suchland

Jeffrey Lewis

Abstract

A culture of control existed in Russia that possesses roots in the tsarist period and continued into the Soviet era. The desire to control evolved to protect and promote the state, as well as to ensure a monopoly over truth; thus communications technologies, because of their ability to transmit information through various means, became a target of this control. This thesis examines the current attempts to recapture a culture of control in Russia in response to the growth of the Internet and social media. It will assess the parallels between the past and present methods of control and conclude that modern methods of control are reminiscent of previous styles of controls. While the intent to control communication is also characteristic of the Soviet period, more modern methods have evolved to control access to information in the post-Soviet context, specifically developed to address the Internet environment and to prevent backlash. Thus, instead of outright control and censorship, methods of control exhibited include second and third generation techniques such as legal regulation, surveillance, and government propaganda. The practice of facilitating the spread of the Internet throughout Russia while maintaining the desire to control it represents an older dichotomy of seeking a modern state infrastructure, while fearing its potential for subversion and instability. This thesis will also explore the difference between the terms *control* and *surveillance*, as surveillance is important for the government's control over communication through knowledge of information flow, and is facilitated by the growth of cellular technology and computer networks today. Finally, the thesis will assess the reasons for recapturing past methods of control and will conclude that the state seeks to control communications not only for political reasons, but also for national security reasons, which may be both real and imagined. There are also efforts to shape the Russian population into a more moral and stable society. The government seeks to do this by ensuring its voice is heard and its hand is seen in one of the only remaining mediums that remains out of the government's full control.

Dedication

I dedicate this thesis to those friends and family who have supported me throughout my endeavors academic or otherwise. And to my love Edwin, without his help and support, this thesis would have seemed undoable.

Acknowledgments

I wish to acknowledge and express deep gratitude to my advisor Dr. Jessie Labov for her help and advice in bringing this project together. I also wish to express gratitude to my committee members Dr. Jennifer Suchland and Dr. Jeffrey Lewis for their assistance and helpful comments.

Vita

2011	International Summer School, University of Stirling
2012	B.A. International Studies, The Ohio State University
2012 to Present	Graduate Student, Slavic and East European Studies, The Ohio State University

Fields of Study

Major Field: Slavic and East European Studies

Table of Contents

Introduction

Throughout recent Russian history, communications technologies have played a special role. On one hand they have been a means of spreading the message of Soviet superiority and of educating the masses in order to cultivate a distinct Soviet culture. On the other, they have been subject to control and suspicion throughout history to varying degrees due to their inherent potential to spread counterrevolutionary and dissident information. The experience with communications technologies represents the dilemma of the tsars and the Soviet state, who wanted modern infrastructure but also wanted to keep control over information. In addition to providing a comprehensive look at the development and control of the Internet space, this thesis will show that the current Russian government is experiencing issues with new communications technologies that exemplify the same dilemma expressed above. Russia wants and needs to develop its telecommunications and Internet sector to become a modernized state and a competitor on the world stage. Government officials continue to be suspicious, just as their Soviet predecessors were, of Western influence, which has brought the Internet into the discussion of national security policy due to the Internet's founding and popularity in the West. There are also calls for a distinctly Russianized internet in order to compete with the Western networks and to have the ability to host all sites locally. Officials also grow cautious of the Internet's power to spread dissident information, which could incite a segment of the population to cause instability in a nation still trying to recover from a long unstable period.

Continuities exist between the tsarist, Soviet, and current periods in regards to control over communications technologies. The most apparent similarities are the usage of government propaganda and the surveillance of communication networks. While the intent to control communication is reminiscent of previous periods, modern methods of controlling access to information have evolved for the post-Soviet context, and are specifically developed to deal with the Internet. These are known as 'second' and 'third generation' methods, and are more subtle and sophisticated than the outright censorship exhibited in the tsarist and Soviet periods. The evolution of methods of control has been a response to the horizontal (peer-to-peer) nature of the Internet, which fosters reciprocal rather than solely one-way communication, and the subsequent creation of a young and educated Internet culture of communication, which is inconsistent with Soviet style controls.

In order to understand the development of control over the Internet, it is important to grasp why the government wants to recapture control. This thesis will argue that while at first glance politics are the motivating factor behind the desire to control, this is a more complex issue because the state is also concerned about threats to national security, whether real or imagined. There is also a case to be made for a moral reasoning behind the control. The "internet blacklist law" targets child pornography, suicide, and drugs, something that is not related to politics or national security, but is reminiscent of the desire to mold and shape a moralistic and stable society. The Information Security

Doctrine of 2000 essentially spells out all of these rationales for control of the information sphere, with the subsequent passage of laws leading up to today reflecting these motivations and the general desire for a government hand in controlling the information sphere.

The differences and similarities between the terms “government” and “security” or “intelligence agencies” need to be clarified in this context. This thesis will look at methods used to control of Russian communications technologies, and at times it is hard to distinguish which body is carrying out the control. The intelligence services are normally seen as the primary organ of control. These organs of control conduct surveillance, and during Soviet times they would intimidate, investigate, and attempt to silence those deemed suspicious. However, the government is determining the policy and laws within which contexts the services work. Stalin’s NKVD, which was controlled by and answered to the leader, was really Stalin’s arm of control and enforcement rather than an independent entity. In talking about Internet controls today, which are increasingly becoming entrenched in the system through legitimate legal frameworks and enforced by communications agencies and police investigative forces, an analysis must include surveillance by intelligence agencies and de facto controls carried out by pro-regime forces. This effectively shows a government working in tandem with its security services.

This thesis will explore the culture of control that possesses roots in tsarist Russia and its relationship to communication system development and implementation, and access to information. Communication systems were not the sole focus of control, especially in the Soviet Union, however they played the role of both friend and foe in that the government could use these systems for one-way propagandistic purposes, while at the same time the systems could be used against the government. There was a fear for the spread of negative or dissident information, as well as the development of horizontal communication networks that would facilitate communication between citizens because these networks were harder to control. The thesis will investigate the efforts of the current government and security apparatus in the recapturing of this culture of control, namely those controls developed in response to the rise of computer networks, the Internet, and social media. A substantial piece of the thesis examines the Internet's burgeoning history and role in Russia today, along with the unique methods being developed to control it. The thesis will also establish the role of surveillance as separate from methods of direct control, even though it is a form of indirect control and signifies the desire for control through knowledge of information flow. There are three main research questions explored: 1. Are there parallels between Russia's past and present experiences with communication technologies, using the Internet as a key player for the present study?; 2. Is the government or are the security services attempting to control or use the Internet and social media for their own benefit?; and 3. If control is exhibited, why is the government interested in controlling the Internet space?

The first chapter examines the views towards communications technologies from the tsarist period through the Soviet era. Examined here are the types of communications technologies controlled, the forms of control, the role of communications technology vs. other science, and the role of ideology in decisions to control. It is crucial to study the history and context within which Russian communications technologies have found their basis. However, it is also important to keep in mind the differences between the tsarist government, the Soviet government, and today's regime, and thus this thesis is primarily interested in parallels between past and present, as well as the specific contexts within which technology has developed. This will be the focus, rather than an explicit argument that certain principles used today are distinctly Soviet or tsarist, or that the government today is deliberately harkening back to either period. This chapter also contains an overview of the development of the intelligence services, which served as the organ of control for the government.

The second chapter seeks to examine the information revolution that took place in the Gorbachev era and the cultural shift that ensued. The collapse of the Soviet Union and the cultural shift to a more open society with a desire for information and modern communication technologies is important to understanding the contexts in which the Internet formed. The information revolution marks a shift in attitudes towards government control, and also towards a more modern state that needs to grow with the rest of the world, experiencing at that time a substantial growth in the telecommunications and computer fields.

The third and fourth chapters provide a study of the Internet era in Russia. The third chapter is a brief overview of how the Internet developed in Russia and the distinct nature of the RuNet. This is important because today's society is increasingly globalized, and although Russia has many of the same technologies as the West and has borrowed or imported them to some extent, the Russian experiences with Internet development and the popular platforms are distinctly Russian. Throughout the thesis one can see the distinct Russian experience with communication technology in general; it is not that Russians had different technologies than the West, but rather that they develop at different rates, are practiced in different ways, and subject to different historical contexts. The fourth chapter will cover the Russian State's reaction to new online practices through regulation and the Intelligence Service's attempts to surveil and control the internet. The thesis will cover some of the attempts to regulate the information sphere and the Internet, with the main conclusion that there were few, if any, regulations directly affecting the Internet before the Putin administration. Today, laws focus on regulating extremist materials, regulating the Internet for moral and national security reasons, and forming a legal framework to give the government a hand in shaping Internet regulation.

The last chapters of the thesis will cover two specific case studies: the FSB's surveillance measure SORM, and the control of the unofficial leader of the political opposition, Alexei Navalny. These case studies serve two purposes. First, they outline some of the ways that the security services and the government seek to exert control over Internet activities. Second, they outline a distinction between surveillance and control. Surveillance is covert and thus it is hard to determine when it is being conducted. It signifies a need for control through knowledge over information flow, whether it is detrimental or not, rather than overt measures of control, which seek to control the information available and those who disseminate it for oppositional purposes.

Literature Review

This review of the secondary literature will consider recent work in several areas germane to the thesis: Communications Technology and the Information Revolution, Control, Surveillance, and the Intelligence Services. These fields often overlap, yet they are distinct areas with different disciplinary foci. The literature fits together to show the overall story of this thesis: a culture of control exists in Russia that dates back to the tsarist period and transcends into the Soviet period; there was a significant desire for control over communications and access to information, however control was not limited to this area. Communications technologies are an interesting case study for control in Russia because they represent the dichotomy between wanting a modern state and using the systems for the propagation of the Soviet ideal, and the fear of access to negative information or ease of communications that could undermine the government. Post-Soviet Russia then loses this control culture in regards to communications systems (though not within the security services) through policies of privatization and a push towards a consumer driven role in communication development. Currently, the Putin government desires to recapture control over communications and access to certain information in response to the growth of the Internet and social media using covert or legal means of control rather than through direct and widespread censorship. Another theme important to the thesis that the secondary literature covers is the difference between the concepts of surveillance and control, and how the concept of surveillance signifies the desire for control over information flow rather than control over content.

Communications Technologies and the Information Revolution

The Soviet Union/Russia has a rich history in communications technologies, although much of this history is characterized by government control over these systems and the information they transmit. Thus, it is crucial to examine the secondary literature on communications technologies' role in the Soviet Union/Russia and what types of control methods were used on these technologies in order to understand the linkages between communication and control, as well as the role that communications technologies played in bringing information to the people in order to drive the information revolution.

For this section, the thesis will compare and contrast four important works that contribute to the story of the Russian/Soviet experience with communications technology: Scott Shane's *Dismantling Utopia*, Terhi Rantanen's *The Global and the National: Media and Communications in post-Communist Russia*. Kristin Roth Ey's *Moscow Prime Time: How the Soviet Union Built the Media Empire that Lost the Cultural Cold War,* and Frederick Starr's chapter in *Science & The Soviet Social Order* entitled *New Communications Technologies & Civil Society*.

In *Dismantling Utopia*, Scott Shane (1994) writes a narrative of communication technologies and information's role in Soviet society and their implementation, but he does not delve into the development of each communications technology in the Soviet Union. Shane contends the Soviet security apparatus was mainly trying to control information, and therefore communications systems and technologies were permitted as long as they transmitted the 'correct' information to society. While Shane is more focused on access to information and how this access brought about the information revolution, Kristin Roth-Ey's book focuses on communications systems or technologies that are a part of shaping culture, namely television, radio, the press, and cinema. Roth-Ey (2011) looks more specifically at how these systems of communication were used for propaganda purposes, in order to make the Soviet citizenry a more modern and cultured society. Cinema, TV, and radio were mediums to transfer Soviet propaganda to the public and develop a superior and distinct Soviet culture to that of the West. While Shane emphasized the role of technology in the Gorbachev era, Roth-Ey traces the development and implementation of media systems from the Stalin era forward. Starr (1990) shows a tradition of emphasis on vertical communication networks is present from early Russian history to the Stalinist period, in that communications systems were under state control in order to ensure top-down communication or were for official government business use only. Those technologies that facilitated horizontal communication (person to person) were either underdeveloped or used for state communication. Starr argues that by the time his article was published in 1990, the realm of communications in the Soviet Union had irreversibly changed in favor of greater horizontal communication networks and that the state increasingly lacked the desire and ability to control communications. Terhi Rantanen (2002), in *The Global and the National*, focuses on new communications technology, but also the distinction between socially new and technologically new (and the corresponding 'old') in Russian society. Starr (1990) also mentions that it is important to analyze the usage and implementation of new technology along with its older counterparts that were re-introduced for new social uses (31). Rantanen's (2002) argument is that although most studies focus on the globalization of national media and communication systems, the issue is more complex and should incorporate the study of the nationalization of global media. Any globalization or changes to the media and communication systems, she argues, occur on a gradient scale because different systems have different uses or are at different points of development and implementation when globalization occurred. This thesis continues the story of the Russian experience with communications technology by including a more detailed focus on the development and widespread implementation of the Internet, as well as social media, keeping in mind the framework of looking at social use and political perspectives, put forth by the authors above, when telling this story.

The information revolution does not necessarily mean a revolution in the invention of communication technologies. The Soviet Union already had the same technologies as the West, however many communication technologies were not widespread because of poor infrastructure, were under lock and key for government use only, or were intended for propaganda purposes. The information revolution signifies the relaxation of control over communications technologies, which led to their more widespread use and development without the massive censorship of the past, and subsequently changed the attitudes of the Soviet people towards their government due to the new information available and their rejection of the culture the Soviet regime imposed upon them. The information revolution is central to a discussion of communication technologies in Russia, especially one that addresses Internet development, because communications technologies and systems in the country acquired new purposes, enjoyed greater freedom and wider spread availability, and entertained legal competition from Western technologies like the VCR, essentially creating the conditions for which the Internet could thrive.

Starr (1990) claims that a communications revolution was underway in the Soviet Union (41), however due to the publishing date of the work, he could not fully realize to what extent information and communications had changed and would change in the future. For Shane (1994), the information revolution directly led to the downfall of the Soviet Union. His narrative shows that the relax on information controls led to an emboldened press who exposed Soviet weakness, and an emboldened and angered public who had been fed lies about their way of life. Roth-Ey (2011) agrees that the Gorbachev era brought about 'cultural infiltration', where the massive demand for Western culture and technology can be explained by a desire for "what is ours and not theirs," in this case "theirs" meaning what was forced upon them by the Party. However, Roth-Ey shows that after Stalin's death there was a 'parting of the iron curtain' beginning with the Khrushchev era, which called for "peaceful coexistence" and "cultural exchange". Rantanen (2002) agrees that the expansion of communication networks in the Soviet Union contributed to its collapse. However, she adds to analyses of the information revolution by showing that it was also globalization, with the help of communications and its social use, "that challenged the old Communist system and now plays an important role in shaping the new system" (102). This thesis will show how the Internet and social media have been molded into a Russian version with its own distinct qualities, as well as show that the information revolution ushered in an era of horizontal communication networks that allowed the Internet to flourish, which only continues to grow.

Control

As previously stated, control is an important theme in the Russian experience with communications technology. In the first part of this section, authors Mark Walker, Loren Graham, and Slava Gerovitch examine how ideology and political factors influence technology. The second part focuses on control of the Internet. Ronald Deibert and Rafal Rohozinski analyze types of governmental controls over the Russian Internet, while Floriana Fossato and John Lloyd, and a publication by the Berkman Center for Internet and Society focus on content control efforts through propaganda or scare tactics.

Science and Ideology, edited by Mark Walker (2003), contains a collection of chapters looking at the relationship between science and ideology. In one of the chapters that focuses on the Soviet Union, the conclusion is that freedom is not necessarily a necessity for science to flourish, and that there were some instances where science fared better in totalitarian societies because of increased investment than in other free, democratic countries. Loren Graham (1993) would likely disagree with this statement as his book, *The Ghost of the Executed Engineer: Technology and the Fall of the Soviet Union,* shows how even though certain sciences, such as the steel industry, fared better in terms of funding, the ideology of the state hindered the scientists' ways of thinking and how the engineers carried out projects, which led to the ultimate failure of massive construction projects. Another theme in Walker's *Science and Ideology* (2003) is "ideologically correct science," or attempts by the state to transform a science into a more ideologically acceptable form. While science is not free of ideology, it will still develop within the constraints of an ideologically driven regime; however, science will still be shaped to fit an ideological construct, so science in the Soviet Union would never be associated with "bourgeois" science. Gerovitch's (2000) chapter in *Cultures of Control* details the development of cybernetics and shows how at first the government and the press labeled cybernetics as a pseudo-science because of its Western origins and therefore its bourgeois nature. Not long after, the same groups (including the scientific community) who had a hand in turning the tides on attitudes towards cybernetics hailed it as a progressive science that will serve communism (Gerovitch, 2000). Focusing on control over the development of computer networks, Gerovitch's article (2008)*, InterNyet: Why the Soviet Union Did Not Build a Nationwide Computer Network,* analyzes the role of politics and ideology in the decisions regarding computer network development in the 1950s-1970s. Any acceleration in the development of computer networks was in response to calls for defense purposes as the United States developed command and control computer networks, or for help in planning and managing the Soviet economy through cybernetic principles. The main takeaway is that computer networks for civilian purposes were not debated as an option (Gerovitch, 2008).

While ideology plays an important role in controlling the outputs of a society, scientific or otherwise, there are also more overt types of control used in Russia today, specifically those affecting communications technologies. In Deibert and Rohozinski's (2010) chapter on Russia in *Access Controlled,* they explore the "seeming disjuncture between authoritarianism in the Commonwealth of Independent States and the relative freedom enjoyed in Russian cyberspace" (15). In regards to the RuNet, controls tend to be more subtle and sophisticated than outright filtering. The chapter also provides a framework for cyberspace controls, which are divided into generations. First generation controls are those that directly block access to Internet content, such as those available in China ("The Great Chinese Firewall"), Uzbekistan and Turkmenistan (Deibert & Rohozinski. 2010). Second generation controls aim to provide a legal framework in order to enable state authorities to invoke filtering as needed. Third generation controls focus on competing in the information sphere without necessarily denying access. Whereas Deibert and Rohozinski focus solely on governmental controls of technology, Fossato and Lloyd examine use and content as well. Fossato and Lloyd's (2013) chapter in *Social Networking* seeks to gauge the validity of the statement that the Internet provides an escape from the controls of the Russian state over TV, radio, and the press. The authors argue that the regime in Russia uses the Internet as a platform for propaganda purposes to drive conversations, spread the presidential message, and consolidate its power without using outright censorship. They claim that the state is the "main mobilizing agent" and that the democratizing effect of the Internet has not yet taken shape in Russia (Fossato & Lloyd, 2013). However, in a publication from The Berkman Center for Internet and Society entitled *Exploring Russian Cyberspace: Digitally-Mediated Collective Action and the Networked Public Sphere,* the researchers do not find evidence that efforts by the government to promote its message online through its supporters are very successful (Alexanyan et al., 2012). Furthermore, they do not find that Russian bloggers significantly alter their online behavior due to perceived government surveillance.

Offline attacks are an important form of control not directly addressed in *Access Controlled.* The literature unfortunately does not directly address criminal cases brought against online journalists or bloggers, which is becoming another form of control. This thesis will provide details on cases where bloggers are criminally charged for their speech and/or actions. A culture of control in regards to communication systems is reappearing and although media systems previously privatized in the post-Soviet period, such as television and the press, are now under the state's direction, Internet and social media are the new targets that are proving to be much harder to control.

Surveillance

Although surveillance is theorized as a third generation technique by Diebert and Rohozinski (2010), it is different in character than outright control. Therefore, studies on Internet surveillance are useful to distinguish the difference in how surveillance is used to control or influence users both directly and indirectly. Because not a lot is widely known about surveillance efforts by the government and security agencies, many studies are simply factual, short articles, or passing references within larger books or articles on Internet controls. In Andrei Soldatov and Irina Borogan's (2013) article *Russia's Surveillance State*, they show through an analysis on the increasing usage of the System for Operative Investigative Activities (SORM), its procedures, and new Internet filtering laws that the Russian security services are, in recent years, turning Russia into a surveillance state. The authors argue that Russia is increasing pressure to host websites locally on the .ru platform under the guise that US intelligence agencies will not be able to access their information, while it gives the FSB the authority to gain access to information previously unavailable due to laws against surveillance on non-Russian hosted websites. In *Revolution Stalled*, Sarah Oates (2013) notes that SORM is "not so much a form of internet regulation, as a means of using the internet to monitor communication" (98). She highlights the notion that both the Russian government and Russian ISPs could argue that the very action of using the Internet opens the individual up to information collection and its subsequent use by the government. Thus, the policy of SORM adds to the debate of privacy and online rights active in many societies, which employ similar methods (Oates, 2013). This thesis seeks to distinguish surveillance as different from the concept of control methods, but also that it is related to control in that it symbolizes the government's desire for control over information flow.

Intelligence Services

The intelligence services in the Soviet Union and Russia have been a crucial piece of this puzzle as they are often the ones who carry out the surveillance or control over communications technology and information. Scholarly literature on the current security service, the FSB, and its partners is scarce. Due to the popular culture interest of Russian spies during the Cold War, there are many books written on the KGB, however many seem to be less than scholarly. It seems information obtained from former KGB officials or defectors serves to fill the holes left uncovered by historical research for books on the KGB.

Christopher Andrew's book, *KGB: The Inside Story of its Foreign Operations from Lenin to Gorbachev (1990),* chronicles the history of the KGB, and with the help of defector Oleg Gordievsky, painstakingly details the history of the security services from its tsarist origins to the Gorbachev era. An interesting and important factor relevant to this thesis is one of his minor arguments, that the security services have elements that have transcended the reorganizing and renaming of the security services through the years. He writes that the myths and symbols of the Cheka and the personality of its leader Felix Dzerzhinsky became a cult then followed by the KGB. The KGB is said to identify more with the ideals and symbols of the Cheka in order to distance itself from Stalin's NKVD. In *Secret Empire: The KGB in Russia Today,* J. Michael Waller (1994) argues against the false impression that the KGB is similar to Western security services like the CIA, because of the service's Chekist origins, which are completely dissimilar to anything regarding a liberal democracy, and embody the theme that everyone is a suspected enemy of the state. He goes on to argue Russia inherited a security service that was technically reorganized and renamed, however was not reformed, and that even after the Soviet Union collapsed the Chekist values and culture brought with former KGB employees still survives in the service today. Andrei Soldatov and Irina Borogan (2010) wrote *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB* in order to reveal the ways the "new nobility" of FSB agents has grown and performed in the last decade. This book was published in 2010, thus it can paint a better picture of the evolution of the KGB into the FSB. The authors argue that the security services today see themselves as the only forces able to save Russia from internal and external enemies. After Putin became president, increasing numbers of former KGB officers were placed in leadership roles throughout government and society, thus providing protection for the FSB in all aspects of society. Soldatov and Borogan argue that the FSB has evolved into a more powerful agency well beyond the bounds of a revival of the KGB. This thesis seeks to provide a comprehensive look at the evolution of the intelligence services from the tsarist period to the FSB today. Through the lens of the study of communication systems, it also becomes clear what exactly these services were interested in controlling, namely information and access to it.

Historical Overview: The Control of Communications Technologies

Cultures of Control

From the years of Tsarist rule to the Soviet period, Russia with its authoritarian tendencies has always focused on containing dissidence towards the state. The 1845 Criminal Code states that "persons guilty of writing and spreading written or oriented works or representations intended to arouse disrespect for Sovereign Authority or for the personal qualities of the Sovereign, or for his government" would be penalized (Andrew, 1990, p.19). Article 70 of the criminal code of the Russian Soviet Federative Socialist Republic prohibited "anti-Soviet agitation and propaganda with the goal of undermining and weakening the Soviet state and social system" (Shane, 1994, p.11). Although the Soviet Union was a unique experiment with political oversight of all aspects of life, Soviet controls on dissident communications clearly possess roots in the tsarist period.

The tradition that vertical communication networks dominate over horizontal communication networks in Russia derives its origins from the tsarist period (Starr, 1990). Vertical communication networks refer to those networks that facilitate top-down, hierarchical communication and disseminate information from the government to the public or those which are solely for the use of the government. Horizontal communications networks are those for the use of the citizenry and facilitate communication between individuals and groups. Services such as the postal service and printing press were reserved mainly for official use. Even roads were first built for military and commercial purposes with a secondary use for private travel (Starr, 1990, p.22). If services with horizontal capabilities were allowed to exist, they were subject to censorship laws or deliberately left underdeveloped (Starr, 1990, p.23).

During the tsarist period, printed literature was the primary form of mass communication. Therefore, the tsars paid close attention to books, journals, pamphlets, and letters in their search for subversive material deemed to be adversarial to the state. The tsars of course were not worried about computers, photocopiers, and televisions; however, railways were thought to be problematic because they could connect great distances and facilitate the movement of people (and more indirectly, ideas) (Shane, 1994, p.48). Indeed, railways did eventually aid the revolutionaries, as it enabled easier correspondence and contact among the population, which was spread out over the vast Russian territory.

Although there was a period of private initiative in the mid-nineteenth century, which led to an increase in the implementation of horizontal communication networks (albeit relatively small), the Bolshevik revolution and subsequent takeover reversed any initiatives for facilitating these kinds of networks. In order to re-establish the priority of vertical channels of communication, the Bolsheviks suppressed horizontal communication by seizing communications channels, regulating the dissemination of information and centrally producing it in the capital, and by suppressing the development of "potentially individuating new technologies", such as the private automobile (Starr, 1990, p.27). This essentially was an attempt at isolating people from one another, and left individuals more readily subject to government control (Starr, 1990, p.27).

Though the concept of authoritarian rule carried over from the tsarist period to the Soviet regime, and both regimes were sensitive to the threat posed by access to information and movement of people, the scale and consequences of Soviet repression are hardly comparable, notably because tsarist Russia never became a fully-fledged police state (Andrew, 1990, p.21). The difference lies in the role of ideology. The tsars were trying to keep the empire strong, and power and wealth for themselves. The Soviets, on the other hand, were trying to reshape and re-educate a society, so along with the push for increased literacy came the need to censor books and political literature. The desire for a cultured population with an emphasis on fostering cinema and music brought monitoring of what message the arts were portraying to the Soviet people and the world. The Soviets promoted a "messianic" ideology, along with the goal of world revolution, so it seemed as though greater sacrifices were necessary and allowable in order to preserve the Soviet state. Another reason Soviet leaders felt more vulnerable than the tsars and therefore conducted repression on a larger scale was the fact that the Bolsheviks had seized power through a coup, thus there needed to be checks in place to ensure an underground movement and subsequent coup did not oust them from power (Shane, 1994, p.47-51).

The Role of Ideology

Communist ideology played a large role in shaping Soviet views towards science and especially communications technologies because of their unique ability to transmit information. This section serves to show that not only were political dissidents and the technologies that transmitted their ideas subject to control, but also scientists more generally, as well as the very science they were trying to practice. The Soviet regime was trying to control access to information and to gain a monopoly over truth. Controlling scientists and their scientific findings is another piece of that monopoly, and in turn raised the stakes for controlling communications technologies because they could be used to transmit ideas contrary to the "truth" the Soviet state wanted the population to know. Every decision the Soviet government made was in the name of socialism, to further the cause of the Soviet Union, to preserve the state, and to make her the strongest and most prosperous country in the world. During the Stalinist period, Party ideologues had a large impact on the scientific community, cybernetics and genetics being perfect examples. The Soviet press launched a war on cybernetics, initially labeling it as a pseudo-science. However, a few years later the same press and scientific community hailed it as a progressive science in the service of Communism (Levin, ed., 2000, p.247). The anti-cybernetics campaign was a by-product of a large-scale propaganda campaign aimed at criticizing and destroying bourgeois philosophy and sociology, especially that of American or Western origin. After Stalin's death, when the political thaw came into effect, scientists began to speak more openly against ideological controls and interference by Party leaders in science. The scientific community worked to re-label cybernetics in a more positive light to reaffirm their intellectual autonomy (Levin, ed., 2000, p.251).

Similarly, the study of genetics in the Soviet Union was influenced by the "ideologically correct science" of Lysenkoism, beginning in the 1930's. Lysenko's theories were rebuffed in the genetics community as "contrary to all known facts about genetics" (Walker, 2003, p.43). After presenting his views in a Marxist framework that caught the attention of Stalin, however, his views were promoted, he was promoted to president of the Academy of Agricultural Sciences, and research in genetics ultimately was banned in 1948, condemned as a bourgeois science. In 1965, after the fall of both Stalin and Khrushchev, Lysenko was brought down and the field of genetics was rebuilt and reinstated (Walker, 2003, p.43).

The Soviet leadership also had a blind obsession with output when it came to technology and industry. This obsession resulted in an enormous cost to human life, workers' conditions, and the environment. Although the Soviet Union was a great industrial power, the standard of living for most citizens could be compared to that of third world countries. Due to ideology, the leadership placed emphasis on producing steel for heavy industry and the armed forces, and thus caused food and consumer goods to be scarce. The Soviet leadership viewed success in both these areas as paramount to Soviet superiority and worldwide respect and recognition (Graham, 1993, p.101)

Communications technologies are an interesting case study because although the various media subvert the Soviet desire for information control, the Soviet government wanted a populace attuned to culture, a modern socialist society, and a method of getting its propaganda to the people. Kristin Roth-Ey believes that "it was the commitment to culture as linchpin of the socialist ideal that delivered broadcasting to Soviet homes" (2011, p.132). This commitment led to a stunning paradox exemplified by the case of radio: Soviet industry was producing shortwave radios so that their propaganda and culture could be transferred to the masses, while these same radios were able to carry shortwave foreign broadcasts to the people. The authorities' response to the foreign broadcasts was not to get rid of radios, but to instead spend millions on jamming the signals and using Soviet media to rail against foreign voices (Roth-Ey, 2011, p.132-3). This resulted in the Soviets devoting more resources to jamming both domestic and foreign broadcasts than to actually broadcasting their own. Soviet jamming efforts also managed to block out their own broadcasts in addition to the ones they were trying to keep off the air (Nelson, 1997, p.91-92). After all, radio still could be used to propagate Soviet culture as long as the "enemy" was kept off the airwaves.

More specifically, the enemy here was not necessarily just foreign voices, but it was the information transmitted, especially that on Soviet domestic affairs. The Soviet government did not want people to have access to this information, as it would undermine the Soviet state. Radio in the Soviet Union was meant to educate, not to entertain, so when citizens listened to foreign broadcasts, which focused more on the needs and desires of the people and their entertainment, these became more popular than Soviet programs. The popularity of foreign radio stations and their subversion of a distinctly Soviet culture was an embarrassment. As a result, the Soviets created broadcasts broadly resembling Western models of round-the-clock news and entertainment stations. Initially, spreading radio technology throughout the cities and the countryside during WWII was a ploy to achieve socialist modernity, to bring those stuck in the past into the future, however the Soviets did not anticipate the flow of information that radio would open (Roth-Ey, 2011, p.133-135). A battle between the Soviets and the

West ensued for the hearts and minds of the Soviet population, as radio was one of the only ways the West could transmit its voice to the people.[1]

Organs of Control

Whether looking at the tsarist period or the Soviet period, the common theme present is the carrying out of control on some or all aspects of society in order to keep the citizenry in line with the ruling ideology. While the ideology that determines the need for control came from the views of the government and leaders themselves, organs of control had to ensure that the people were controlled effectively in the field and that no "bad information" got around. These "organs of control" are more widely known as intelligence agencies or political police agencies, and were responsible for controlling subversion within the population and helping to propagate the good image and ideologically correct culture of the state. A short history of some of the most important organs of control from the tsarist period to the Soviet Union is useful here in demonstrating the continuities and articulating the differences between the two systems.

In August 1880, after assassination attempts on the Tsar Alexander II's life continued to increase despite efforts by the Third Section[2], the Department of State Police was created to consolidate responsibility of all aspects of state security into one department. Political crime was the responsibility of special departments and sections

[1] For more information on the battle over radio broadcasting in the Soviet Union, see*: War of the black heavens: The battles of Western broadcasting in the Cold War*, Michael Nelson; and: Badenoch, A., Fickers, A., & Henrich-Franke, C. (2013). *Airy curtains in the European ether: Broadcasting and the Cold War.*

[2] Tsar Nicholas I established the Third Section in 1826 to act as the political police in charge of quelling uprisings and political dissent. The Third Section was disbanded in 1880 after it was declared unable to respond effectively to the wave of terrorism and assassinations in the late 1870's. (Andrew, 1990, p. 18-20)

collectively known as the Okhrana[3]. In 1883, the “Foreign Agentura” (Zagranichnaya Agentura) formed in Paris as a special branch of the Okhrana abroad. Offices later opened throughout Europe including in England, Germany, Switzerland, and Italy. The foreign branch was created to keep watch over Russian émigrés and suspected revolutionary groups around Western Europe (Fischer, 1997, p.6). The Okhrana was unique in the extent of its powers relative to other European state security organs, and in regards to political crime it had the right to persecute on its own authority. However, the Okhrana’s usage of powers paled in comparison to Soviet standards (Andrew, 1990, p.20).

The All-Russian Extraordinary Commission for Combatting Counterrevolution and Sabotage (Vserossiiskaya Chrezvychainaya Komissiya po Borbe s Kontrrevolyutsiei i Sabotazhem), also known as the Cheka, was established on December 20, 1917 and was the political police and foreign intelligence wing of Lenin’s Bolsheviks. The Cheka’s emblems, the shield and the sword, symbolized defending the revolution and smiting its foes, respectively. Lenin did not believe at first that a political police would be needed because of the supposed popularity of the Bolshevik revolution. However, the opposition to the new government was a larger threat than he initially thought, and he concluded that a special apparatus needed to be established to deal with opposition both at home and abroad (Andrew, 1990, p.38-40).

[3] A special department (osobyi otdel) within Police Headquarters and a regional network of Security Sections (Okhrannoye Otdelenie) made up the political crime unit. The Okhrana is a nickname, seemingly from the Russian word for the security sections, given to the whole tsarist political police system. (Andrew, 1990, 20)

In 1934, the NKVD, People's Commissariat for Internal Affairs (Narodnyy Komissariat Vnutrennikh Del), consolidated the political police, regular police, security troops, investigations, and the penal system into its control. Though the political police was only one part of the whole apparatus, it was the one most typically referred to as the NKVD. The entire system ultimately answered to Stalin, therefore it was more specifically Stalin's organ of control (Andrew, 1990, p.131). Among the massive repressive efforts carried out by the NKVD, they shot members of the Communist Party leadership and executed the Great Terror in which they acted on the counterrevolutionary conspiracy idea that foreign spies and "enemies of the people" were living throughout the Soviet Union waiting to subvert the state. These enemy agents were found among the ranks of government leaders, scientists, literary figures and even within the NKVD itself; it seemed that no one was safe from Stalin's repressive purges. Millions of people were shot or died in the labor camps, put there to control any dissidence that the paranoid Stalin and his NKVD saw within the population, even though the fears were usually unfounded (Andrew, 1990, 131; 138-145). The OGPU[4] implemented the gulag (labor camp) system in which millions died during the repressive Stalin years, but was transferred to the NKVD's supervision when it absorbed the OGPU and its powers in 1934 (Andrew, 1990, p.121; 131).

[4] The OGPU (Obyedinyonnoye gosudarstvennoye politicheskoye upravleniye) or the Unified State Political Directorate was the Soviet security service from 1923-1934. The creation of the OGPU and its newfound status as a federal agency after the formation of the USSR in 1923, solidly established the security services' position in the Soviet state. Its predecessor, the Cheka, was created to be a temporary service to defend against counterrevolutionaries and terrorists. In July 1934, the OGPU transformed into the GUGB (Main Administration of State Security) and was then merged into the newly created NKVD.

In March 1954, not coincidentally after Stalin’s death in 1953, Soviet state security underwent the last major reorganization into the Committee of State Security or the KGB (Komitet gosudarstvennoi bezopasnosti) (Andrew, 1990, p.427). The Cheka can be considered the ancestor of the KGB, as agents referred to themselves as “Chekisty,” wanting to distance themselves from the horrors of the NKVD and Stalin (Andrew, 1990, p.38).

Targeting Communications

While it seems to be the trend to focus on media and ‘newer’ technologies in studies of communications history, these are not the only mediums Russia and the Soviet Union sought to control. In order to analyze communications on a much broader scope, communications scholar Armand Mattelart uses the definition of communications technology as any technology that involves "the multiple circuits of exchange and circulation of goods, peoples, and messages" (Mattelart, 1996, p.xiv). This is a useful definition here because, as already stated above from Scott Shane and Frederick Starr’s works, even though tsarist Russia, or early Soviet Russia for that matter, did not have concern for such things as televisions or fax machines, they did have concern about access to information and communication tools such as political journals, personal mail, and railroads. Because the term communication or communications technology is so broad, it is critical to distinguish which facets of communication were targeted by the different intelligence agencies, from tsarist Russia’s Okhrana to the KGB in the Soviet Union.

The Okhrana's main goals were to monitor émigrés abroad for revolutionary tendencies, to penetrate revolutionary groups, and essentially to make sure no one overthrew/undermined the Tsar. Therefore, its main concern was with monitoring printed literature and communications between suspected revolutionaries. It screened mail going to suspected revolutionaries, which was only possible because mail workers or porters/landlords were on the payroll (Fischer, 1997, p.7). The Okhrana also targeted journals or books considered to be subversive revolutionary literature (Zuckerman, 2003, 167). Another form of interference in communications by the Okhrana was the intercepting and decrypting of government and diplomatic communications (Andrew, 1990, p.26). They also participated in covert active measures such as bombing a print shop, which of course was also quite symbolic (Andrew, 1990, p.25).

The Cheka only existed until 1922, however it was able to suppress u communications it found to be subversive as well. One of the first measures of control after the Bolsheviks' seizure of power in 1917 was to take control of St. Petersburg's Central Telegraph Office and the Russian Telegraph agency[5], which shows how much importance was placed on controlling access to information (Shane, 1994, p.261). In an effort to ensure that any revolutionary movements could be swiftly put down, the Cheka intercepted and read every piece of mail (Rayfield, 2004, p.98). They also arrested and punished newspaper editors as 'counterrevolutionaries' (Kenez, 1985, p.43).

[5] During the attempted takeover of Gorbachev in 1991, troops moved in to seize control of and restrictions were placed on any print and electronic media deemed to be unofficial. However, they made the mistake of not shutting down the telecommunications lines within the country enabling citizens, including Yeltsin, to get the message out that this was a coup and not a 'state of emergency'. For more information about the 1991 attempted coup and media seizures, as well as the media's response, see Ganley, 1996, p.127-204.

The NKVD answered directly to Stalin so there seems to be no distinction between the NKVD, the government, or Stalin in regards to who is directly responsible for different aspects of control. Of course, Stalin heavily monitored communication over telephone lines, made easier by their lack of widespread availability, even going as far as monitoring members of his own party (Rayfield, 2004, p.157). Reading the citizenry's private mail was a widespread practice as well (Rayfield, 2004, p.123). Within the realm of cinema, Stalin exerted his control acting as screenplay editor, casting and cinematography expert, and ultimate censor on every film shown in the country (Roth-Ey, 2011, p.28). Radio was a mass phenomenon in the 30's and was widely available, however it transmitted the voice of Moscow as the supreme political and military authority, illustrating how the technology was used solely for propaganda and not as entertainment or as a means to access information (Roth-Ey, 2011, p.136-7). Soviet newspapers, such as *Pravda*, also fell under the government's control (Rayfield, 2004, p.39). Interestingly, the NKVD decreed in the 30's that no accurate maps should be given to civilians for fear that they would fall into the hands of potential enemies (Shane, 1994, p.3). This is another example of the wide range of communication tools the government showed interest in controlling.

The KGB had more communications technologies to control than any of the previous agencies. However, books and political journals were some of the worst offenders for the spread of information. It was a crime to possess anti-Soviet literature and banned books, and the KGB reacted accordingly by confiscating such materials (Shane, 1994, p.10). People suspected of dissenting views also had their letters intercepted and their telephone calls monitored (Shane, 105). Letters addressed to enemy broadcasters were also intercepted (Roth-Ey, 2011, p.142). If the suspects indeed held dissident materials or repeatedly expressed dissident views, they would likely be interrogated and/or arrested (Shane, 1994, p.12-13). Although it is known that telephone conversations were monitored dating back to the Stalin era (Rayfield, 2004, p.157), the fact that telephones in the Soviet Union were scarce coupled with the crudeness of the country's telecommunications lines, in and of itself quelled telephone communications even into the later Soviet period. In the late 1980's, the Soviets had 113 phones for every 1,000 inhabitants, compared with 770 per 1,000 in the US (Ganley, 1996, p.18). In an attempt to counter the effects of foreign radio broadcasts, the Soviets spent more money trying to jam these frequencies than they spent on broadcasting their own (Roth-Ey, 2011, p.131). The KGB also probed suspicious individuals for their listening habits. For example, a Ukrainian plumber was charged with "recounting programs from foreign radio and anti-Soviet poetry to workers" (Roth-Ey, 2011, p. 142). VCRs and tapes were a problem in the 80's. The government's reaction was to prosecute those receiving VCRs as a gift abroad, to develop a network of informants against those using audio and videotape recorders, and to counteract the effects by producing a homegrown product that they could control. Photocopiers were kept under lock and key and could only be used under certain circumstances (Ganley, 1996, p.5). Fax machines, which would easily transmit information in the later Gorbachev years, were simply not widely available outside government offices until that time period.

The KGB controlled radio and television programming content, while the military and defense ministries controlled the "development, allocation, launch, and uses of communications satellites" (Ganley, 1996, p.5). Television and media were in such widespread use, that while the KGB of course monitored them for subversive materials, the oversight of these mediums was given to Gostelradio (State Committee for Television and Radio) and Glavlit (Main Department for the Affairs of Literature and Publishing, later named Main Board for the Protection of Military and State Secrets in the Press). Gostelradio had complete control over broadcasting, while Glavlit censored and banned publications, and gave permits for press bodies to be formed (Ganley, 1996, p.5-6). Essentially, all television and media were censored so that the Party and the Soviet Union was portrayed positively and provided what leadership thought the public should know, not what they wanted to know, see, or read. In film, for example, the KGB was looking for subversive elements because, "a Soviet institution was duty bound to protect its image in the public eye" (Roth-Ey, 2011, p.31)

Fax machines, telephones, and other electronic communications devices, such as computer networks, are interesting examples when researching Soviet control methods because unlike literature, cinema, television, and radio, these technologies were not widespread among the average civilian population. The technologies mentioned first are different from the latter mentioned forms of media because they facilitate peer-to-peer communication, which is harder to control and harbors the potential for subversive speech that may go unnoticed. They also could not be used by the state to widely transmit cultural and political propaganda, so the state did not have a purpose for these technologies in regards to the general population (other than to promote internal and external communications, which was not a goal for most of the Soviet era). There seemed to be a choice present to keep these technologies for official government use or to deliberately keep the technology underdeveloped so that, in essence, their usage was controlled by these decisions rather than directly by the KGB's hand (Ganley, 1996, p.17). Of course, whenever possible, they could and would crack down on any subversive activities, cue the listening of telephone calls.

Cultural Shift: The Information Revolution

Communication and media systems underwent massive repression under Stalin due to his push for a distinct Soviet culture free from Western influence. While Stalin's death is often perceived as the end of complete Soviet cultural autarky, complete cultural isolation was never the absolute reality. The Soviet Union had never been completely walled off from Western culture, due to Soviet citizens' exposure to capitalist culture when outside the borders of the USSR during World War II, and the postwar expansion of the Soviet Union into territories with a more developed bourgeois class and capitalist infrastructure. Even though cultural autarky was not the reality, Stalin headed a vigorous attempt at pushing the Soviets onto this path. In 1946, the regime launched an ideological campaign to secure Soviet culture's "purity and preeminence." No one was permitted to admire any aspects of Western culture because the official view through the lens of Soviet patriotism was that the Soviet culture had contributed more in the realm of feats of genius and cultural greatness than any other in the world (Roth-Ey, 2011, p.7). When Secretary of Ideology Andrei Zhdanov spoke to Soviet writers in 1946, he claimed:

> It goes without saying that our literature, which reflects an order that stands higher than any bourgeois democratic order, a culture that is many times superior to bourgeois culture, has the right to teach others the new universal morals….We know the strength and advantages of our culture very well….It is not for us to

> bow to all things foreign or to take a passive position of defense! (Roth-Ey, 2011, p.7)

This quote embodies the purpose of Soviet culture at this time, which was to compete against the West for cultural supremacy that in the Soviet leadership's eyes was rightfully theirs anyway.

After Stalin's death, cultural development changed dramatically due to the relaxation of repressive efforts and mass terror. While Soviets still believed in their cultural supremacy, Khrushchev and other regime officials called for "peaceful co-existence" and "cultural exchange" with the West. This marked the first time after the Stalin era that the USSR would open up to cultural competition from the West, and the general view is that the Soviet citizenry loved it. "Every well read tourist to the USSR knew to bring gifts of blue jeans and Beatles albums" (Roth-Ey, 2011, p.10). While the end of the Stalin era brought about a "cultural thaw" that served to appease the desires for bits of Western culture, the same period experienced a huge growth in homegrown Soviet culture and the cultural infrastructure, which found its way into the everyday lives of the Soviet people on a previously unseen scale. It is also important to note that peaceful coexistence and more openness towards the West in no way meant that the Soviet regime's position changed towards the ideological struggle: Soviet culture was still the exceptional culture and Soviet culture was still committed to promoting propaganda about the supremacy of the Soviet state in all realms of life (Roth-Ey, 2011, p.6-11). The slight parting of the curtain[6] during the Khrushchev era gave the Soviet citizenry a look into life on the other side, and showed them an alternative to Soviet life. Although there was a cultural thaw of sorts in this period, it pales in comparison to the era of Gorbachev's policies of *glasnost* and *perestroika* and the effect of the information revolution.

In 1985, Mikhail Gorbachev became the General Secretary of the Communist Party. Soon thereafter, he began calling for reform of the outdated and crumbling Soviet economy. This reform came through the policies of *glasnost* (openness) and *perestroika* (restructuring). The plan was to restructure the failing Soviet economy into a more modernized one using greater openness in regards to information, especially politically important information (Ganley, 1996, p.49). While the Western world was enjoying an inflated economy that was the result of the communications technology boom in computers and other electronics, the Soviets were still producing outdated items no consumer wanted. For one, certain communications technologies hardly could find a place in Soviet life as poor public infrastructure was the reality for technologies viewed as not having a significant ability for disseminating propaganda[7], such as the telephone.

[6] By slight parting of the curtain, I mean the opening up of Soviet society for cultural exchange of goods and information. The Soviet Union was still very restrictive in its policies, for example on the issue of travel restrictions. For more information about the parting of the Iron Curtain after the Stalin era, see: Hixson, W. L. (1997). *Parting the curtain: Propaganda, culture, and the Cold War, 1945-1961*. New York: St. Martin's Press.

[7] This touches on an earlier point that the Soviet Union placed emphasis on developing certain technologies, in the case of communications, when there was a potential for using it as a tool for spreading propaganda and seemed to not develop those technologies which were only useful for personal communication.

The paradox of shoe availability serves as a telling example of the inefficiency of the troubled Soviet economy during this period[8].

In essence, *glasnost* ushered in the relaxation of information control and ultimately led to an "information revolution" that took place between 1987 and 1991 (Shane, 1994, p.287). The information revolution enabled greater usage and availability of a wider range of communication technologies within the general population.[9] It also ushered in a relaxation of the controls on information and a political climate where dissidence was tolerated and not completely criminalized. When this happened, the people were inundated with a flow of information about their own world. Some of the most influential information that became available was about the atrocities committed by Stalin and the deliberate distortions of historical fact. The populace was overwhelmed at the extent of the misrepresentation of history and their society. Entire history textbooks were considered to be full of half-truths or complete inaccuracies. The Soviet press conducted interview after interview and published article after article exposing the historical inaccuracies fed to the people for years about their great Soviet state. Previously, the press had been fearful of exposing anything about the KGB or the government, yet the information revolution and *glasnost* gave them both the access to

[8] People stood in lines for hours just to buy a decent, usually imported, pair of shoes. However, when one does the fact checking, they will find that the Soviet Union was the largest producer of shoes in the world. It was all a façade; the people did not want the shoes, yet the government was able to use the fact they were the largest producers of shoes as another piece of propaganda that shows the Soviet system as being superior (Shane, 75-77).

[9] This period also made Western technologies easier to import into the Soviet Union. It is important to remember that the Soviet Union had many of the same technologies as the West (and many of these technologies have reasons for creation that were rooted in the Cold War), but certain technologies, like the computer and fax machine, were first created for military or official state use and were not widespread among the civilian population or did not find a use there at all.

new information and a political climate which allowed them to share the information and not worry about political exile, jail, or death (Shane, 1994, p.121-23).

While the print media was integral in beginning the reexamination of history, after the initial shock and the rabid desire for anything historical subsided, the people's attention shifted to politics. This is when television became an important medium in the reexamination of Soviet politics. Television, which had been made available on a wide scale because of its use for the dissemination of Soviet propaganda, enabled citizens to become involved in politics. It operated as a catalyst and amplifier for the first powerful wave of political enthusiasm, beginning with the political campaign of 1989 (Shane, 1994, p.149). For the first contested elections in 1990, people were able to watch the candidates debate on television, allowing them to make more informed decisions about who they wanted to vote for (Shane, 1994, p.151). Television brought politics and Congress to the people, giving them faces and showing their vulnerabilities. The live broadcasts of the Congress of People's Deputies came to be one of the most watched broadcasts of all time (Shane, 1994, p.145). Not only did the television bring politics to the people, it also, in broadcasting Congress, introduced the people to legitimized debate and the lessening of fear towards the government. It instilled the idea that if an official could go on television and publicly disparage the KGB, the average citizen could speak their mind whether expressing their views about everyday corruption or disdain of the Party and ideology (Shane, 1994, p.151).

Not only did the information revolution bring about increased political participation and expose historical inaccuracies, it also opened the door for the dissemination of a wider range of information. Publications containing politically subversive information that would have been banned to protect the Soviet image were suddenly available. Hundreds of samizdat newspapers and magazines hit newsstands, with their political affiliations ranging from ultra left to ultra right, from Marxist to monarchist (Ganley, 1996, p.58). On the street corner one could now find books on psychology, history and politics (even critical accounts), business, Western classics such as *Gone with the Wind* and *Jane Eyre*, Russian classics previously censored such as *Doctor Zhivago* and *Gulag Archipelago*, and even books about sex. People were enamored by the influx of new books not only because of the newness of the experience, but because they now had access to information they were interested in, not only that which the state thought to be important. In fact, not all of these topics and publications had necessarily been banned, but rather the publishing houses were too busy printing copies of Party propaganda to print anything else not deemed important (Shane, 1994, p.183-184).

Thanks to the policy of *glasnost,* the information revolution, and the subsequent disintegration of the Soviet Union, the former Soviet people developed a fervent demand for anything and everything Western as ‘cultural infiltration’ set in. They wanted what was Western and rejected ‘theirs’ (Soviet), not because what was foreign was necessarily better, but because ‘theirs’ had been forced upon them by the Party (Roth-Ey, 2011, p.8). However, the rejection of their own culture did not last. Just as the initial shock and fascination with everything related to Stalinism and Soviet historical inaccuracies subsided, the Russian people[10] seemed to have reached a saturation point with Western culture, reflected in their consumption of popular culture in the 1990's (Rantanen, 2002, p.102). For example, Russian audiences seemed to have "lost its taste" for U.S. TV series, while preferring domestically produced and Latin American serials by 1999. This saturation point seems to have occurred in films as well, with audiences returning to domestic films, although many Russians continued to be fans of Hollywood action films (Rantanen, 2002, p.101-102). The information revolution and the dissolution of the Soviet Union brought about a vacuum, which allowed foreign films and TV series to flood the airwaves. Although the Russian population did seem to reach a saturation point, there is another explanation for this happening than simply that the Russian people became tired of Western culture. The saturation point could be due to Russian domestic productions competing with Western and other foreign programs, becoming popular right alongside those from the US.

Eventually, there was a drive to Russify or nationalize cultural productions. This was quite evident in the dubbing over of foreign programs with the Russian language. English was rarely heard and dubbing the programs seems to make the program less foreign. Dubbing of foreign programs is quite expensive, three times the cost as subtitles, however Russian television has opted to pay the extra costs for dubbing (Rantanen, 2002, p.100). Although Russian television adopted the contents and formats of Western shows, their own nationalized Russian versions found their way into the homes of citizens. This

[10] It is important to make the distinction that this thesis and subsequently this historical overview examines the experiences of Soviet Russia and not that of the entire Soviet Union, as the other members of the Soviet Bloc may have different experiences. As such, the thesis here moves into a discussion of post-Soviet Russia.

can be observed in Russian game shows such as “Pole Chudec” (Wheel of Fortune) and “Ugadai melodiiu” (Name that Tune), as well as “Chas Pik” (Rush Hour) which is a copy of Larry King’s nightly interview format (Rantanen, 2002, p.100).

In the subsequent years following the disintegration of the Soviet Union, media and communications systems were restructured to fit the changing landscape of the Russian political and economic spheres. Of course, the media and communication systems did not change overnight, nor did all systems develop at the same rate. The changes occurred on a gradient scale and varied because each system was in a different stage of development. For example, television and radio had well developed infrastructure, yet the telephone did not enjoy the same widespread availability, and new electronic media, such as the Internet, were in the early stages of development at the time of the collapse (Rantanen, 2002, p.25).

One of the first major changes associated with the media system in Russia actually occurred before the Soviet Union collapsed. The Law on the Press and Other media, which came into force in 1990, guaranteed the freedom of the press, prohibited censorship, established freedom of information, and allowed private broadcasting, while it prohibited the ownership of mass media by foreign citizens, though not by foreign companies (Ganley, 1996, p.89-92; Rantanen, 2002, p.28). After the adoption of this law, privatization came in the form of the establishment of national daily newspapers, as well as television channels and radio stations that were all independent of political parties or movements (Rantanen, 2002, p.28). The privatization of certain parts of the Russian media system does not mean that there has been a complete change from state to private ownership: often we see the two hand-in-hand (Rantanen, 2002, p.38). For example, in 1994, Yeltsin decreed that the Ostankino Broadcasting Company would be privatized although the government owned 51 percent of the shares (Rantanen, 2002, p.28). The first non-governmental television company, Telekanal, founded in 1990, became popular due to its entertainment programming, and set the groundwork for the establishment of about 30 similar companies. Although the first private television channel appeared in 1990, state-owned media ran the national channels until 1993 when NTV began its operations on the Fourth Channel. It is interesting to note that even after the collapse and the policies of privatization permeated the economic sphere, Russian media remained mainly in domestic ownership. Foreign investment in media did not play a key role, except for the notable example of *Pravda*, which was bought by a Greek publisher (Rantanen, 2002, p.29). The shift from print to electronic media (television and radio) began in 1991, with the circulation of central newspapers from 100 million copies during the Soviet period declining to only 20-24 million in the period between 1991 and 1992 (Rantanen, 2002, p.30). Not only does this shift mark a globalization of Soviet media systems, but it also represents the shift from a state centered approach to media, to a system where entertainment and the people's wishes dominate.

The end of the Soviet Union did not only bring changes to media and communications systems. The government turned its focus to reforming the intelligence services as well. Even before the Soviet Union officially collapsed, Gorbachev and Yeltsin expressed their desire to reform the KGB because the KGB needed to be stripped of its overwhelming grip on power. Although members of the Soviet state and Russian parliamentary commissions demanded that the KGB be dismantled, Gorbachev and Yeltsin did not take advantage of the opportunity to do so (Waller, 1994, p.63). After the attempted coup in August 1991[11], Gorbachev announced that Vadim Bakatin, the reformist former USSR Interior Minister who knew nothing about intelligence work, would be the new KGB chairman. Gorbachev gave him the authority to "prepare a proposal for the reform of the state security organization" (Waller, 1994, p.64). With this authority, he did not try to abolish the KGB per se, yet he set out to break apart the monopoly of power it held by dividing it into smaller compartments and attempting to shuffle, reform, and depoliticize the ranks within, all the while making them answerable to new laws (Waller, 1994, p.65). Bakatin then embarked on a massive forced retirement and firing spree of KGB leadership (Waller, 1994, p.66-73).

All of the restructuring and reform that Bakatin put into place for the KGB seemed to be for naught as of December 25, 1991, the day the Soviet Union ceased to exist by declaration. After the collapse, Russian president Yeltsin now had to decide what to do about the state security apparatus. Instead of taking the opportunity to institute reforms across the board, he decided to leave the former KGB fairly untouched as a service in the Russian Federation, by leaving many of the same workers in their positions (Waller, 1994, p.102). Amid the turmoil and confusion of the collapse, the status and

[11] This refers to the attempted takeover of power from Gorbachev by members of the Soviet government on August 18, 1991. While Gorbachev was held hostage in his vacation home in the Crimea cut off from communications, the Soviet people were told he was too ill to carry out his duties and thus a state of emergency would be put into place with a State Committee of State Emergency leading the country. The attempted coup was likely in response to a new treaty waiting to be signed that would give back some powers to the governments of the republics and recognize the republics as sovereign states. The coup eventually failed due to the ineptitude of the coup conspirators and to the role of communications technologies, such as the telephone, fax machine, and computer networks, in getting out word to the people that it was a coup not a real emergency. For more information about the attempted coup see, Ganley, 1996, 127-227.

reform of the security services in this period is itself a story of confusion, however there are some important points of restructuring. Yeltsin abolished the USSR Ministry of Internal Affairs (Ministerstvo Vnutrennikh Del, MVD) and Inter-republic Security Service (Mezhrespublikanskaya Sluzhba Bezopasnosti, MSB) and folded them in with the Russian MVD and Federal Security Agency, creating a huge bureaucratic force entitled the Ministry of Security and Internal Affairs (Ministerstvo Bezopasnosti i Vnutrennykh Del, MBVD) (Waller, 1994, p.103). In 1992, after much criticism of the creation of the Ministry, it was disbanded and the Ministry of Security (Ministerstvo Bezopasnosti, MB) was created along with a separate Ministry of Internal Affairs (MVD) (Waller, 1994, p.109). In December 1993, Yeltsin disbanded the Ministry of Security after public complaints that the MB had not supported him during the election cycle, and created the Federal Counterintelligence Service (Federalnaya Sluzhba Kontrrazvedki, FSK) (Waller, 1994, 119). The FSK was responsible for counterintelligence and counterterrorism (Borogan, 2010, p.13); it did not inherit the responsibility for external or foreign intelligence gathering from the KGB. The separate Foreign Intelligence Service or SVR (Sluzhba Vnesheny Razvedki) was tasked with this responsibility. The former KGB division responsible for electronic eavesdropping and cryptography was called the Federal Agency for Government Communications and Information (Federalnoye Agentstvo Pravitelstvennoi Svyazi i Informatsii, FAPSI). Several other former KGB divisions are now their own agencies, such as the Federal Protective Service and the Federal Border Service (Borogan, 2010, p.13). In 1995, the FSK was renamed the Federal Security Service or the FSB (Federalnaya Sluzhba Bezopasnosti) as it is still called today. Although the former KGB has gone through quite a few name changes, has had many agencies created from its directorates, and has had priorities mixed around, the main issue is that the KGB was never fully reformed in regards to its culture, since many of the old Soviet KGB ways stayed with those who continued in their positions (Waller, 1994, p.148).

In 1998, Yeltsin appointed Vladimir Putin to the head of the FSB, who later, with his decisive leadership, strong rhetoric, and ties to the KGB, rose to the Presidency. Under Putin as president in 2003, the border guards were absorbed by the FSB and the FAPSI was divided between the FSB and the Federal Protective Service. The communications agency (FAPSI) gave the FSB a crucial responsibility: overseas electronic intelligence. (It is also interesting to note that in the 90's, FAPSI was responsible for licensing information security software.) Under Putin, the FSB gained considerable power, coming to "outstrip the other security services" with no parliamentary oversight or competitors. The FSB under Putin can be characterized as an agency that advances and absorbs responsibilities, even extending its reach into the armed forces (Borogan, 2010, p.20-22).

The Internet Era

Although continuities from past to present exist in regards to control, these methods have evolved to fit the modern case of the Internet. The case studies at the end of this section function not only as examples of how the government is trying to control information and communication on the Internet, but also as examples of how these techniques are unique to the Internet age. These methods do not exhibit outright censorship or blatant Soviet-style crackdowns. They are sophisticated, subtle, and even within the legal framework. This section serves as context for showing the unique characteristics of the Russian Internet in comparison to Soviet models of communication, like the television or radio, due to the relative freeness, choice, and interactivity it provides, and its capability of disseminating information from sources other than the government.

Development of the Internet in Russia

Unfortunately, communications technology did not see a substantial growth in availability in all of Russia even after the collapse of the Soviet Union. Access to telephone service, something almost taken for granted in the United States, was a scarce commodity in the Soviet Union. Because the telecommunications infrastructure was largely insufficient, Russia fell behind other countries in its ability to apply Internet connectivity on a wide scale. The poorly built networks using old copper wires that existed in the early transition period could not support a modern network like the Internet nor could it support data transfer at speed. Funding was also a problem with the implementation of the Internet, as both before and after the collapse of the Soviet Union funding for communications was scarce from both the state and foreign investment (Rantanen, 2002, p.47-57). Another obstacle for Internet, and even telephone network penetration, was the extensiveness of the country and the cost to the government of installing modern telephone lines. This enormous cost was not viable for a government rife with corruption and an economy that substantially lagged behind the West, with foreign investors afraid to put their money into this environment (Franda, 2002, p.102, 106-7). Poor infrastructure and lack of funding were not the only reasons for underdeveloped computer networks; political reasons must also be taken into account. The Soviet Union placed emphasis on using communication resources for state or military purposes, so although technologies such as computers did exist, they were not implemented for use by an ordinary Soviet citizen (Gerovitch, 2008).

Connection to the Internet as we think of it today was not a reality for much of Russia until the mid-90's. Computer networks were developed in the 1950s for military purposes and initiatives were proposed for computer networks that helped plan and manage the economy, yet a national computer network for use by civilians was not seen as viable or desired (Gerovitch, 2008). Civilian access to computer networks started popping up in the late 80's and very early 90's, however these were computer 'nets' such as FidoNet, USEnet, EARN (European Academic and Research Network), and GlasNet, not the 'World Wide Web'. Businesses, government agencies, schools and universities, scientists, and computer enthusiasts or hackers used these networks for information exchange and electronic mail services (Ganley, 1996, p.35-41). It is important to note that these Internet type networks were created by commercial enterprises and not by the government (Gerovitch, 2008, p.346). In 1993 Rel-Com, Reliable Communications, the Soviet company operated by the Soviet UNIX Users Group, acquired a connection to the EUNet, which signaled the beginning of the Internet as known today in Russia (Bulashova; Rocich). The connections, however, were mainly made in Moscow and St. Petersburg where the telecommunications infrastructure and other resources were most reliable/accessible. After this first step towards Internet connectivity by Rel-Com, other companies and networks began to follow suit in the proceeding years, along with research institutes and universities, which played a critical role in bringing Internet connectivity to Russian cities. Citing the poor and limited infrastructure issue, it was not until 1996 that access to the Internet began to spread into the Russian regions (Rocich, 2000).

Internet penetration in Russia continued to grow, albeit very slowly. According to research by the independent pollster the Levada Center, in 2001 only 5% of Russians used the Internet (Bogodvid, 2013). In 2003, the Internet usage rate was only at 9% of the population according to a survey conducted by the Public Opinion Foundation (FOM/Fond Obshchestvennoe Mnenie) ("Интернет в России: динамика проникновения: Осень 2013", 2014). In the later 2000's, the country experienced a large jump in the number of Internet users, with a significant portion of the growing number of Internet users coming from the Russian regions. In 2007, the percentage of Russians over the age of 18 who used the Internet at least once a month was 24%; in fall of 2013, the percentage had grown to 57% or 66.5 million people. The percentage of

Russian adults who use the Internet daily is 46% or 53.2 million people (FOM (Фонд Общественное Мнение), “Интернет в России: динамика проникновения: Осень 2013”, 2014). In cities with a population of more than 100,000 people, 94% of Internet users have access at home with the majority having broadband access (Analytical Group of Yandex Marketing Department, 2013). In recent years, cities with under 100,000 people are experiencing a large percentage of growth in Internet penetration; however, villages still lag significantly behind.[12]

Mobile devices are another platform on which users can access the Internet, and they have seen a large growth in use in recent years. In 2010, the Public Opinion Foundation conducted a survey of Russians aged 12 and over, finding that of those ages 12-17, 49 per cent were mobile Internet users. The study also finds that “the prevalence of mobile Internet use decreases with age, as 43 per cent of respondents aged 18-24, 26 per cent of respondents aged 25-34, and 11 per cent of those aged 35-44 reported usage” (UNICEF, Beger, Hoveyda, & Sinha, 2011, p.10). In 2012, the percentage of pages viewed on mobile devices was 25.1%, lower than only those percentages in the UK and Ireland (this study only takes into account users in Europe) (RIA Novosti, 2013). By the end of 2012, there were approximately 22.5 million mobile internet subscribers, an increase of 88 percent from 2011, with approximately 230 million mobile phone subscribers among the top seven Russian mobile service providers (Freedom on the Net

[12] It seems as though the growth is beginning to slow according to survey results and percentages; Russia only experienced 12% growth from 2011 to 2012, while from 2010 to 2011 the growth was 17%. While Moscow and St. Petersburg enjoy the highest Internet penetration rates at 70 and 71 percent respectively for 2012, 86% of new Internet users live outside the two cities (Analytical Group of Yandex Marketing Department, 2013). These numbers are based on survey results from the Public Opinion Fund, which surveys adults over the age of 18. TNS research group data covers users over the age of 12 and sets the usage rate at 76.5 million people or 53 percent of the total population (Bogodvid, 2013). As of 2010, 84% of Russians 12-17 were users of the Internet (UNICEF, Beger, Hoveyda, & Sinha, 2011).

2013: Russia, 2013, p.3). The increase of popularity for mobile phone Internet access possibly experienced growth in recent years due to the implementation of 3G technology in 2009 (UNICEF, Beger, Hoveyda, & Sinha, 2011, p.9-10).

It is important to note that more Russians have access to television than to the Internet. Television has been a staple in homes since the Soviet period and the nation has achieved a 98% penetration rate as of 2002 (Rantanen, 2002, p.35). Leon Aron suggests there is a television nation and an Internet nation, referring to those who use the television to get their information and those that use the Internet to get their information. Those in the television nation outnumber members of the Internet nation by nearly threefold (Aron, 2011). Consequently, the number of users who get information about events in the country from state television (88%) is more than double that of those who get their news from the Internet (41%) (FOM (Фонд Общественное Мнение) "О средствах массовой информации", 2014). Russians who get their information and news from the Internet "tend to be politically active: younger, better educated, concentrated in the largest urban centers, and middle and upper-middle class" (Aron, 2011). For example, in 2010, 62 percent of eighteen- to twenty-four-year-olds were regular Web users or between 1.3 and 1.6 times the national rate for all adults (Aron, 2011). With 62% of the population saying they trust state run media over non-state media, according to a poll by the Public Opinion Fund (Фонд Общественное Мнение), the groups with the larger amount of trust for state media are those with income below 20,000 rubles, those older than 46, those who don't work, and those who live in villages ("О средствах массовой информации", 2014). Those with higher levels of education are more likely to use the

Internet: 55 percent compared with 17 percent of those with only a high school education (Aron, 2011).

It is useful to remember that television is a quintessential example of the Soviet model of control. It represents the vertical network of top-down decisions regarding transmission and thus control over indoctrination of the public. The Internet represents a horizontal network allowing choice and the communication of ideas between groups and individuals. Television also represents a model of one-way communication (from the government to the people), and the Internet represents reciprocal communication (the government can provide information but the population can respond and find other sources of information). According to a poll by the Public Opinion Fund, searching for information and news are the top two things that Internet users do with their time online ("Для чего люди используют интернет", 2013). It is important to look at what kind of news and information each 'nation' consumes because the younger, more politically active crowd is choosing what news it wants to see, which is often that which is detrimental or contrary to the government's official line of thinking or story.

RuNet, as users call the Russian language part of the Internet, has established itself as distinct from its Western counterparts: Russian language sites dominate. It was the introduction of Windows 95, which came with the Microsoft standard for Cyrillic encoding that increased the desirability of creating a Russian Internet space differentiated from its Western counterparts by enabling the construction of Russian-language web pages without having to transliterate (Schmidt, Teubener, & Konradova, eds., 2006, p.21). Today, Russian companies "reign across search, social networking, digital media and email services" in the domestic market (Barnett, 2011). Four out of the top five sites in Russian are .ru domains, with the search engine Yandex as the top accessed site in Russia, reigning over Google (Alexa Internet Inc., n.d.). "Russian social media sites are among the fastest growing in the world, and Russian Internet users are said to be among the most engaged social networking audiences worldwide" (Aron, 2011). The number of Russian users of social media sites and the times of usage are among the highest in the world (Aron, 2011). VKontakte is the second most popular site in Russia with Odnoklassniki coming in at number 7 on the list. It is interesting to note that Facebook is number 8, below these two Russian social media sites (Alexa Internet Inc., n.d.).

Although Russians have been using the Internet to share information and ideas for years, Russian social media did not exist in its current form until the mid-2000s. While taking a cue from Western platforms, Russians have developed their own social media infrastructure suited to meet their needs, and numbers show that Russians prefer these sites to Western options such as Facebook and Twitter[13]. VKontakte users "create profiles, connect with friends, update statuses, create and join groups, share and download files, blog and/or post photos and videos"; unlike Facebook, VKontakte also offers a file-sharing feature (UNICEF, Beger, Hoveyda, & Sinha, 2011). Odnoklassniki users use the service primarily to locate classmates. Both were founded in 2006, two years after Facebook was founded. Although the Russian sites are the most popular, Facebook and Twitter have gained some ground, now the 8th and 16th most popular sites in Russia (Alexa Internet Inc., n.d.). These sites likely saw the increase in traffic due to

[13] The analysis that Russians prefer Russianized versions of Western social media platforms draws continuities with the discussion on customized elements of pop culture, such as Russian language versions of Western programs, in the 1990's.

the implementation of their Russian language versions (Prabhu, 2011). MoiMir is another Russian social media site, though it is integrated in the mail.ru platform, which is the most popular email application in Russia. Launched in 2007, it likely receives its comparatively small number of visitors from users of mail.ru who happen to stumble on the site (Prabhu, 2011).

Although LiveJournal is technically a blogging site, any social media analysis that fails to take it into account would be inadequate. LiveJournal, which got its start as an American company, has gained in popularity among Russians since 2001 when the first active Russian language journal was created on the site (Schmidt, Teubener, & Konradova, eds., 2006, p.31). Users can comment, control access to their pages, and post and exchange information, which makes the site more similar to a social media site like Facebook than a traditional open blog (Schmidt, Teubener, & Konradova, eds., 2006, p.31). Russian bloggers prefer blog platforms that combine blog features with other services normally synonymous with social networking sites like Facebook or VKontakte (Etling et al., 2010, p.3). According to Alexa statistics, LiveJournal is currently the 11th most visited site in Russia, and is well known as a haven for popular bloggers, especially opposition bloggers who feel that blogs are the only and best way to get their message to a large audience (Aron, 2011).

The growth of the Internet and social media in Russia signifies a shift to a fundamentally different culture of communication inconsistent with Soviet style control. A horizontal network that facilitates massive amounts of information exchange, allows choice, and is interactive rather than just a source of information, is in contrast to the tsarist and Soviet traditions of emphasis on vertical networks. This is important to later discussions in this thesis in regards to the current government's desire to recapture control over communications because the Internet poses a problem as to how one can control such a vast horizontal network that had been left to flourish with a high degree of freedom.

The State Seeks to Regain Control

Legal Restrictions and Regulation Regarding the Internet

Likely due to the delayed spread of the Internet throughout Russia, the 2000 Information Security Doctrine seems to mark the first time direct regulation of the Internet became a legitimate concern. However, there were some important pieces of legislation that emerged in the 90's in regards to electronic communications, information transfer and the expansion of computer networks.

As Internet and computer usage began to grow in the 1990's, laws were needed to regulate and protect usage. The Law of the Russian Federation Concerning the Legal Storage of Computer Programmes and Databases adopted in 1992 provides some legal protection for software designers against piracy, although enforcement was inadequate (Ellis, 1999, p.150). In February 1994, the Committee Attached to the Presidential Office on the Policy of Informatization (Roskominform) was created in order to "coordinate work on the implementation of state policy in the sphere of information in the system of state organs" (Ellis, 1999, p.151). In January 1995, the Federal Law Concerning Communications was adopted. The law establishes the legal basis for activity conducted in the area of communications in the Russian Federation, determines the authority of the organs of state power concerning communications regulations, and determines the rights and obligations of persons involved in communications. The law covers all forms of communications and not just the Internet (Ellis, 1999, p.152).

The adoption of the Federal Law "On Information, Information Technologies, and Information Protection" in 2006, discussed later in this section, rendered the following laws adopted in the mid-90's obsolete, most likely because the new law updated and consolidated ideas present in these laws (Organization for Security and Co-operation in Europe, n.d.). The Federal Law Concerning Information, Informatization and the Protection of Information, adopted in 1995, established organs of state power as the determining factor in access to information, information resources, and developing information policy (Ellis, 1999, p.153-54). The Federal Law Concerning Participation in the International Information Exchange, adopted in 1996, "set out the terms and conditions for the participation of Russia in the international exchange of information." This law also ascribes a powerful role to the government in the provision of resources with private investors being largely secondary (Ellis, 1999, p.155). One notable provision of this law is that "the dissemination of unreliable false foreign documentary information received as a result of international exchange, on the territory of the Russian Federation is not permitted," which presents a threat to free speech online[14] (Ellis, 1999, p.157). The use of the qualifiers "unreliable" and "false" for determining what information is prohibited opens up the Internet to possible broad and inappropriate interpretations of the terms. This argument is similar to the fear of broad interpretations for the word "extremism" as discussed later in this section under the 2002 Law against Extremism.

In June 2000, the Security Council adopted the Information Security Doctrine, which was designed to strengthen the government's role in monitoring the information

[14] The ACLU challenged a similar provision in the American government's Communications Decency Act of 1996. Its goal was to limit the spread of materials deemed "indecent" and "patently offensive". For more information see: Franda, 2002, 157-160.

sphere (Franda, 2002, p.112). It also laid out the “official views on the goals, objectives, principles and basic guidelines for ensuring information security in the Russian Federation” ("Information Security Doctrine of the Russian Federation," 2008). Putin justified the doctrine by saying that “the state has lost the capability of informing society and that the Information Security Doctrine will create the appropriate state mechanism.” Although he stated that the ideas put forth by the doctrine will “safeguard journalist’s rights, help crackdown on computer crime, and support the telecommunications industry,” those who wish to see the Internet continue as a free space for the flow of information were alarmed by some of the measures implemented after the adoption of the doctrine. In May 2000, for example, the government implemented a law that allowed security services to tap into email messages and other Internet content, using procedures that include the mention of a search warrant, but are not clearly defined (Franda, 2002, p.112).

After the adoption of the Information Security Doctrine, a series of laws were passed regulating different aspects of the information sphere, effectively cementing the government’s role in setting guidelines for the use of the Internet and computer networks. The Federal Law on Communications of 2003 protected the secrecy of communications, provided a simplified licensing regime for ISPs, and guaranteed that restrictions on individual privacy are only allowed after a court order, unless otherwise noted by federal law ("Russia," 2010, p.215). “Measures Providing Information Security to the Russian Federation in the Information Exchange area” is a presidential decree signed in 2004 that restricts government officials, whose computers have access to classified information, from accessing the Internet ("Russia," 2010, p. 215). In 2006, Russia adopted the law on Personal Data and the Law on Information, Information Technologies, and the Protection of Information[15]. These laws established a new legal framework for handling access to personal data and public information. Although the Law on Personal Data provides security for the individual's data, the law also provides broad exemptions for the government in processing this data ("Russia," 2010, p.215). The Law On Information, Information Technologies, and the Protection of Information provides legal definitions for the information sphere and information technologies, as well as providing guidelines on the right of access to information and the restrictions on that access. Interestingly, the law states that restriction to information shall be established by federal acts or for "purposes of protection of the constitutional system, morality, health, rights and legal interests of other persons, provision of the defense of the country and security of the state" (Organization for Security and Co-operation in Europe, n.d.).

In December of 2008, a presidential decree established the Federal Service for Supervision in the sphere of Telecom, Information Technologies, and Mass Communications (Federal'naya Sluzhba po Nadzoru v Sfere Svyazi, Informacionnyx Tekhnologii i Massovyx Kommunikacii or Roskomnadzor). Similar in idea to its Soviet predecessors Gostelradio and Glavlit, Roskomnadzor is "a federal executive authority entitled to carry out permitting and licensing activities, validation and supervision in the spheres of telecommunications, information technologies, and mass communications" ("Federal Service for Supervision in the Sphere of Telecom, Information Technologies

[15] For an English translation of the entirety of the Law On Information, Information Technologies, and the Protection of Information, see: http://legislationline.org/documents/action/popup/id/17757

and Mass Communications (ROSKOMNADZOR)," 2013). Roskomnadzor is under the jurisdiction of the Ministry of Telecom and Mass Communications of the Russian Federation ("Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR)," 2013).

The Constitution of the Russian Federation grants citizens the right to free speech, however this right is often not extended to Internet users and currently there are no special laws protecting online speech. As a result, online journalists do not possess the same rights as offline journalists unless their websites are registered as mass media (Freedom on the Net 2013: Russia, 2013, p.9). Under the Law on Mass Media, enforced as of 1991, the Internet is not specifically regulated, although Article 2 of the law may provide language for just that. The article states that the law covers “other forms of periodic distribution of mass information”, and thus theoretically gives the government grounds on which to prosecute people for opinions expressed on the Internet. The problem here is that requiring all websites, which qualify as ‘media’, to register as mass media outlets is almost impossible, however only registered websites are subject to the media law restrictions, as well as its protections. By 2009, there were around 20,000 registered websites, probably because there are benefits to being an official registered media outlet ("Russia," 2010, p.216). In 2013, United Russia considered an amendment to the media law that would define popular blogs as mass media outlets, however the actual approval of this proposal is viewed as a stretch (Bogodvid, Russia Today, 2013).

Under the guise of protecting children, one of the most recent and worrisome laws enacted that directly controls information on the Internet is Federal Law #139-FZ.

Enacted in November 2012, it has been dubbed in the press as the “Internet blacklist law.” Until its enactment, no law has solely targeted the Internet for censorship of access to information[16]. Under this law, authorities can place websites deemed harmful to the health and development of children on a blacklist of sites that ISPs are required to block without court rulings. Websites deemed harmful to the health and development of children, such as those depicting child abuse or pornography, information about committing suicide, or drug use, can be placed on this list within two days. Roskomnadzor decides the fate of the blacklisted websites (Freedom on the Net 2013: Russia, 2013, p.5). Although the law is portrayed as protecting the safety of children, critics foresee problems with it. Because prosecutors can and do call website owners and ISPs first to coerce them into removing unwanted content, self-censorship of what goes on the site is encouraged to avoid responsibility for both direct and indirect violations, such as ads placed on the site depicting drugs or porn. Implementation of the law has led to a trend of opposition sites moving to foreign site hosting providers in order to escape persecution (Freedom on the Net 2013: Russia, 2013, p.6-8). Skeptics of the law also worry that the government could seek to expand the now limited list of banned items, and that the law opens itself up for misuse and further censorship ("Russia's Parliament Votes for Internet Censorship Law," 2012). When the law came into force, 4,000 sites that shared IP addresses with banned sites were blocked, and many other websites were blocked for “arbitrary reasons”[17] (Freedom on the Net 2013: Russia, 2013, p.5). Because

[16] Although the next section examines extremist laws, which do prosecute Internet users and block extremist content, these laws target all forms of media.

[17] For example, a site called Lurkmore.ru was blocked for posting material on marijuana use (Cross, 14). Lurkmore is a “user-generated encyclopedia focusing on obscure Internet jokes and memes”. The site had an entry for a dudka, which is slang for a bong. (Economist)

sites are banned by IP address, the site can simply change its address to get around the ban, but any other sites that share the same IP address can be blocked as well. The lack of transparency involved in the blocking process is troubling to those wary of the law's potential usage ("Internet Censorship in Russia: Lurk No More," 2012).

Although The Federal Law on Combating Extremist Activity[18] is relatively old, it has come back into the spotlight due to an increase in prosecution of protest and opposition activity under the law in recent years. The cases of Internet users prosecuted by this law seem to be on the rise as well (Kravchenko, 2013). The anti-extremism laws may have been the inspiration for the Internet blacklist law, which broadens what can be prosecuted online to that which is specifically harmful to children. Adopted in 2002, this law 'defined' extremism and has been used to combat the dissemination of material that might incite violence or racial hatred, although the law does not require establishing use of threats for violence in order to prosecute. This has resulted in the law being used against peaceful religious groups such as Hare Krishnas, Scientologists, and Jehovah's Witnesses. The law was originally supposed to fight extremism and terrorism in the country; as such, the law has targeted many Islamic publications and groups, as well as extreme nationalist groups, such as the Skinheads or Nazis. However as more and more items are added to the list of extremist activities and banned materials, there are questions

[18] For a full English translation of the Federal Law On Combating Extremist Activity, see: file:///C:/Users/ktjo89/Downloads/RF_law_combating_extremist_activity_2002_am2008_en.pdf

as to the validity and broad interpretation of what counts as "extremism"[19] (Cross, 2013, 9-14).

While there are multiple articles in the Russian criminal code that can be used to prosecute the various definitions of extremism, Article 282 deals with prosecuting acts of extremism that incite hatred or are insult related. It is one of the oft-cited codes that provides ground for the prosecution of extremist activities, but it does not deal directly with acts of violence, which makes it problematic because, in essence, people are being criminally prosecuted for an insult towards another person or group (Kravchenko, 2013). The code states that "incitement of national, racial, or religious enmity, abasement of human dignity, and also propaganda of the exceptionality, superiority, or inferiority of individuals by reason of their attitude to religion, national, or racial affiliation, if these acts have been committed in public or with the use of mass media" is punishable by fines of up to two years salary and up to two years in prison. For example, Bankfax, a content provider, was charged under the extremism code for insulting a group by calling them oligarchs ("Russia," 2010, p.217). The case of Ivan Moseev, the president of the Association of Pomors of the Arkhangelsk Region, opened in July 2012, who was charged under Part 1 of Article 282 ("incitement of hatred or enmity, or humiliation of human dignity") is a well-known case of prosecution for extremism. According to investigators, Moseev left a comment, insulting ethnic Russians, on the Web site of the online news agency Ekho Severa under the username "Pomor" (Kravchenko, 2013). In December 2012 Smolensk City Council Deputy Andrei Ershov was prosecuted under the

[19] For a detailed study of the inappropriate use of the anti-extremist laws see, Kravchenko, M. (2013, June 26). Inappropriate Enforcement of Anti-Extremist Legislation in Russia in 2012 (Rep.). Retrieved http://www.sova-center.ru/

same article in the December 2012 for his statement about former juvenile prisoners of Nazi concentration camps (Kravchenko, 2013).

The main criticism concerning the laws on extremist activities is the broad interpretation of the word extremism, which has recently included negative comments about the government or the ruling United Russia party.[20] The Internet used to be a place where users felt free from repression, however with the turn in recent years to arresting or blocking those who speak out against the government[21] under the banner of extremism, many Russians are becoming wary that blocking websites or content classified as 'extremist' will lead to widespread censorship of the web (Cross, 2013, p.15). Aggravating factors for extremism charges include the Internet and social media platforms because existing laws do not differentiate between online and offline activities (Freedom on the Net 2013: Russia, 2013, p.10). The ban against public incitement opens up prosecution to seemingly anyone who uses the Internet to make provocative comments.[22] For example, in 2012, a blogger was sentenced to 11 months in labor camp for a terse article about the governor of the Kemerov region. A criminal case was also opened against a blogger in 2012 for writing a blog post encouraging an unauthorized protest and using force against police (Cross, 2013, p.15).

The cases of prosecuting extremism among online communities are on the rise with 103 cases in 2012, up from 38 in 2011 (Cross, 2013, p.15). Russia's former Minister

[20] For examples of prosecution under the extremism laws for speech against the government see: http://grani.ru/Internet/m.196855.html; http://en.gazeta.ru/news/2012/03/21/a_4099301.shtml

[21] Not only those bloggers who speak out against the government are being prosecuted for extremism. Religious hatred is a crime as well, and has included those who speak out against the Russian Orthodox Church. For an example of a blogger charged for statements against the Church, see: http://en.gazeta.ru/news/2012/04/13/a_4345165.shtml

[22] For example, in 2012 more people were convicted for hate speech than hate crimes (Wilson Center).

of Interior Rashid Nurgaliyev suggested that monitoring of mass media, including YouTube and Facebook, was necessary for managing "hate mongering" and "extremism". Although the "Internet blacklist" is limited to child porn, drug abuse, and suicide, Roskomnador would still monitor for other unlawful information that could instigate national religious hatred or war propaganda. Any content on the Internet that is thought to violate extremism laws will be removed (Cross, 2013, p.4). The Russian Ministry of Justice keeps a list[23] of all prohibited extremist content, which ISPs are instructed to block or face legal consequences (UNICEF, Beger, Hoveyda, & Sinha, 2011, p.21). As such, the extremist laws and blacklist law seem to be working in tandem to combat online "threats" (whatever these "threats" are defined as) to national security and the moral underpinnings of society (Cross, 2013, p.4). Government officials have been actively exploring the question of whether social networking services could represent a national security threat, organizing a major conference entitled "Social Networking Services in the Contexts of National and International Security" (Cross, 2013, 4).

National security concerns are not only present in regards to 'extremism' and other online threats. In January 2013, Putin signed Decree #31c "On the formation of a state system for detecting, preventing and mitigating the effects of computer attacks on the information resources of the Russian Federation" (Freedom on the Net 2013: Russia, 2013, p.13). Under this decree, the FSB is responsible for developing methods to prevent and investigate hacker attacks on Russian computer networks and for "promoting

[23] There are currently 2242 items on the Ministry of Justice's list of extremist materials. For a complete listing see: http://minjust.ru/ru/extremist-materials?search=&page=11.

international cooperation in the fight against cybercrime" (Freedom on the Net 2013: Russia, 2013, p.13).

The Restructuring of the Intelligence Services in Response to the Internet

The Russian federal security services have launched several programs to control information published online, with the FSB, Interior Ministry, SVR, and the Investigative Committee acquiring new software systems to monitor social networks and identify participants in online debates. One such program is called Semantic Archive, whose task is to monitor any open data, like media archives, online sources, blogs, and social networks, and then analyze it to produce "objects of interest" (Soldatov & Borogan, 2013).

The FSB's Information Security Center, located within the FSB's counter intelligence directorate, seems to be the leader of the fight for control of the Internet (Borogan & Soldatov, 2010, p.243). At first, the Center was charged with protecting computer networks against hackers, but as of the later 2000's it became responsible for monitoring social networks and the Internet as a whole (Soldatov & Borogan, 2013). Presidential edict No. 31 in February 2013 tasked the FSB with "establishing a nationwide system for protecting Russia's critical information structure, including the exchange of information with foreign governments" (Soldatov & Borogan, 2013). It is likely that the Information Security Center will head up this task (Soldatov & Borogan, 2013).

Department "K" was established within the Ministry of Internal Affairs to "monitor for compliance with the regulations in cyberspace" ("Russia," 2010, p.218). The special department has branches in different regions and is tasked with investigating crimes in the sphere of information technologies, including online hate speech and defamation, especially of officials, unauthorized access to computer systems and networks, and the distribution of pirated software ("Russia," 2010, p.217).

Information is scarce in regards to the extent that the intelligence services have been restructured, added new departments, or employed new tools in response to the growing use of the Internet. Considering the examples in this section, it is clear that the government and the intelligence services are developing responses to the growth of the Internet in Russia and the growing use of social media networks. It is also clear that they are worried about the potential derogatory effects posed by widespread Internet usage; out of this worry arose a desire for monitoring the information sphere.[24]

[24] For comparative information on how other regimes interested in controlling the Internet have responded, see: Kalathil, S., & Boas, T. C. (2003). Open networks, closed regimes: The impact of the Internet on authoritarian rule. Washington, D.C.: Carnegie Endowment for International Peace.

Case Study: SORM

Outside regulatory laws, the government also has the power to conduct surveillance on communications, including Internet activities. Surveillance is important to the discussion of control because although it is different from overt methods, such as banning certain publications or jamming foreign radio broadcasts, it still signifies the desire for control through knowledge of information flow and communications. As already discussed in earlier sections, the security services throughout Russian history have monitored communications where they thought subversive conversations and materials could be present. This case study is relevant to the thesis because it will examine a concrete example of how the FSB uses surveillance to exert control over the Internet in Russia today, whether it be through user's knowledge that the government could be listening or through outright judicial action aimed at the owners or providers of the information collected.

The mechanism used by the FSB to conduct surveillance is SORM (Sistema Operativno-Rozysknyx Meropriyatii) or the System for Operational Investigative Activities. The term is both used to refer to the legal framework underlying the FSB's ability to conduct surveillance and the system itself. SORM can trace its foundations to a KGB research institute in the mid-1980s, although the adoption of the Law on Systems for Operational Activity (SORM) did not come until 1995. This law authorized the FSB to monitor communications from postal correspondence to cell-phone calls and electronic mail, as long as agents obtained a warrant from the court (Tracy, 2000). Adopted in 1999, but not coming into effect until July 2000, SORM-II, which served as an amendment to SORM-I, requires ISPs to provide the FSB access to Internet traffic statistics including “the time of an online session, the IP address of the user, and the data that was transmitted” ("Commonwealth of Independent States," 2010, p.127). The law requires ISPs to install the necessary system hardware and connections, and conduct maintenance at their own cost; noncompliance brings fines and the possibility of the loss of their license (Freedom on the Net 2013: Russia, 2013, p.12). Shortly after Putin first took office as president, the list of agencies that can monitor communications under SORM was expanded to include the tax police, Ministry of Internal Affairs, Border Guards, Presidential Security Service, Kremlin Security Service, parliamentary security service, and the Foreign Intelligence Service ("Russia," 2010, p.219). Today, SORM is still in effect and enforced through the current regulatory document “Order No. 6 of the Ministry of Information Technologies and Communications of the Russian Federation dated January 16, 2008 (Елагин, n.d.).

Under the law, Russian authorities are technically required to obtain a court order before accessing electronic communications data. Since there is no mechanism blocking unauthorized access, court orders may not always be obtained beforehand, which is a troublesome thought for Internet users ("Russia," 2010, p.218). The system works like this: the FSB owns special control centers, which are connected directly to the computer servers. To monitor any type of communication, an FSB agent simply enters their request into the control center located in their local FSB headquarters; no direct contact with the

ISP is required. In every Russian town, “there are protected underground cables, which connect the local FSB bureau with all Internet Service Providers (ISPs) and telecom providers in the region” (Soldatov & Borogan, 2013). Another issue with the process of obtaining data is that ISPs cannot demand that the FSB show them the warrant. Although ISPs are required to pay for the installation of SORM equipment, they are denied access to the surveillance boxes and do not know whose or what kinds of data the FSB is intercepting (Soldatov & Borogan, 2012).

The system is comparable to Western systems of surveillance, specifically the Carnivore/DCS1000 software used by the U.S. Federal Bureau of Investigation, although there are some key differences (when the Western systems are used correctly according to the law) (Freedom on the Net 2013: Russia, 2013, p.12). In the US and Western Europe, the law enforcement agency needs to submit a request to the ISP, who then intercepts and provides the requested data (Soldatov & Borogan, 2012). As already outlined above, the FSB does not need to contact the ISP directly, as the SORM system is already connected to the server and all of the surveillance and data collection is done through the FSB control centers.

Russia is not the only country in the region that employs communications surveillance systems. Kazakhstan, Uzbekistan, Belarus, and Ukraine have all passed regulations that allow for the installation of SORM-II or similar systems ("Commonwealth of Independent States," 2010, p.128). One of the heads of the SORM testing laboratory in the St. Petersburg branch of the Central Research Institute of

Communications acknowledged that Ukraine's system is more restrictive than Russia's, because it possesses the ability to interrupt the conversation (Soldatov & Borogan, 2012).

Although SORM seems like an ominous all-knowing force, it is unlikely that the FSB can legitimately surveil every piece of Internet traffic that comes through, especially with the continued rise of Internet usage. In reality, random surveillance of all communications is unlikely to produce any results. Also, SORM only gives the FSB access to services physically hosted on Russian territory (Soldatov, 2014). This, however, does not mean that SORM cannot be considered a blatant invasion of privacy with a severe lack of oversight ("Russia," 2010, p.219).

It is a stretch to say the FSB is watching everyone at all times, yet critics point out that the FSB may be targeting certain individuals or groups, who are a part of the anti-Kremlin/Putin opposition. Because the FSB has access to websites through direct server connections, they have the ability to monitor closed groups and accounts on Russian social networks like Vkontakte and Odnoklassniki; Facebook and Twitter are not hosted in Russia, thus surveillance of those sites is technically illegal (Soldatov & Borogan, 2013). However, on June 18th 2013, during the trial of ChronoPay owner Paul Wroblewski, who was charged with conducting Distributed Denial of Service (DDoS) attacks on a rival pay agency's server, it was revealed that the FSB hacked into Facebook servers to collect information for use in Wroblewski's trial. Although Wroblewski's lawyer Pavel Zaitsev protested the inclusion of the conversation obtained through Facebook because it was obtained through illegal hacking of his Facebook account, the court allowed the information as evidence in the trial. The FSB supposedly first requested the information through official channels, since Facebook servers are located in the US out of the reach of SORM, however when the request was denied the FSB simply hacked the account (Lenta.ru, 2013).

There is increasing evidence that Russian surveillance technology is being used for political purposes, including the targeting of opposition leaders. In a Supreme Court case in November 2012 against Maxim Petlin, an opposition leader in the city of Yekaterinburg, the court upheld the government's right to eavesdrop on Petlin's phone conversations using SORM because he had taken part in so-called "extremist activities": rallies where calls against extending the powers of Russia's security services were overheard (Freedom on the Net 2013: Russia, 2013, p.12; Soldatov & Borogan, 2012). Wiretaps of opposition activist Alexei Navalny's telephone conversations were used as evidence against him in court when he was put on trial in 2013 for embezzlement charges (Blyth, 2013). In December 2011, during the first post-election anti-Putin protest rallies, the opposition believes it observed use of the SORM system on its leaders. On December 19, 2011, records of nine taped phone calls between Boris Nemtsov, former deputy prime minister and opposition leader, and other activists were posted on the Kremlin-friendly website lifenews.ru days before one of the biggest protest rallies "For Fair Elections". Since then, leaks of compromising video footage and audio recordings of opposition activists have appeared almost regularly on the Internet and in pro-government media (Soldatov & Borogan, 2012).

Putin defended Russia's surveillance activities as a "fight against terrorism" during a televised interview with Russia Today in early June 2013 (Blyth, 2013).

However, immediately after the Arab Spring, the government began looking at the threat to political stability seemingly posed by social networks. In August 2011, the main topics of discussion at a summit of the Collective Security Treaty Organization (CSTO), a regional military alliance led by Moscow, "were the revolutions in the Middle East and the role played by social networks" (Soldatov & Borogan, 2013). The summit, which then Russian president Dmitry Medvedev attended, "adopted a confidential document recognizing the potential danger of social media in the organization of protests in Russia" (Soldatov & Borogan, 2013).

It is also widely reported that the Sochi Olympics were heavily monitored by the FSB using SORM. Every athlete, journalist, and spectator was subject to monitoring through their cell phones, Internet usage, and any other forms of electronic communications, in response to the increased threat posed to the games by Chechen terrorists. It is possible the system will be used to conduct surveillance to track protests regarding gay rights or other human rights issues (Walker, 2013). Whomever the government is targeting, evidence shows that surveillance attempts are not slowing down. According to figures released by Russia's Supreme Court, "the number of intercepted telephone conversations and email messages has doubled in six years, from 265,937 in 2007 to 539,864 in 2012" (Soldatov & Borogan, 2013). The warnings from Roskomnadzor issued to ISPs and telecom providers who failed to meet the FSBs obligations increased as well, with 16 warnings in 2010, down to 13 in 2011, but a jump to 30 warnings in 2012 (Soldatov & Borogan, 2013).

Case Study: The Attempted Control of Alexei Navalny

While the previous case study focused on the efforts by the FSB to conduct surveillance on ‘suspicious’ individuals or groups, this section will focus on efforts to overtly control those who are deemed suspicious or detrimental to national security in some way. Because efforts to control often intersect with the world of criminal proceedings, this section will not focus solely on the FSB’s efforts, but also those of any other government, intelligence, or police agency that attempts to control the blogosphere. This case study focuses on the control of the online political opposition, specifically the de facto leader of the political opposition, Alexei Navalny. The study demonstrates in detail what tactics the security services are actively employing to control the online and offline communications of the political opposition, and highlights why the government is interested in targeting Navalny in particular. The case of Navalny concretely demonstrates that the government is continuing to use control methods against those who speak ill of the government and other elites. This section shows the multitude of agencies, namely the Investigative Committee, the FSB, and the Kremlin itself, working in tandem to control the opposition. Similar to previous periods in Russian history, namely the Stalinist and tsarist periods, Putin and other ruling elites seem to have a say in who is targeted, especially in the case of Navalny who continually exposes or defames political and economic figures he feels are corrupt. This section also shows that not only are the opposition being singled out for increased surveillance, but also for outright control using tactics within the boundaries of the legal framework. The case of the control of the online opposition brings out the theme present throughout this thesis, where Russian leaders want to develop a modern infrastructure in the country (i.e. the Internet), but must also figure out how to control a modern communication system because of the potential it brings for the appearance of subversive rhetoric towards the state.

Alexei Navalny is a lawyer by trade, who began blogging in 2008, addressing issues of corruption in major corporations ("Profile: Russian Opposition Leader Alexei Navalny," 2013). Navalny is also co-founder of the Democratic Alternative movement and was vice-chairman of the Moscow branch of the political party YABLOKO, until he was ousted from the party in 2007 (Coalson, 2013). With the aim of exposing corruption, Navalny became a "minority shareholder in major oil companies, banks and ministries in order to ask awkward questions about holes in state finances" ("Profile: Russian Opposition Leader Alexei Navalny," 2013). In 2010, he launched RosPil, a web-based anti-corruption platform, which serves as a "public repository of tips and evidence of violations within the state procurement system" (Milashina, Ognianova, & CPJ Europe and Central Asia Program, 2013). Continuing his activities as an anti-corruption activist, in 2011 he started RosYama, an organization combating fraud in the road construction sector ("Alexey Navalny Bio," n.d.). Eventually he turned his attention to criticizing Putin, as well as the entire ruling party, United Russia, for rampant corruption. Navalny's method of public criticism involved "reaching out to predominantly young followers on social media in sharp, punchy language, mocking the establishment loyal to President Vladimir Putin" ("Profile: Russian Opposition Leader Alexei Navalny," 2013).

Navalny’s fame would rise, and consequently turn the Putin regime’s gaze towards his increasingly problematic behavior after the 2011 parliamentary election, during which he urged his blog readers to vote for any party except United Russia ("Profile: Russian Opposition Leader Alexei Navalny," 2013). After the election results came back in which United Russia still gained the majority of seats in Parliament, Navalny called those frustrated with the results to take to the streets and protest, using his blogs and Twitter feed to make his calls to action (Barry, 2011). During the first protest on Dec. 5, 2011, Navalny was arrested and jailed on charges of resisting police, but was later able to speak at the biggest post-election rallies in Moscow on December 24, attended by as many as 120,000 people ("Profile: Russian Opposition Leader Alexei Navalny," 2013). Since these massive protests took place, Navalny has emerged as the unofficial leader of the protests and a uniting force behind an opposition movement that in the past has been troubled with fragmentation and disorganization. Although Navalny began his work as an activist whose goal was to combat corruption and work for fair elections, he has become more interested in playing an active role as a politician. In September 2012, Navalny ran in the Moscow mayoral race and came in second with 27% of the vote (Mills, 2013).

Although Navalny is popular among bloggers and the young and politically active in the large cities, he and the opposition are not believed to have strong support from other demographics in Russia. According to a Levada Center poll, Navalny’s name was known by only 6 percent of the population in April 2011. That number has steadily increased since then to 54% in October 2013, with the latest poll results in January 2014 showing an interesting decline to only 45% of the population having knowledge of the activist. However, that same poll only shows 17% of respondents stating they would vote for Navalny if he ran for a seat in parliament, and only 2% responding with ‘definitely yes’ (Levada Center, 2014).

Navalny’s fight against corruption and for fair elections was a cause that all who oppose Putin and the ruling party could rally around. Factors of charisma aside, this is seen as a major reason for his leadership status within the opposition (Judah, 2013; Coalson, 2013). However, many more liberal opposition figures are worried about Navalny’s nationalist policies, associations in protests attended by Skinheads and other ultra-nationalist groups, and his advocating for issues affecting ethnic Russians (Guillory, 2011). Moscow Carnegie Center analyst Lilia Shevtsova suggests that Navalny does not have the support of everyone who is frustrated and that he will not become a real political figure, rather than just a social activist, until he forms a clearer and broader agenda (Sanford, 2013).

The Kremlin’s interest in Navalny is unquestionable. His ability to translate his activism from the blogosphere and turn it into a protest movement, known as online to offline activism, is troublesome, along with the fact he is a Yale World Fellow (following a semester he spent there in 2010), which concerns those who are wary of US influence ("Profile: Russian Opposition Leader Alexei Navalny," 2013). The Kremlin has long controlled Russia's leading TV channels, which are still the main source of news for most Russians, and therefore the Internet has become a safe haven for opposition bloggers and activists to convey their grievances against the government. Of all the opposition figures, the Kremlin may fear Navalny the most. Pro-regime websites and television stations portray him as a CIA operative or Hitler-like nationalist. He is the only opposition leader unofficially barred from state-controlled television. For example, when television host Ksenia Sobchak invited Navalny on her popular show on Russian MTV, it was taken off the air, presumably due to government orders (Kaminski, n.d.).

The three main ways that the government controls dissenting online speech, especially of those within the political opposition movement, are through the dissemination of counter pro-government propaganda; offline attacks, arrests, or threats; and distributed denial of service attacks (Alexanyan et al., 2012, p.11-12). Navalny and his blogs, Twitter, etc…, are continually direct and indirect targets of these tactics.

Manipulation efforts by the government include “employing” (which can mean calling on youth organizations or other pro-Kremlin groups) bloggers to spread the President’s message online; disrupting the online activities of Kremlin opponents by using abusive language, preventing or trolling discussions; and/or acting in an organized way to prevent certain issues from making it on the Yandex Top 20 list of headlines (Fossato, et. al.,, 2013, p.110-111). Political technologists, as they are called, make ample use of these tactics and social media technologies (Fossato, et.al, 2013, p.111).

In December 2011, during the protests of the parliamentary elections, “thousands of Twitter accounts apparently created in advance to blast automated messages were being used to drown out Tweets sent by bloggers and activists” ("Krebs on Security", 2011). #Triumfalnaya, the hashtag referring to the protests on Triumfalnaya Square in Moscow, was spammed with pro-Kremlin tweets sent by what looked to be Twitter bots, drowning out the message traffic from legitimate protesters trying to Tweet out information. Thousands more accounts were found that were “rapidly posting anti-protester or pro-Kremlin spam to more than a dozen hashtags and keywords that protesters were using to share news, including #Navalny” (“Krebs on Security”, 2011). Most of the accounts were created at the beginning of July 2011, and have very few tweets other than those “meant to counter the protesters, or to simply fill the hashtag feeds with meaningless garbage” ("Krebs on Security", 2011).

Social media companies have received pressure from the government to quiet the opposition. In 2012, an official of Vkontakte, reported pressure from the FSB to block access to opposition groups, but said his company refused. A top Interior Ministry official also proposed that “all social media users be required to register their legal names and addresses,” which would make it easier for the government to track down those who use pseudonyms or are anonymous (Mackinnon, 2012). Instances of hacking or DDoS attacks against Navalny and the opposition are on the rise. The popular Russian blogging site LiveJournal.com came under heavy DDoS attacks from at least two different botnets in April 2011, targeting Alexey Navalny’s blog as well as other controversial sites. These attacks came after Navalny began attacking United Russia by calling them the “party of crooks and thieves”. Navalny's blogs were spammed with derogatory comments and at least one advertisement was found online which offered $14,000 rubles per month for individuals to continue the campaign against Navalny. There is suspicion that members of Nashi, the pro-Kremlin youth organization, are responsible for the attacks against Navalny and LiveJournal (Carr, 2011).

Navalny won the most votes in a three-day online poll asking voters whom in the opposition they would put on a Coordinating Committee. Although the Kremlin officially ignored the poll, attacks on candidates in the media and cyber strikes on the ballot's website, which could not be accessed at times, still occurred. Voting was extended another day because the website had been hacked. Opposition officials said the voting had also been disrupted in Chelyabinsk, “because of a search by agents from the Federal Security Service” ("Anti-Putin Opposition Elected in Russian Online Poll," 2012).

Navalny has asked investigators to look into whether law enforcement officials helped hackers break into his e-mail and Twitter accounts in June 2012. Navalny's Twitter account was taken over by a hacker named “Hell” who insulted Navalny’s supporters and claimed that he had been working for President Vladimir Putin all along.[25] After the head of the independent Golos election-monitoring group Lilia Shibanova’s, laptop was seized at Sheremetyevo airport, emails from her personal account appeared on Lifenews.ru. The authorities have denied connections to the attacks, and no one has been charged in connection with the hacker attacks or leaks, which is a common occurrence for similar attacks (Earle & Martinez, 2012).

Navalny is famous for getting into trouble with the police during protests, and for investigations of fraud launched against him. In 2009, Navalny was accused of embezzling $500,000 worth of stolen timber while working as an adviser for the Kirov regional governor, however those charges were later dropped. In July 2012, Navalny

[25] The hacker also “changed the account's avatar to a photograph of d'Artagnan, the hero of Alexandre Dumas' "The Three Musketeers," with the caption "You are all pedophiles, and I am d'Artagnan!" and a new profile description: ‘Crook and thief Navalny's e-mail account, leaking hundreds of personal e-mails onto the Internet Alexei Navalny 2.0.’”. The hacker also claimed to have previously hacked into Navalny's e-mail account, leaking hundreds of personal e-mails onto the Internet (Earle and Martinez)

accused Aleksandr Bastrykin, head of Russia's Investigative Committee, also known as Sledkom, of having property holdings in the Czech Republic, which would be going against Russian norms of not holding property in a NATO country. Navalny published documents and a statement from Czech authorities supporting the allegations, however, Bastrykin denied the charges. After this incident, Sledkom reopened the embezzlement case against Navalny and brought forth charges in the same month as the accusation (Denber, 2013). The embezzlement charge was not only denied by Navalny, but also by the Kirov regional governor who testified as a prosecution witness (Milashina, Ognianova, & CPJ Europe and Central Asia Program, 2013). Navalny was tried and found guilty, sentenced to five years in jail. However, the next day he was released on bail through appeal and subsequently was allowed to run in Moscow's mayoral elections in September. The court later amended his jail term on appeal to a suspended sentence (Walker, 2013).

"Sledkom has become a major player in the clampdown on the protest movement, and Alexei Navalny its biggest target to date" (Sanford, 2013). According to Sledkom, a company run by Navalny conducted fraud against the now defunct party Union of the Right Forces in 2007 by taking payment for advertising and not fulfilling the contract. If convicted, Navalny could be jailed for up to 10 years. The Investigative Committee also previously charged Navalny and his brother with embezzling 55m roubles in 2008-11 while working in a postal business ("Russian Opposition Leader Navalny Faces Third Inquiry," 2012). Sledkom has also brought into question Navalny's credentials as a lawyer. A statement said that on Navalny's application to be a lawyer, he stated he had the “necessary two years' work experience as a legal specialist”, however investigators contend this is not true ("Russia's Alexei Navalny Accused of New Fraud," 2013).

Conclusion

The Internet in Russia is an interesting case study because for much of its existence, Russians have generally regarded it as a free and open space, even a place for people to “let off steam” (Aron, 2011). Both Medvedev and Putin have expressed positive views towards the Internet as a modernizing force for Russia. In an attempt to show that Russia is able to participate in the modern world, we have seen Medvedev open a Twitter account and start a blog, and Putin open government websites to increase communication with the public, as well as champion correspondence through email. For years, Putin and Medvedev showed no interest in controlling or censoring the Internet on a massive scale, with Putin defending the freedom of the Internet repeatedly. However, in recent years, there have been increasing numbers of calls for Internet regulation throughout the ranks of government and increasing numbers of threats and arrests against those who have said things against the government or something that falls under the broad definition of extremism. This call for a government hand in the information sphere began with the Information Security Doctrine in 2000, which provides the justifications and suggestions for shaping policy, citing a lack of government oversight as a threat to information security in Russia, along with terrorism and foreign governments. The doctrine states that it is important to convey reliable and trustworthy information to both the Russian and international public, with one suggestion to achieve this goal by bolstering state mass media. According to the doctrine, national interests consist of “securing the interests of the individual in the information sphere, reinforcing democracy, creating a rule of law social state, achieving and maintaining public harmony, and of the spiritual renewal of Russia” ("Information Security Doctrine of the Russian Federation," 2008). This means not allowing for “propaganda or campaigning that serves to foment social, racial, national, or religious hatred and strife” ("Information Security Doctrine of the Russian Federation," 2008). The doctrine also mentions interest in the preservation and reinforcement of the moral values of society, traditions of patriotism and humanism, and the cultural and scientific potential of the country. The important role of the development of the information sphere and infrastructure in creating a modernized state is mentioned as well.

Continuities in regards to control methods exist between the Russia of today and the past, namely propaganda and surveillance. Media such as television and radio were crucial in spreading Soviet propaganda, but they also demonstrated that the Soviet Union had modern technologies. Today, the growing popularity of the Internet shows that Russia is a modernizing state, while government propaganda is increasingly found on the Internet in the form of pro-government blogs, attacks against the opposition online, and concerted efforts to hinder the spread of oppositionist information. The difference today is that one can legally find politically controversial information on the Internet. Within certain restrictions, people are relatively free to search for what they want to see, whether it be politics, entertainment, sports, and so on. The Internet looks more like a laxly controlled communication technology during the Gorbachev era than a tightly controlled medium under a totalitarian regime. The blacklist law is worrisome because access to content put on the blacklist is banned outright, normally under a broad interpretation of the terms for blacklisting a source, and signals a possible step towards continuing Soviet era censorship. This raises the question of whether the semi-censored status of the Internet will remain the status quo in the future.

Surveillance over communication has evolved from intercepting and reading mail, to listening in on telephone calls, to having the power to surveil almost every data transmission on computer networks. The concept of surveillance is a subtle form of control and is different from outright control in that it signifies a desire for the knowledge of information flow, which gives the authorities the upper hand in quelling subversion. Surveillance conducted by SORM goes largely unnoticed and only becomes visible when someone is charged for content discovered by SORM. However, the FSB and other agencies have the power to know what is going through the lines of communication. Because it is public knowledge that the FSB carries out this surveillance, users may practice self-censorship and reveals another way that surveillance exhibits control over a population.

We also see the state consolidating power with the security services and an increased blurring of lines between who is monitoring or controlling the internet in Russia. The FSB is not the only government agency allowed to monitor Internet traffic and the Investigative Committee and various policing agencies are becoming more involved in investigating and charging those who post “extremist” or politically oppositionist speech. Roskomnadzor, with its supervision of communication, exhibits parallels with Soviet media control organizations like GlavLit and Gostelradio.

Today, the traditional forms of media are widely understood to be under state control or pro-regime, although in contrast to the total monopoly on state media throughout a large portion of the Soviet period, some independent news sources do exist. The intent for control over access to information on the Internet exists, as exemplified in the Information Security Doctrine, yet the control methods themselves have evolved from the tsarist and Soviet periods in response to the entirely different and modern communication structure of the Internet, social media, and computer networks. The controls that have evolved in regards to the Internet are second and third generation techniques, meaning they are within the legal framework, go largely unnoticed, deal with disseminating the official government message, or are carried out by entities not directly tied to the security services. There is no broad censorship or control of the Internet, and relative to other areas of the world such as China or Uzbekistan, Russia's internet is still largely free. This is quite different than the deliberate state censorship of popular communication technologies and the information that they transmitted during the Soviet period. However, during the nineties and until the later 2000's, access to the Internet was not widespread throughout Russia. It is likely that the government did not place emphasis on controlling the Internet until recent years because it did not affect a large percentage of the population and they did not fully realize the potential (and in recent years, regime-toppling potential) of the Internet to influence people. This is similar to the anecdote that the tsars did not place a large emphasis on controlling what writers and poets wrote about, because the populace was largely illiterate.

Taking into account the discussion of parallels between the past and present use of control over communications technology, it is safe to say that the Russian government and intelligence services are trying to control the Internet and social media, though not in the outright way seen in previous periods. Russia employs second and third generation techniques to control certain forms of information that under the guise of the law are deemed extremist or detrimental to children. Russia's leaders are not trying to control the entire Internet, nor will they put social media under their control; however, they have realized the mobilizing potential of the Internet after the December 2011 election protests. Although Russia is not blindly and explicitly censoring the Internet, and there is no "anti-Internet policy," users are worried because the Internet was always a free place where the politically minded citizens could go to voice their opposition without fear of prosecution. It looks as if this freedom is slowly deteriorating and the frightening fact for many is that this is occurring under a veil of legality, despite increasingly suspect accusations.

Finally, in looking at the control and surveillance of the Internet in Russia, one can possibly extrapolate the reasons why the government would want to exert some control over the Internet and social media sites. Most critics of the Internet crackdown contend that the controls and surveillance are there to undermine the political opposition. It is hard not to see a political reason behind the controls, with the increasing crackdowns coming after a fairly fragmented and disorganized opposition moved their online protest offline into public spaces. The fact is that while there are indeed instances of controls on the online opposition, there are also other forms of expression that are banned, such as many Muslim publications, ultra-nationalist rhetoric, and religious hate speech, as well as many instances of hate speech against the role of the Russian Orthodox Church in politics. While political motivations are a factor, especially in smear campaigns or attacks against those that have addressed negative aspects of a particular policy, there are other dimensions to the reasoning behind the controls. After the Arab Spring, officials in Russia worried about the destabilizing effects of social media for national security. Studies suggest that after the December 2011 protests, calls for controls over the Internet and social media increased, as well as various forms of lawful controls put into action against the opposition. While a political reason is likely behind the push for these controls, there is a more complex answer. When online speech turns into offline activities such as protests, the Internet is no longer a place where there is lively discussion among users and the opinions stop at the computer screen. It is a revolutionary force that can incite instability through action and sometimes violence. Protests over building flats in a public park seem to be fine, but protests in a major city over election fraud denouncing Putin and the government's legitimacy are not (Gladarev & Lonkila, 2012, p.1375). That said, this thesis is not arguing that Putin is only using the guise of extremism and national security to quell protests against his political power and that of the church, with which he has close ties. Government officials, including Putin, repeatedly ask for controls on social media because they believe the West is using these mediums to undermine the government by cultivating protests and oppositionist rhetoric. This shows that wariness against the West and its power to transmit information to the Russian populace through its communication technology has not fallen with the Soviet Union. Russia is a vast territory with many different ethnic groups and political opinions and it would be in the interest of the government to control anything that may incite fighting or instability. In 2011, Russian officials proposed implementing an International Code of Conduct for Information Security, which would ban information “that incites terrorism, secessionism or extremism, or undermines other countries’ political, economic and social stability, as well as their spiritual and cultural environment” (Freedom on the Net 2012: Russia, 2012). The question is whether these threats to national security posed by the Internet are real or imagined, yet their presence in deciding to control the Internet cannot be disputed. In controlling the Internet, there also seems to be a justification for the spiritual and moral improvement of Russia. Anything said that speaks ill of the church is not tolerated under the extremism laws and the “Internet blacklist law” targets drugs, suicide, and child pornography with the aim of protecting children from harmful Internet content. The efforts to create a moral and spiritual space online, when fit together with other efforts to control society, such as the gay propaganda law, and the efforts to quell any threat to national security, show a larger effort to create a moralistic and stable society that ensures a superior Russian culture whose stability and legitimacy is not undermined by external or internal sources.

Due to the novelty of the Internet’s popularity, much research is still needed on the effects of the Internet on Russian society and the controls put upon it. It is interesting to note that Navalny’s most recent arrest came with a symbolic sentence of no access to the Internet or his blogs. The state is recognizing the potential power of the Internet to spread information. However, just as the information revolution during the Soviet period opened up the population to new technologies, influences, and ideas, which led to an irreversible phenomenon that factored in its downfall, it is likely impossible to shut the Internet and its voices down after its potential has already been realized among segments of the population, and especially when those voices do not trust the government. After the fall of the Soviet Union, the state allowed to flourish a horizontal communication network unmatched by other communications technologies in its scope of bringing ideas and people together across time and space. Even as the government tries to recapture its control over communications, the Internet looks to be the network that can hold its ground with its history of free and uncensored thought that users do not want to give up quietly.

References

Alexa Internet Inc. (n.d.). Top Sites in Russia. Retrieved March 1, 2014, from http://www.alexa.com/topsites/countries/RU

Alexanyan, K., Barash, V., Etling, B., Faris, R., Gassey, U., Kelly, J., Roberts, H. (2012, March 2). Exploring Russian Cyberspace: Digitally-Mediated Collective Action and the Networked Public Sphere. Retrieved from http://ssrn.com/abstract%3D2014998

Alexey Navalny Bio. (n.d.). Retrieved from http://worldfellows.yale.edu/alexey-navalny

Analytical Group of Yandex Marketing Department. (2013, Spring). *Development of the Internet in Russia's Regions* (Rep.). Retrieved http://download.yandex.ru/company/ya_russian_regions_report_2013.pdf

Andrew, C. M., & Gordievsky, O. (1990). *KGB: The inside story of its foreign operations from Lenin to Gorbachev*. New York, NY: HarperCollins.

Anti-Putin opposition elected in Russian online poll. (2012, October 23). Retrieved from http://www.bbc.com/news/world-europe-20037209

Aron, L. (2011, June 28). Nyetizdat: How the Internet is building civil society in Russia. Retrieved from http://www.aei.org/

Badenoch, A., Fickers, A., & Henrich-Franke, C. (2013). Airy curtains in the European ether: Broadcasting and the Cold War. Baden-Baden: Nomos.

Barnett, E. (2011, January 13). Runet: Why the Russian internet doesn't need the West. Retrieved from http://www.telegraph.co.uk/technology/news/8255183/Runet-Why-the-Russian-internet-doesnt-need-the-West.html

Barry, E. (2011, December 09). Rousing Russia With a Phrase. Retrieved from http://www.nytimes.com/2011/12/10/world/europe/the-saturday-profile-blogger-aleksei-navalny-rouses-russia.html?_r=1&

Blyth, K. (2013, June 17). PRISM and SORM: Big Brother is watching. Retrieved from http://themoscownews.com/russia/20130617/191621273/PRISM-and-SORM-Big-Brother-is-watching.html

Bogodvid, M. (2013, July 15). Blogs soon to be listed as mass media. Retrieved from http://rt.com/politics/blogs-media-russia-amendment-100/

Bogodvid, M. (2013, May 21). Two Thirds of Russians are Internet Users - Survey. Retrieved from http://en.ria.ru/russia/20130521/181264590.html

Borogan, I., & Soldatov, A. (2010). *The new nobility: The restoration of Russia's security state and the enduring legacy of the KGB*. New York, NY: Public Affairs.

Bulashova, N., Burkov, D., Platonov, A., & Soldatov, A. (2013, May). *Internet in Russia* [Scholarly project]. In *Asia Internet History Project*. Retrieved from https://sites.google.com/site/internethistoryasia/country-region-information/ru

Carr, J. (2011, April 7). The Kremlin's Online Hit Squad. Retrieved from http://jeffreycarr.blogspot.com/2011/04/kremlins-online-hit-squad-nashi-attacks.html

Coalson, R. (2013, July 28). Russia's Aleksei Navalny: Hope Of The Nation -- Or The Nationalists? Retrieved from http://www.rferl.org/content/russia-navalny-nationalist-fears/25059277.html

Commonwealth of Independent States. (2010). Retrieved from https://opennet.net/research/regions/cis

Cross, S. (2013). Russia and Countering Violent Extremism in the Internet and Social Media: Exploring Prospects for U.S.-Russia Cooperation Beyond the "Reset" *Journal of Strategic Security, 6*(4), 1-24. doi: 10.5038/1944-0472.6.4.1

Deibert, R., & Rohozinski, R. (2010). Control and Subversion in Russian Cyberspace. In J. G. Palfrey, J. Zittrain, R. Deibert, & R. Rohozinski (Eds.), *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, MA: MIT Press.

Denber, R. (2013, July 18). By jailing opposition leader Navalny, Putin has silenced a leader and messenger. Retrieved from http://www.theglobeandmail.com/globe-debate/by-jailing-opposition-leader-navalny-putin-is-silencing-all-dissent/article13295985/

Dresen, F. J. (2013). Anti-Extremism Policies in Russia and How they Work in Practice. Retrieved from http://www.wilsoncenter.org/publication/anti-extremism-policies-russia-and-how-they-work-practice

Earle, J., & Martinez, K. (2012, June 27). Navalny Fears State Hand in New Hacking Attack. Retrieved from http://www.themoscowtimes.com/news/article/navalny-fears-state-hand-in-new-hacking-attack/461087.html

Елагин (Elagin), B (V). (n.d.). СОРМ-2 история, становление, перспективы. Retrieved from http://www.sorm-li.ru/sorm2.html

Elder, M. (2012, April 15). Nervous Kremlin seeks to purge Russia's internet of 'western' influences. Retrieved from http://www.theguardian.com/technology/2012/apr/15/kremlin-purge-russia-internet-western-influences

Ellis, F. (1999). *From glasnost to the Internet: Russia's new infosphere*. New York: St. Martin's Press.

Etling, B., Alexanyan, K., Kelly, J., Faris, R., Palfrey, J., & Gassey, U. (2010, October 19). *Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization* [Scholarly project]. In *Berkman Center Research Publication*. Retrieved from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Public_Discourse_in_the_Russian_Blogosphere_2010.pdf

Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR). (2013, December 16). Retrieved from http://rkn.gov.ru/eng/

Fischer, B. B. (1997). *Okhrana the Paris operations of the Russian Imperial Police*. Washington, D.C.: History Staff, Center for the Study of Intelligence, Central Intelligence Agency.

FOM (Фонд Общественное Мнение). (2013, September 18). Для чего люди используют интернет?; For what do people use the Internet? Retrieved from http://fom.ru/SMI-i-internet/11088

FOM (Фонд Общественное Мнение). (2014, January 15). Интернет в России: динамика проникновения: Осень 2013; Internet in Russia: Penetration Dynamics. Fall 2013. Retrieved from http://fom.ru/SMI-i-internet/11288

FOM (Фонд Общественное Мнение). (2014, March 27). О средствах массовой информации; About Mass Media Retrieved from http://fom.ru/SMI-i-internet/11427

Fossato, F., Lloyd, J., & Verkhovsky, A. (2013). The web that failed: How opposition politics and independent initiatives are failing on the Internet in Russia. In N. Berlatsky (Ed.), *Social networking*. Detroit: Greenhaven Press.

Franda, M. F. (2002). *Launching into cyberspace: Internet development and politics in five world regions*. Boulder, CO: Lynne Rienner.

Freedom on the Net 2012: Russia (Rep.). (2012). Retrieved http://www.freedomhouse.org/report/freedom-net/2012/russia#.UyCbBPldX3Y

Freedom on the Net 2013: Russia (Rep.). (2013). Retrieved http://www.freedomhouse.org/report/freedom-net/2013/russia#.UxJCxfldX3Z

Ganley, G. D. (1996). *Unglued empire: The Soviet experience with communications technologies*. Norwood, NJ: Ablex Pub.

Gerovitch, S. (2000). Striving for 'optimal control': Soviet cybernetics as a 'science of government' In M. R. Levin (Ed.), *Cultures of control* (pp. 247-261). Amsterdam: Harwood Academic.

Gerovitch, S. (2008). InterNyet: Why the Soviet Union did not build a nationwide computer network. *History and Technology, 24*(4), 335-350. doi: 10.1080/07341510802044736

Gladarev, B., & Lonkila, M. (2012). The Role of Social Networking Sites in Civic Activism in Russia and Finland. *Europe-Asia Studies, 64*(8), 1375-1394. doi: 10.1080/09668136.2012.712272

Gordin, M., Grunden, W., Walker, M., & Wang, Z. (2003). "Ideologically Correct" Science. In M. Walker (Author), *Science and ideology: A comparative history* (pp. 35-65). London: Routledge.

Graham, L. R. (1993). *The ghost of the executed engineer: Technology and the fall of the Soviet Union*. Cambridge, MA: Harvard University Press.

Guillory, S. (2011, December 26). Russian Opposition Leader Alexei Navalny: Uniting Nationalists and the Urban, Educated Middle Class. Retrieved from http://exiledonline.com/russian-opposition-leader-alexei-navalny-uniting-nationalists-and-the-urban-educated-middle-class/

Hixson, W. L. (1997). *Parting the curtain: Propaganda, culture, and the Cold War, 1945-1961*. New York: St. Martin's Press.

Information Security Doctrine of the Russian Federation. (2008, December 29). Retrieved from http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument

Internet Censorship in Russia: Lurk no more. (2012, November 16). Retrieved from http://www.economist.com/blogs/easternapproaches/2012/11/internet-censorship-russia

Judah, B. (2013, August 21). Navalny: Russia’s opposition hero cult. Retrieved from http://blogs.reuters.com/great-debate/2013/08/21/navalny-russias-opposition-hero-cult/

Kalathil, S., & Boas, T. C. (2003). Open networks, closed regimes: The impact of the Internet on authoritarian rule. Washington, D.C.: Carnegie Endowment for International Peace.

Kaminski, M. (n.d.). The Man Vladimir Putin Fears Most. Retrieved from http://online.wsj.com/news/articles/SB10001424052970203986604577257321601811092

Kenez, P. (1985). *The birth of the propaganda state: Soviet methods of mass mobilization, 1917-1929*. Cambridge: Cambridge University Press.

Kravchenko, M. (2013, June 26). *Inappropriate Enforcement of Anti-Extremist Legislation in Russia in 2012* (Rep.). Retrieved http://www.sova-center.ru/

Krebs on Security [Web log post]. (2011, December 8). Retrieved from http://krebsonsecurity.com/2011/12/twitter-bots-drown-out-anti-kremlin-tweets/

Lenta.ru. (2013, June 19). ФСБ обвинили во взломе фейсбука основателя Chronopay; FSB accused of hacking into the Facebook of the founder of Chronopay. Retrieved from http://lenta.ru/news/2013/06/19/fsb/

Левада-Центр (Levada Center). (2014, February 7). Россияне об Алексее Навальном; Russians on Alexei Navalny. Retrieved from http://www.levada.ru/07-02-2014/rossiyane-ob-aleksee-navalnom

Mackinnon, M. (2012, September 6). Intrepid blogger Putin's worst nightmare. Retrieved from http://www.theglobeandmail.com/news/world/intrepid-blogger-putins-worst-nightmare/article4181050/

Mattelart, A. (1996). *The invention of communication* (S. Emanuel, Trans.). Minneapolis, MN: University of Minnesota Press.

Milashina, E., Ognianova, N., & CPJ Europe and Central Asia Program. (2013, July 8). The targeting of Russian blogger Aleksei Navalny. Retrieved from http://cpj.org/blog/2013/07/targeting-russia-blogger-aleksei-navalny.php

Mills, L. (2013, September 12). Alexei Navalny, Moscow Opposition Candidate, Contests Election Results In Mayor's Race. Retrieved from http://www.huffingtonpost.com/2013/09/12/alexei-navalny-contests-election-results_n_3913226.html

Nelson, M. (1997). War of the black heavens: The battles of Western broadcasting in the Cold War. Syracuse, NY: Syracuse University Press.

Nikiporets-Takigawa, G. (2013). Tweeting the Russian Protests. *Digital Icons,* (9). Retrieved from http://www.digitalicons.org/issue09/files/2013/06/DI_9_1_Nikiporets.pdf

Oates, S. (2013). *Revolution stalled: The political limits of the Internet in the post-Soviet sphere*. Oxford: Oxford University Press.

Organization for Security and Co-operation in Europe. (n.d.). Federal Law "On Information, Information Technologies, and Information Protection", No. 149-FZ, July 27, 2006. Retrieved from http://legislationline.org/documents/action/popup/id/17757

Prabhu, L. P. (2011, November 17). Social Media in Russia. Retrieved from http://www.dreamgrow.com/social-media-in-russia/

Profile: Russian opposition leader Alexei Navalny. (2013, July 19). Retrieved from http://www.bbc.com/news/world-europe-16057045

Rantanen, T. (2002). *The global and the national: Media and communications in post-Communist Russia*. Lanham, MD: Rowman & Littlefield.

Rayfield, D. (2004). *Stalin and his hangmen: The tyrant and those who killed for him*. New York, NY: Random House.

RIA Novosti. (2013, April 24). Russia leads Europe in terms of Internet audience. Retrieved from http://en.ria.ru/regional_company_news/20130424/180824109/Russia-leads-Europe-in-terms-of-Internet-audience-.html

Rocich, Y. (2000, June 7). Internet Development In Russia: Territorial And Institutional Particularities. Retrieved from http://rocich.ru/article/57

Roth-Ey, K. (2011). *Moscow prime time: How the Soviet Union built the media empire that lost the cultural Cold War*. Ithaca, NY: Cornell University Press.

Russia. (2010, December 19). Retrieved from https://opennet.net/research/profiles/russia

Russian Ministry of Justice. (n.d.). Федеральный список экстремистских материалов. Retrieved March 14, 2014, from http://minjust.ru/ru/extremist-materials?search=&page=11

Russian opposition leader Navalny faces third inquiry. (2012, December 24). Retrieved from http://www.bbc.com/news/world-europe-20836116

Russia's Alexei Navalny accused of new fraud. (2013, February 27). Retrieved from http://www.bbc.co.uk/news/world-europe-21598356

Russia's parliament votes for internet censorship law. (2012, July 11). Retrieved from http://www.bbc.com/news/technology-18805039

Sanford, D. (2013, July 19). Alexei Navalny jailed: Russia's Mandela moment? Retrieved from http://www.bbc.com/news/world-europe-23348735

Schmidt, H., Teubener, K., & Konradova, N. (Eds.). (2006). *Control shift: Public and private usages of the Russian internet*. Retrieved from http://www.katy-teubener.de/joomla/images/stories/texts/publikationen/control_shift_01.pdf

Shane, S. (1994). *Dismantling utopia: How information ended the Soviet Union*. Chicago: I.R. Dee.

Soldatov, A., & Borogan, I. (2012, December 21). In Ex-Soviet States, Russian Spy Tech Still Watches You. Retrieved from http://www.wired.com/dangerroom/2012/12/russias-hand/all/

Soldatov, A., & Borogan, I. (2013). Russia's Surveillance State. *World Policy Journal, 30*(3), 23-30. doi: 10.1177/0740277513506378

Soldatov, A. (2014, February 6). FSB Makes Eavesdropping an Olympic Event. Retrieved from http://agentura.ru/english/projects/Project_ID/olympicevent/

Starr, F. (1990). New Communications Technologies & Civil Society. In L. R. Graham (Ed.), *Science and the Soviet social order* (pp. 19-50). Cambridge, MA: Harvard University Press.

Tracy, J. (2000, February 4). New KGB Takes Internet by SORM. Retrieved from http://www.motherjones.com/politics/2000/02/new-kgb-takes-internet-sorm

UNICEF, Beger, G., Hoveyda, P., & Sinha, A. (2011, October 11). *The RuNet Generation: An Exploratory Study of the Russian Digital Landscape* (Rep.). Retrieved http://www.unicef.org/ceecis/TheRuNet_Generation(1).pdf

Walker, M. (Ed.). (2003). *Science and ideology: A comparative history*. London: Routledge.

Walker, S. (2013, October 6). Russia to monitor 'all communications' at Winter Olympics in Sochi. Retrieved from http://www.theguardian.com/world/2013/oct/06/russia-monitor-communications-sochi-winter-olympics

Waller, J. M. (1994). *Secret empire: The KGB in Russia today*. Boulder, CO: Westview Press.

Zuckerman, F. S. (2003). *The Tsarist Secret Police abroad: Policing Europe in a modernising world*. Houndmills, Basingstoke, Hampshire: Palgrave Macmillan.