The Internet in Putin's Russia: Reinventing a Technology of Authoritarianism

Marcus Alexander*
Department of Politics and International Relations
University of Oxford

April 2003

Abstract

By focusing on Internet policy in Russia, this article addresses the potential and actual impact of the Internet on increasing freedom in an authoritarian regime. Traditionally, authoritarian governments have responded to the IT revolution by censoring sources of free and unbiased information (China, Singapore, Middle East), while democratic governments focused on public concerns such as protection of minors and hate speech (United States, European Union). The game theoretic model developed from the evidence of Russian Internet policy-making shows that governments have a third choice: to use Internet for direct and indirect propaganda. Not only does the paper refute the claim that the IT revolution can automatically lead to more freedom and better democracy in Russia, but it also shows the danger of an authoritarian government learning how to appropriate the befits of the Internet in order to increase its control over the public information space.

Presented at the Annual Conference of the Political Studies Association, University of Leicester, UK, April 15-17, 2003

^{*}Address: Brasenose College, Oxford OX1 4AJ; email: marcus.alexander@bnc.ox.ac.uk. I thank Nazli Choucri, Benoit Frydman, Matthew C. Harding, Monroe E. Price, Andrei Richter, Christian Sandvig, Roxanne Varzi, Stefaan Verhulst, and participants of the 2002-2003 Nuffield College Graduate Workshop in Political Science for their comments and suggestions. For funding, I am grateful to the Markle Foundation and the Fox Fellowship program at Yale University.

2

1 Introduction

The survival of Russia's hybrid post-communist regime, first under President Boris Yeltsin and then under President Vladimir Putin, poses difficult challenges for students of comparative democratization. One of these challenges is the question of how these regimes resist both consolidation of democracy and return to full-blown authoritarianism. The case of Russian Internet policy is of special interest as it brings to forth two interesting puzzles on this topic: (1) Can non-democratic governments such as Putin's Russia allow for more freedom in order to increase their political control? (2) Do non-democratic governments such as Putin's Russia learn? The evidence presented here will show that the answer to both questions is affirmative.

The question of Internet policy, and especially its role in promoting democracy, has occupied some attention and yielded interesting but contradictory observations. If the proliferation of the Internet in the developing world was to follow the proliferation in the developed world, it was logical to assume that the promise of the scholars of Internet in developed democracies (Arnold, 1992; Davis, 1999; Dertouzos, 1997: Rheingold, 1993; Selnow, 1998) would also apply to emerging democracies. At once, at leat in theory, the Internet held the potential to increase individuals' access to free information, the ability to communicate both one-to-one and one-to-many without interference from the government or other public/private agencies, and the opportunity to participate directly in public decision-making.

But three trends betrayed initial enthusiasm: (1) The gap between those with access to the Internet and those without, "the digital divide", looks likely to increase (Norris, 1999, 2001; Wresch, 1996; NTIA, 2000); (2) So far, access to the Internet depended on access to old technologies such as the telephone, and at least in the developed countries it was usually the rich and the politically-privileged that gained access to the Internet before the disenfranchised and the poor (Anderson et al., 1995; Bimber, 2000; Bucy, 2000; Clemente, 1998; Hoffman, Novak and Schlosser, 2002; Davis, 1999; DiMaggio et al., 2001; Norris, 1999; Wilhelm, 2000); (3) The pattern of Internet use started to reflect the pattern of traditional media consumption, and concerns arose regarding the true potential of the Internet as a truly multi-channel, one-to-one, instant-time democratic means of public and private communication (Margolis and Resnick, 2000).

This article challenges the assumption that proliferation of Internet technology in transitional countries such as Russia will lead to an increase in freedom of speech and further democratization. It does so by introducing the concept of the modern authoritarian government that can not only restrict and control the Internet but also use it actively to stifle political freedom. In this respect, the case of the Russian Federation is a first. It shows the danger of authoritarian governments learning how to appropriate the benefits of the IT revolution in order to increase their control over the public information space. The argument begins by outlining reasoning behind the assumption that the Internet would diminish political control of authoritarian governments, and therefore lead to both increased individual freedom and democratization. The next part presents the story of Russian Internet policy making in four parts: proliferation of the Internet, early attempts of the government to establish control, rise of government-controlled online media, and establishment of an aggressive government policy to win Internet users through commercial competition and regulation. The next part uses the story of Russia's Internet policy-making to introduce a game theoretic model of government control over the Internet news media sector, and the effects of these government actions on Internet content providers and individual users. The final part brings the lessons of the theoretical model back into the discussion of Russian democratization, and offers some concluding remarks on Russian President Putin's policy of consolidating his country's nascent authoritarian regime.

2 Internet and Democratization

Freedoms to access information and express oneself are generally accepted as basic requirements for a democracy. Minimalist conceptions of democracy (Schumpeter, 1942; Huntington, 1991; Przeworski, 1991, 1999) implicitly require some degree of freedom of information in order for contested elections, which these theories see as a minimal requirement for democracy, to be fair and effective. In practice, this usually means that parties should have access to media to present their candidacies and voters should have access to these presentations. More taxing definitions of democracy rely more heavily on freedom of speech as a basic democratic requirement. Most importantly, these include Dahl's theory of polyarchy that requires responsiveness of the government to voters' preferences during interelection period (Dahl, 1956, 1971), participatory or deliberative views of democracy (Mansbridge, 1980; Fishkin, 1991; Gutmann and Thompson, 1996) that require citizen involvement beyond a simple vote in an election, and explanations of democracy that demand presence of some form of democratic beliefs and culture (Putnam, 1993, 2000). In practice, this means that individuals in a society, either individually or through media independent of the government, should: (1) be able to express their opinion of government's performance (watchdog function), (2) contribute diverse views that form a pluralistic media environment (participatory function), and somehow internalize and help sustain tolerance by respecting others' right to free speech (cultural function).

Habermas's understanding of democracy most explicitly relies on freedom of the information media by stressing the need for an unconstrained "public space." (Habermas, 1989, 1996). In this public space, individuals can rationally deliberate free from government interference, and the persuasiveness of different voices is judged on the merits of their arguments. One of the most immediate effects of democratic revolutions in Eastern and Central Europe was reconstitution of the information space. Studies trying to develop a concept of "liberal" or "consolidated"

¹In Poland and in Russia for example, multiparty elections occurred only after slow but steady

democracy have recognized explicitly freedom of media as both an important measurement of the state of a democracy and a means of democratic consolidation. (Palma, 1990; Diamond, Linz and Lipset, 1990; Diamond, 1999)² Media law and policy scholars have focused on developing theory and practice of regulating media in transitional societies in order to foster pluralism, human rights, and general democratization (Rozumilowicz, 2002; Foster, 1996; Price, 1995; Price and Krug, 2000). In sum, democratic theory suggests that liberalization of the information space – characterized by decreasing government control over the media, multiplication of voices, and increase of citizens' access to information – should promote democratization.

By the unique virtue of its architecture and its speed of proliferation, the Internet should hold a potential to liberalize the information space and subsequently lead to democratization, especially in states where governments tightly control traditional media such as the newspapers, radio, and television. While in developed democracies, the Internet is seen as a potential means to develop a more informed, pluralistic, and participatory electorate; the potential contribution of the Internet in authoritarian and democratizing states is more basic. The focus in this paper is on the potential of the Internet to liberalize the information space, weaken the political control of an authoritarian government, and increase both individual freedom in the short run and the potential for democratization in the long run.

The definitions of Russia's regime type, the term Internet, and the process of Internet policy-making are necessary before presenting the Russian case. The form of government undoubtedly affects the process of policymaking, and media and Internet policy is no exception. Although all incumbent governments seek to implement policies that help them stay in power, there are fewer limits on authoritarian governments' willingness to monopolize the information space (based on institutional restraints, leaders' interests and motivations) than this is the case in democracies. Russia here is defined as a non-democracy; following most Russian experts Putin's Russia is considered some form of soft, quasi, semi, electoral authoritarianism.

The information space is defined as the set of public media that includes print, television, radio and the Internet. The Internet refers to the World Wide Web, e-mail, interactive computer games, and means of one-to-one and one-to-many communication (voice or chat room) using a computer. The structure of the In-

deterioration of government's control over the media. With most revolutions, and most prominently in Romania and Serbia, authoritarian forms of control over the print and broadcast media (through censorship and propaganda) disappeared literally overnight and new voices entered the information space.

²Diamond, Linz and Lipset (1990) explicitly defined freedom of the press as one of the requirements of a democracy.

³In developed Western democracies, the Internet's potential for democratization has been studied under the general rubric of e-democracy – a means by which access to new information communication technologies (not only the World Wide Web but also e-mail, message boards, chat forums, and other) can contribute to improved communication between the government and the citizen and to forms of direct participation of citizens in governmental policy making.

ternet is such that users can act simultaneously as content providers. This is part of the important democratic architecture of the medium. Nevertheless, in this study, we will pay special attention to the Internet's ability to replace and supplement traditional forms of media (print, television, radio) through online news providers. Here, Internet Content Providers (ICP) are artificially distinguished from the individual users for the purpose of understanding the impact of the Internet in the context of traditional media politics. ICPs are defined as entities that provide content on the Internet (for our purposes news and political content are of special interest) and target individual users throughout the general public. Most prominent examples in the United States are MSN, AOL, or Yahoo! Ability to access the diverse and truthful information is considered freedom of access that contributes to freedom in general. The government's attempts to affect behavior of either ICPs or users are considered Internet policy.⁴

In this study, the situation before is one of little or no access and high degree of government control over information. The intermediate situation is one of higher but still low access where government control over the general information space is challenged. The final, after, situation is one in which the government restores control over the information space despite the further rise in Internet access. This story is documented bellow.

3 The Making of Russian Internet Policy

In 2002, there were 10 percent of Russians online; the government planned to invest US\$2.6 billion in IT industry development to drive this number further; and the Russian Duma passed the Law On Electronic Signatures, which was the first law exclusively targeting Internet use. The original proliferation of the Internet at first encountered an unprepared government that dealt with the new medium not much different from its Soviet tradition in national media and technology regulation. The government's first-round response also included attempts at direct censorship of the Internet, but the general assumption about the inherent democratic nature of the Internet architecture proved true: Internet use in Russia escaped tight regulation as the government was initially unprepared for the challenge. With President Putin's coming to power, the picture changed rapidly and dramatically. This section presents the initial challenge of the Internet's proliferation in Russia and proceeds to chart the evolution of Russian government's policy of Internet regulation.

⁴This is a broader definition than simply stating that government Internet policy is a method by which the government affects availability of access within a country. This distinction is crucial. New research on comparative Internet development has focused its efforts on defining the variables that affect a country's transition from the situation *before* (no or little access to the Internet) to the situation *after* (wide access and use of Internet for various economic, political and social activities).

3.1 The Challenge: Proliferation of Internet use in Russia

VICOM date from the beginning of 2002 shows that not only 10 percent of Russians are online but also that nine percent of Russians use computers several times a week, while this number is 26 percent in Moscow. Additional four percent Russians use computer once a week and an additional one percent use computers less than once a week.⁵ Both Internet use and computer ownership numbers are remarkably low by European or U.S. standards, as the telecommunication infrastructure in Russia remains underdeveloped, with poor quality analog telephone lines and long waiting times for new phone numbers, and Internet provider services remain unrealistically expensive in comparison to mean household income, even for the basic subscription. ⁶Yet with 200 telephone lines per 1,000 people in 1999 and 3.5 Internet hosts per 1,000 people, Russia is far ahead of other large developing countries such as India and China in both access to telephone lines (ground and cellular) and in the number of Internet hosts (see figure 1).

Relatively high number of Internet hosts compared to other developing countries is also characterized by high government stake in the Internet service providers (ISPs) market. In March 2000, the largest ISP in Russia was Relcom, followed by Demos and Russia On-line. Relcom was entirely government-owned and enjoyed a near-monopoly in the market, with its Moscow hub subscribing 10,000 users and approximately 150 other regional hubs with an average of 500-1,000 subscribers. (Brown and Wright, 1997) During the past two years, the competition between ISPs has somewhat increased, but the government maintains large stake in the ISP market oligopoly. Analyzing the problem of the digital divide in Central and Eastern Europe, a 2000 Global Internet Liberty Campaign report recommended putting pressure on governments to extend the principle of universal service obligation to the Internet, and encouraged consumers to exercise their role through the market and political action to increase demand for more affordable access. ⁷ In the case of Russia, the move towards increasing access to the Internet under the present conditions of high-level of government control may not be as desirable as the report suggests in the general context. If our recommendation is to encourage the government's interference in the Internet sector (even through subsidies of access for the poor) we must first examine the government's past motivation and practice or Internet regulation. ⁸

⁵As for computer use, 84 percent of Russians never use computers and this number is 69 percent in Moscow. In January 2002, computer ownership was at 6 percent of national households and 23 percent of Muscovite households.

⁶Evaluating Russia's potential to deal with the emerging digital divide at home, a 2000 Global Internet Liberty Campaign report concluded that "despite the country's best efforts, the telecommunications infrastructure in Russia is simply unsuitable for modern computer communication needs and is not expected to reach Western standards for many years to come." (GILC, 2000, 47)

⁷On a positive side, the report indicated the rise of mobile telecoms and increasing competition between ISPs as a positive development, potentially leading to these changes. (GILC, 2000, 3-4)

⁸The ultimate challenge will be to delineate the government's role in financing development of infrastructure necessary for development of the Internet on one hand, and the government's tendency to use its privileged position in order to control Internet content and monitor personal communications on the other hand.

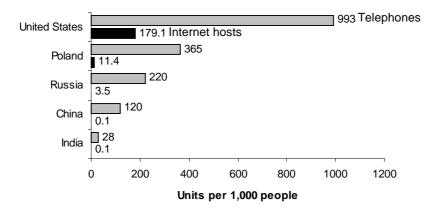


Figure 1: Telephones (mainline and cellular) in 1999 and Internet hosts in 2000 per 1,000 people in selected countries. Source: UNDP(2001).

The Internet, together with the telecommunication industry in Russia, rebounded well after the 1998 recession that was characterized by the crash of the rubble, meltdown of the banking system and mass exodus of foreign investors from the country. In October 1997, the number of Internet users in Russia was approximately 600,000, which was 0.4 percent of Russia's 150 million-strong population. By the time of the crisis, in July of 1998, the number had reached 1 million or 0.6 percent, and in March of 1999, the number climbed to 1.3 million. (ROCIT, 1999) In 2000, Russia had approximately 180,000 Internet hosts. (GILC, 2000)⁹ According to a forecast by IDC, formerly the International Data Corporation, there will be a total of 9.4 million Internet users in Russia by 2004. The Interfax reported that there were 45,000 registered web servers in Russia in 2000 – more than three times that in 1998 – and that e-commerce transactions totaled between US\$500 million and US\$600 million. (Shanetskaya, 2001)(See figure 2 for comparison of Internet use growth in Russia and worldwide.)

An ethnographic snapshot of Russian Internet makes the empirical picture of Internet proliferation more accurate. A tour of Moscow's Internet cafés gives one picture of the current Russian Internet use, at least in public spaces. In the affluent neighborhood of Vorobyovi Gori, a local computer hardware store in the basement of an apartment building was recently refurbished into an "Internet and Game Café". The customers are mainly boys aged 7-12, they play interactive video games, and one hour costs US\$1.00. Not far away from the neighborhood café is the grandiose campus of the Moscow State University (Moskovskii Gosudarstvenii Universitet imeni M.V. Lomonosova). In its Humanitarian Complex II—which houses the faculties of History, Economics, Politics, Law, Philosophy, Religious Studies, and Public Policy—you can also find an Internet café. Main

⁹Original source: RIPE Regional Hostcount

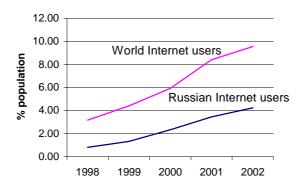


Figure 2: Worldwide and Russian Internet users as percentage of total population. Sources: Nua Ltd. and ROCIT.

users are students, they surf for news and term papers, and US\$1.00 will buy you 30 minutes. There are finally the super-Internet cafés like TimeOnline, located on the lowest level of the shopping mall Okhotny Ryad, "one of the world's miracles" if you are to believe the recorded announcement that welcomes tourists and the Moscow elite (among all the others) into the underground complex on Manyezhna Ploschad adjacent to the Kremlin. The NightOnline deal gives you about 8 hours, starting midnight, for just under US\$3.20. The cafe is packed with teens and young adults (mostly under 30), and they use the cafe's close to 300 flat-screened computers to chat, surf the web for music, and on occasion use the Internet to prepare term papers or search for jobs.

The average user is relatively young, 20-29 years of age, with two third of Runet users being under the age of 34. 60 percent of the users are male and 50 percent have some higher education. In interviews, this 'average user' said she is a "hard worker and enjoys work." Most interestingly, users by-and-large tend to identify themselves as liberal but in support of President Putin. They also watch TV often and tend to live in cities. (Mulvey, 2001)

These observations present a challenge to the general assumption that Internet will automatically lead to an increase in personal freedoms—be it by increasing access to information, improving the quality of information, or enabling freedom of expression. It may be simply false to assume that intelligent, educated, and young persons in a country such as Russia will flock to the Internet in order to find the truth about their government, and then use Internet to spread this truth and mobilize opposition. But even before this question is raised, it is important to investigate how has the Russian government responded to proliferation of the Internet.

Rank	Media	Visitors
1	Gazeta.ru	670,148
2	Lenta.ru	646,196
3	Dni.ru (daily)	630.973
4	Ntv.ru	527,914
5	Izvestia	429.271
6	Rol.ru News	404,110
7	Strana.ru	398,378
8	Komsomolska Pravda	378,020
9	3D News	374,728
10	Grani.ru (daily)	339,944
12	Nezavisimaya Gazeta	302,301
18	Vest.ru	141,767
28	Polit.ru	99,844
38	RTR	$63,\!192$

Table 1: Most-visited Russian Online Media (April 2002). The number of visitors is calculated for the period of 30 days, from March 24 to April 23, 2002. These dates are arbitrary. Source: dir.spylog.ru [April 23, 2002]

3.2 Government's reactionary response

The first period of Russian Internet policy-making, which lasted for the major part of the 1990s, was first characterized by legislation closely resembling Soviet tendencies of state bureaucratic oversight, at cost both to free growth of the industry and practical efficacy of executive policy-making. Much as is the case in the Western developed states, the Internet in Russia is governed by laws concerned with commerce regulation and laws concerned with the regulation of media. From the beginning of the 1990s, the Russian government showed concern for two other areas regarding Internet use: security of new technology (grounded in the Cold War-motivated rivalry in the industrial-military complex) and national identity (protection of any communication medium from overwhelming foreign influence). In 1990s, these four legal concerns have resulted in a complicated set of regulations that apply only partially to the Internet, a relatively new phenomenon. The main body of these older laws includes: the Law on Databases, the Roskominform Statute, the Law on Communications, the Law on Information, and the Law on Information Exchange. 10. The contribution of these laws, as well some of the most important subsequent documents is listed in Table 1.

The five early laws—the Roskominform Statute and the laws on Databases, on Communications, on Information, and on Information Exchange — were grounded not so much in a reactionary mood as they were attempts of the government to deal with the new challenge of the IT revolution by using old mechanisms of bureaucratic oversight and control. As the result, the laws set up a precedent of government's justification for active control of the Internet by the process of regis-

¹⁰These laws are surveyed in Ellis (1999)

tration, setting up of government bodies to monitor and guide development of the industry, and delineation and qualification of rights (even Constitutional) when applied to the Internet. In addition to these laws, it was the 1992 Law on Mass Media that held perhaps more potential than any other law to enable government to gain control over Internet content. But issues regarding this law arose only after the rise of online media during the Putin's rise to power.

What opens possibility for the Russian government to go beyond regulation through censorship is that these laws demonstrate development of government interest in "infomratization" policy-making. In particular, Roskominform is the kind of hybrid executive-legislative body that is close enough to the office of the President, and therefore can have access to the resources and cabinet power brokers, to be able to implement far-reaching policy. In other words, these laws demonstrate that the government was moving – however slowly and perhaps in the wrong direction – towards developing policy-making mechanisms in the area of Internet policy.

In addition to these legislative moves, the government engaged in a few bluntly political attempts to increase control over the Internet. In particular, the case of SORM, which stands for "System for Operational-Investigative Activities," has been cited often as the worst kind of government interference in the IT age. As a part of it, the FSB (the Federal Security Service) forced Internet service providers to install hardware that allowed FSB to monitor Internet usage and e-mail messages of the provider's customers. (Warren, 1998) Putting the issue in quite stark perspective, Anatoly Levenchuk said: "Introducing Sorm is equivalent to having to surrender copies of the keys to your flat or car or garage to the nearest police station so that the police can visit your home or break into your car or garage whenever they like, supposedly to catch potential criminals." (Warren, 1998).

Upon its introduction in 1999, SORM2 – the revised and updated version of SORM - required all ISPs to route their incoming and outgoing data through FSB computers. Those providers who did not cooperate were forced out off line by FSB, which also at the time controlled the government's ISP licensing procedure. For example, Bayard-Slavia of Volgograd was disconnected and its capital assets frozen after the ISP threatened to sue the FSB for demanding its clients' passwords without a warrant. The FSB cited "licensing errors," as grounds for its hostile action. Another interesting effect of the Sorm2 is that the FSB's demand for ISPs to pay themselves for the spying hardware has threatened to put many small sub-providers out of business (who represented 90 percent of Russia's 360 ISPs in 1999), giving a greater market share to a few larger ISPs. Since 1999 and the vocal public criticism of FSB actions, SORM2 has been revised and now requires the FSB to obtain a warrant prior to looking at a user's electronic traffic. Still, it is doubtful that the FSB actually puts great priority on following this rule. Instead it is the high rise of Internet data traffic, eventually overwhelming anyone's ability to monitor it in detail, that is likely to frustrate the FSB efforts. (Hammersley, 1999)

Year	Document	Contribution
1992	Database Law	some legal protection for software designers
		some privacy protection
		sets up registration mechanism
1994	Roskominform Statute	sets up a 12-person "informatization" policy body
		Roskominform to set national priorities
		Roskominform to draft legislation
		Roskominform to cooperate with international bodies
1995	Information Law	granted citizens access to "state information resources"
		economic and non-government actors identified
1996	Communications Law	emphasizes the Constitutional right to privacy
		interference needs Court sanction
1996	Information Exchange Law	empowers government for specific areas of the Internet:
		information architecture, flow and access
2000	Information Security Doctrine	defines Internet policy as national security concern
		gives the executive branch more power
		limits individual rights in cases of security concerns
2001	E-Russia Plan	an investment plan to boost Internet development

Table 2: Important Legal and Policy Documents Dealing with Internet Policy in Russia.

3.3 Emergence of online news media

The main challenge to the government through the Internet medium came with the rise of online media and political websites. Table 2 lists most visited news web sties in Russia, and figure 3 illustrates the relative reputation that different online news providers enjoy in print media. One of the earliest controversies happened during the 1999 State Duma elections, when Gleb Pavlovsky's Foundation for Effective Policy (FEP) web site www.election99.com published the results of exit polls. The Central Election Committee, under pressure from the Fatherland-All Russia block, attacked Pavlovsky and the FEP under allegation that the publication of exit polls violated the Law on Elections. ¹¹ The ensuing public dispute brought forward the difficulty of classifying online media as mass media under Russian law. If classified under the heading of mass media, political and news websites would have to come under tighter control of the Kremlin. (MMLPC, 2000)

Pavlovsky's brush with the Internet during the Duma elections was only a sign of things to come. As Boris Yeltsin's time in office neared its end, Pavlovsky tightened his ties with Kremlin though his FEP. Once the time for Presidential election came, Pavlovsky led an elaborate and aggressive smear campaign against former Prime Minister Yevgeny Primakov and Moscow Mayor Yuri Luzhkov. As a part of this campaign, Pavlovsky used a number of Internet news sites (strana.ru, vesti.ru, smi.ru, russ.ru, lenta.ru (30 percent stake)), and coordinated political

 $^{^{11}}$ "On the Fundamental Guarantees of Election Rights and the Right of Citizens of the Russian Federation to Participate in Referendums"

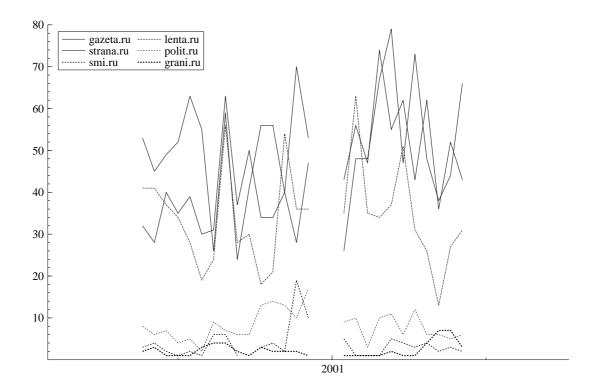


Figure 3: Number of weekly citations of Russian online news providers in leading national newspapers/magazines. The significance of this graph is that the all of the most popular online new providers (the top lines) are government-supported and funded. Of the bottom three, grani.ru has been the most independent, and also finds itself at the bottom of the graph.

ridicule sites directly smearing Primakov and Luzhkov (primakov.ru, mayor.ru, ovg.ru, and lujkov.ru). (Mulvey, 2001). Subtlety and complexity are the characteristics of Pavlovsky's strategy that made his online assault as effective as it was. Most of the new online news providers exercised degrees of independence far greater than what was possible in television or even in print. Strana.ru was most explicitly in support of Putin and was funded by mainly anonymous private sources. In 2001, the website reported incriminating statements made by Russians abroad who criticized the government, a chilling reminder to the Soviet-style government propaganda. On the other hand, some online news websites like vesti.ru exercised more moderate judgement in what news to report and was at the time linked to the independent TV station NTV. (Mulvey, 2001) Reportedly, Pavlovsky called on Kremlin to create a special center to take charge of "information security," and BBC reported abut rumors that a "rapid reaction unit" had been set up to track journalists reporting off-message. (Mulvey, 2001)

Pavlovsky tapped into a truly rich source of potential for improving Kremlin's control over public opinion. One recent study of Internet in Russia found that sites of online only newspapers had more visitors that any other source of political and current information on the Internet in Russia. Online versions of offline news providers followed, and the least popular sources of information were websites of political parties and individuals' campaign websites. (Smetko and Krasnoboka, Forthcoming) And the same study of the Ukraine's election crisis in December 2000 and January 2001 lead Smetko and Krasnoboka (Forthcoming) to conclude that "in a political crisis freedom of expression and up to date information become the most important qualities of online information." With this need for up-to-date information during political crises, Kremlin gains incentive to interfere with the Internet at times such as elections, and devise approaches to using the new technology most effectively for its purpose of controlling public opinion.

3.4 Government's proactive response

Since President Putin's election, both the Duma and the Kremlin have become active in drafting and discussions of Internet-related legislation, most importantly including legislation on e-commerce and Internet mass media. In 2001, the Duma considered laws intended to increase protection of intellectual property and give electronic signatures legal weight. In 2002, it passed the Law on Electronic Signatures. On the media side, it considered requiring online newspapers to register officially as "mass media." But by the end of the 2001, the most immediate and direct Internet regulatory mechanism in place was the Ministry of Justice's requirement of Internet service providers to pay for the hardware for security services to monitor their clients' e-mails. (Mulvey, 2001)

The Russian government, officially, sees Internet regulation as a tool for enabling

 $^{^{12}}$ The debate on whether the online newspapers are to be considered "mass media" is addressed in the following section below."

¹³This requirement is a modified version of the SORM project discussed above.

growth of e-commerce, and preparing Russia for its entry in the World Trade Organization. Yury Travkin, a consultant to the Duma's commission on information policy, said that the Russian Internet regulation should serve to ban commercial spam e-mail, protect intellectual property, prevent copyright infringement, secure online payments, and legitimize digital signatures. (Shanetskaya, 2001) It is clear that some of the goals of the Duma are directly related to encouraging economic growth through strengthening of the country's IT sector. The numbers used by the government are truly encouraging. According to a forecast by the International Data Corporation, there will be a total of 9.4 million Internet users in Russia by 2004. The Interfax reported that there were 45,000 registered web servers in Russia in 2000-more than three times that in 1998-and that e-commerce transactions totaled between US\$500 million and US\$600 million. (Shanetskaya, 2001)

But one needs to question proposals such as that reported by the Segodnya newspaper, that in 2001 the Duma's economic policy committee had recommended that only officially registered self-employed businesspeople be able to shop in Internet stores. In addition, Timofei Kotonev of the Lovells law firm warned that the new signature law may require companies wanting to use digital signatures for contracts to register with the Federal Communications and Information Agency. (Shanetskaya, 2001) The E-Signature Law was passed by the end of 2002. At the end of 2001, the Duma was also considering an amendment to the law on trademarks, which would allow companies to strip internet owners of their internet domain names if these domains resembled the companies' trademarks. And additionally, anyone applying for a .ru domain name would have to go though the Rospatent, Russian trademark and patent agency. Nikolai Bogdanov, deputy general director of Rospatent, told The Moscow Times: "Usually, the rights of trademark owners to have an individually named product are broken, not the rights of domain holders. No opposite process exists yet." But Anton Nosik, the vice president of the Rumbler Internet company said that "Such amendments are useful for uneconomic purposes, such as the confiscation of property." (Boreiko, 2001)

While these discussions were taking place in the Duma, the executive branch pushed for a new and more comprehensive Internet initiative called the Electronic Russia Plan (E-Russia). At the July 5, 2001 meeting, the cabinet appointed the Ministry of Communications as a coordinator of the plan, while official E-Russia documents still listed the Ministry of Economic Development and Trade as responsible for developing and commissioning the program. The Ministry of Economic Development and Trade was also the one behind the drafting of the document, and the primary coordinator of E-Russia within this ministry, Tseren Tserenov, said that "the new economy doesn't just mean getting the internet to people, but a change in lifestyle and the way government works." (Wolfe, 2001) In short, this statement of E-Russia goals is indicative of the aggressive and far reaching ambitions of the Russian government to appropriate some of the benefits of the Internet for its purposes (in this case the purpose being to stimulate economic growth.)

¹⁴Detailed information about the plan, in Russian, is available from the program's website at www.e-russia.ru.

The cost of the program was astronomic by Russian standards, especially for a domestic program dedicated to the IT infrastructure: \$US2.6 billion. It was partially because of its astronomic size and its complicated intra-governmental funding arrangements, that the budget for E-Russia was slashed by the end of 2002. The plan for the funding was that 51 percent of the budget should come from the federal budget, 30 percent from regional budgets, and 19 percent from non-budgetary funds (such as corporate sponsorship). Half of the E-Russia project budget was to come from the federal budget and a third from regional administrators. The bureaucratic machine was just not up to the task of mobilizing the kind of management effort needed to gather the allocated money and spend it as it was intended. The strategic vision of Kremlin suffered, and the limits of government learning and proactive policy came to the fore. In the fall of 2001, the budget submitted to the State Duma contained a starting amount of \$11.9 million. But the amount allocated in 2002 was 10 times less than originally proposed. (Boreiko and Nefedov, 2001) (Seregina, 2001)

The second document that emerged as a defining guideline of a more aggressive approach to Russian Internet policy-making was the Information Security Doctrine. Signed into law on September 9, 2000 by President Putin. (The doctrine grounded media policy in general, and Internet policy in particular, in the core "national security" concerns of the state. This shift was significant for three reasons: (1) endowing the government with the right not only to interfere but also to engineer Internet development; (2) defining the limits to rights of individuals and private groups to use the Internet; and (3) pushing the government into an aggressive policy to expand its control over the Internet in Russia.

First, the endowment of the government with rights to control the information space is spelled explicitly by the Doctrine:

The interests of the state in the information area consist in creating conditions for the harmonious development of the of the Russian information infrastructure, for the excise of constitutional human and civil rights and freedoms in the field of obtaining information and using it for the purposes of ensuing the stability of the constitutional order, sovereignty and territorial integrity of Russia, political, economic and social stability, the unconditional ensuring of legality, law and order, and the development of equal and mutually beneficial international cooperation (Information Security Doctrine, 2000).

The means to fulfilling not only this state priority but also the rights of individuals and of the society at large, the Doctrine lays out a strategy of state leadership in development of information architecture, promotion of access, and formation of strong state information agents that ensure that the government activities are presented accurately. This is the third contribution of the Doctrine named above; the Russian government had defined the state as the dominant actor in not only

 $^{^{15} {\}rm In}$ Russian: "Doktrina Informacionnoy bezopasnosti Rossiyskoi Federacii"

developing but also guarding the proper information infrastructure.

Of course, the role of the state here is explained by the national interest, which importantly includes individual rights and liberties (the second contribution of the Doctrine named above) as much at involves stability of the Constitutional and other political order. Arguably, the main addition to individual rights, at least from the government's perspective, is that the Doctrine identifies spiritual revival and language rights as important individual rights. Contrary to a Western, democratic, understanding of these rights, the Russian government sees them as tied to constituting and defending Russian national identity (both from foreign and domestic threats) rather than promoting plurality or minority rights.

Finally, one of the most important contributions of the Information Security Doctrine is that these politically-charged strategies of Internet development are tied in with the kind of e-commerce and copyright advancements that will help Russia integrate into the international community when it comes both to IT issues and to general trade issues such as World Trade Organization membership. Two important examples of recent laws that strengthen this move are the law establishing validity of e-commerce, which was in fact approved in January of 2002, ¹⁶ and the working version of a laws that extend Russian document laws to the Internet and further protect online authors' rights. ¹⁷

4 Modelling Government Internet Control

4.1 A Basic Model of Government Information Control

In this section, the goal is to model the strategic interaction between an independent Internet content provider (ICP) and the government who is interested in maximizing its popularity. Although this is only a stylized example it captures the basic strategic relationship of the situation. It is important, nevertheless, to note that we purposefully do not model the consumer here.

The players of the game are: a non-government owned ICP, the government (including a government-owned ICP if that is the case), and a representative agent (the individual). The model assumes that support for the government is defined as an agent's belief in the "goodness" of the government. The belief of the agent in the "goodness" of the government is measured by a continuous real-valued variable with support on [0, 1]. The model also assumes that the government's true degree of "goodness" is given by t, defined on [0, 1], with government being perfect when t = 1. The value of t can be correctly observed by an independent ICP but cannot be observed by the representative agent. The agent has a prior belief regarding the "goodness" of the government defined by $t_0 \in [0, 1]$. The prior belief t_0 is based

 $[\]overline{\ }^{16}$ In Russian, "Ob elektronskoy cifrovoy podpisi," adopted on January 10, 2002.

¹⁷For example, see the working version of the law in Russian, "O sdelkah, soverhaemih pri pomoschi elektronih sredstv," available at www.duma.ru.

on the agent's history and previous experience in interacting with the government.

The play of the game is as follows. The independent ICP moves first and reports a value t_1 for the government's degree of "goodness" based on its observation of the true value t and its expectation of the government's response to its report. Notice that t_1 does not necessarily reveal truthfully the value of t to the agent. The government moves second, after having observed the reported value t_1 by the ICP. In this stylized example, the government has three courses of action: noninterference, censorship, or an introduction of a government-sponsored competing ICP. If the government chooses not to interfere, the agent observes the reported value t_1 and uses it to update its prior belief t_0 regarding the government's degree of "goodness." If the government chooses to censor, it effectively shuts down the ICP and eliminates the signal reported by the ICP to the agent. Instead, it may provide its own source of information about its "goodness." In the long run this is equal to preventing the ICP from independent reporting in the first place. However, this action presents a non-negative risk for the government as the agent may find out about the government's action and hence conclude that the government is "bad", i.e t=0. The third action open to the government is the introduction of a competing government-supported or government-owned ICP, over which it can exert control with regard to information reported. The information concerning the government's degree of "goodness" is determined by $t_2 \in [0, 1]$.

At every stage of the game, the individual uses the newly reported information to update its belief concerning the government's degree of "goodness," starting with the prior belief t_0 . Although there are many ways in which this dynamic belief process could be modelled, we shall assume for simplicity that the agent's belief as the result of the acquisition a new piece of information is given by a weighted average between her belief regarding the government's degree of "goodness" before and after receipt of the information at the current stage of the game. For example, if the agent has a prior belief t_0 at the start of the game, and receives a signal t_1 from the ICP at the first stage of the game, she will update her intermediate belief such that $t_I = \alpha t_0 + (1 - \alpha)t_1$.

To complete the description of the game, the payoffs accruing to the players must be specified given their motivations. The government aims to maximize the difference between the agent's belief in the government's degree of "goodness" at the end of the game, t_f , and its prior belief, t_0 . The ICP aims to minimize the squared difference between agent's final belief, t_f , and the true value, t. The ICP's aim is thus to facilitate the agent's beliefs converging on the truth.

If the government chooses not to interfere, the agent's final belief t_f equals her intermediate belief t_I . The ICP's payoff is given by $1-(t_f-t)^2$. The government's payoff is given by t_f-t_0 .

If the government decides to shut down the ICP (censor), then the ICP's payoff is zero. The government receives a payoff $t_f - t_0$, where $t_f = (1 - p)[\beta t_0 + (1 - \beta)t_p]$.

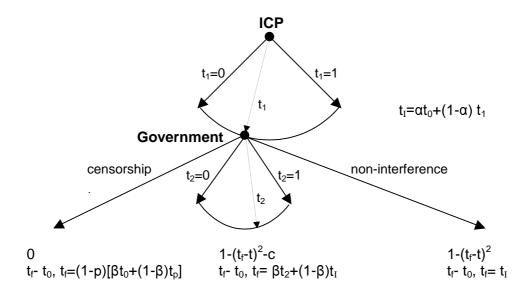


Figure 4: Government response to the provision of independent information by a non-government Internet content provider (ICP).

The degree of direct government propaganda is given by $t_p \leq 1$. This is because the government's ability to distribute propaganda and convince the agent of its honesty may be imperfect. The agent may realize that information provided is pure government propaganda, or she may decide to penalize the government for its shut down of the ICP, and update her belief to $t_f = 0$ with probability p.

If the government decides to introduce a competing ICP of its own (government-supported or government-owned), this government ICP will choose an optimal signal t_2 so as to maximize the government's payoff $t_f - t_0$. For the sake of simplicity the government-supported ICP is assumed to fully associate with government's aims. The independent ICP's payoff is given by $1 - (t_f - t)^2 - c$, where c is the payoff loss associated with competition in the market for online information provision. The agent's final belief $t_f = \beta t_2 + (1 - \beta)t_I$, a weighted average between the information supplied by the government-supported ICP and her updated belief following the receipt of independent ICP's information.

The game is illustrated in figure 4.

4.2 Solving the Model

In this section the model will be solved using the concept of subgame perfect equilibrium (SPE) to reveal the conditions under which the government decides to introduce its own competing ICP rather than shut down the existing independent ICP or not interfere at all. A SPE is an extension of the concept of Nash Equilibrium (where for each player, each player's strategy is a best response to the

expected strategies of the other players) to a multi-stage dynamic game consisting of several subgames. In a SPE the players are required not only to play a Nash Equilibrium in the entire game, but must also induce a Nash Equilibrium in every subgame. ¹⁸

A backwards induction argument can be used to discover the conditions under which the government introduces its own competing ICP for any reported value of t_1 by the independent ICP. Let Π_1 be the government's payoff when it shuts down the ICP, Pi_2 be the government's payoff when it chooses to introduce a competing government-supported ICP, and Pi_3 the government's payoff when it chooses not to interfere. The government chooses to introduce a competing ICP if

(A)
$$\Pi_2 \geq \Pi_1$$

(B)
$$\Pi_2 \geq \Pi_3$$

Substituting from above gives:

(A)
$$\beta t_2 + [(1-\beta)\alpha - 1]t_0 + (1-\beta)(1-\alpha)t_1 \ge (1-p)\beta t_0 + (1-p)(1-\beta)t_p$$

(B) $\beta t_2 + [(1-\beta)\alpha - 1]t_0 + (1-\beta)(1-\alpha)t_1 \ge (1-\alpha)(t_1-t_0)$

If the government chooses to introduce its own ICP, the linearity of its payoff structure dictates a value of $t_2 = 1$, that is the government-supported ICP will always fully support the government. At the first stage of the game, the independent ICP will have a payoff $\Pi_{ICP} = 1 - (t_f - t)^2 - c$, given that the government will introduce its own competing ICP at the next stage of the game. The independent ICP chooses a value of t_1 such that it maximizes Π_{ICP} . The first order condition for profit maximization is given by

$$\frac{\partial \Pi_{ICP}}{\partial t_1} = -2 \frac{\partial \Pi_{t_f}}{\partial t_1} (t_f - t) \tag{1}$$

$$= -2(1-\beta)(1-\alpha)\{\beta - t + (1-\beta)[\alpha t_0 + (1-\alpha)t_1]\}$$
 (2)

$$=0. (3)$$

The optimal value of t_1 can be solved as

$$t_1 = \frac{t - \beta - (1 - \beta)\alpha t_0}{(1 - \beta)(1 - \alpha)}. (4)$$

Note that t_1 does not necessarily equal t but rather is a function of t (the true "goodness" of the government), t_0 (the individuals prior belief concerning t), and the structural parameters α and β . The independent ICP's payoff is maximized when the individual's final belief is as close to the true value t. The ICP may well under-represent the government's degree of "goodness" in order to encourage the agent's beliefs to converge to the true state of the world. In general the formula above reveals that it is in the interest of the independent ICP to exaggerate the degree of "badness" which the government exhibits.

¹⁸Subgame perfect equilibrium (SPE) was defined by Selten in 1965. (Gibbons, 1992, 95)

Using the obtained optimal value of t_1 that reflects the revelation made by the independent ICP concerning the degree of "goodness" of the government, further progress can be made in analyzing the conditions required for the equilibrium where the government introduces it's own competing ICP in the market. Condition (B) can be reduced to $t - \alpha t_0 \ge (1 - \alpha t_1)$, which after a further substitution can be shown to hold as long as $t \le 1$. Thus, as long as the government is less than perfect it always has an incentive to interfere, whether by direct censorship or the introduction of a government dependent ICP.

Notice however that this relies on the assumption that the government does not face any direct costs of interference. If however these costs do exist it is likely that the government will not want to interfere if it is already placed at the upper end of the distribution with regard the true degree of "goodness" which it exibits. Thus, the higher the potential costs of interference are likely to be, the less likely it is that a "good" government will interfere with the free provision of information.

Similarly the first necessary condition (A) can be simplified to give $t - t_0 \ge (1 - p)\beta t_o + (1 - p)(1 - \beta)t_p$, which can be easily shown to equal

$$t_p \le \frac{t - [1 - (1 - p)\beta]t_0}{(1 - p)(1 - \beta)}. (5)$$

The interpretation is immediate. The government chooses to introduce a government-supported ICP rather than shut down the independent ICP and engage in direct propaganda, if it expects the degree of responsiveness of the individuals to direct propaganda to be relatively low. The threshold level is given by a function of the structural parameters of the model, such as the probability of the agent finding out the "true" nature of the government following a shut-down of the independent ICP, the degree to which the agent is willing to update her beliefs in favour of the government following a government sponsored broadcast and the relative difference between the government's "true" degree of goodness and the agent's prior belief regarding it.

This completes the equilibrium analysis and interpretation of this game. The question of when censorship might be a dominant strategy irrespective of what the reported value of t_1 by an independent ICP may be should be further considered. That is, when can values of the model parameters be found such that $\forall t_1, \Pi_1 \geq \Pi_2$? From the equations above a condition on t_2 can be easily obtained:

$$t_2 \le \frac{1}{\beta} \{ (1-p)\beta t_0 - [(1-\beta)\alpha - 1]t_0 + (1-p)(1-\beta)t_p \}$$
 (6)

The interpretation is intuitive. The government chooses to always implement full censorship if it is uncertain how pro-government information given by a government-supported ICP may be. If the government perceives the attitude of the government-supported ICP to be uncertain it may well decide to shut down the independent ICP rather than introduce its own ICP. A corollary is that should the government be able to fully control the information disclosed by a government dependent ICP,

it has no incentive to engage in direct censorship and propaganda, but will choose to allow the two ICP's to compete for the attention of the individuals in the society.

4.3 Censorship or Propaganda?

The above model of government control of Internet content providers is simple and general. It led to a series of interesting conclusions derived from minimalist assumptions about the government and the content provider's preferences. The model is simple in that it does not take into consideration any complexities associated with technology (the Internet vs. the traditional media), government regulation and control mechanisms (legislative v. judicial for example) or individual's patterns of information consumption and use. Yet, the model yields a series of interesting and useful general conclusions, given the assumptions: (1) even independent content providers may have incentive to exaggerate the truth in order to most effectively combat government information; (2) government has an incentive to enter the information market by influencing content as long as its record is not close to perfect and the costs of this government intervention are not prohibitive; (3) given the option to influence content through a government-supported or government-dependent media, the government looses an incentive to introduce censorship and/or direct propaganda but both can be introduced if government's efforts to influence the content fail.

The main importance of this model is that the emergence of the Internet in societies such as Russia actually opens up this third alternative of government interference (in addition to direct censorship/propaganda on one side and allowing for freedom of information on the other side). The Internet offers this possibility by opening a new medium of communication that escapes the traditional structures of government control as is the case in broadcast, radio, and newsprint. Once a government decides it is unable to control the Internet medium completely (either for the moment or permanently), the incentive for its engagement in it rises and it starts to prop up Internet content providers to compete against independent ones. Once this competition starts, the structure of the information space is radically transformed, both in relation to that of totalitarian states and that of democratic states. What emerges is a third way, as an undemocratic government enters competition for maintenance and propagation of its image and power among its population.

Now, the model that we have here needs to be expanded if we are to include all the specificities of the Internet, most importantly five criteria: interactivity, multiplicity, architecture, cost, and timing. Under interactivity, we know that there in fact is not such a thing as an Internet content provider that is entirely different from an Internet user. Each user can provide content through communication by e-mail, bullied boards, design of own websites, many forms of realtime 'talk', and other means. Multiplicity is the Internet's ability to offer multiple channels that, at least in theory, should by far surpass number of television channels, newspapers, radio stations. Without scarcity of frequencies and with low start-up costs, Internet provides for potentially greater plurality of information than any other

medium. Architecture of the Internet also plays an important role, as what we call the Internet actually uses virtually all possible physical networks of communication (telephone lines, optical and other cables, radio and satellite connections, and other) to connect individual nodes into a 'network of networks.' If they ever wish to fully control the Internet, governments need to develop much more sophisticated and diversified means of controlling these network nodes. The cost associated with providing and consuming information over the Internet differs from costs associated with traditional media. Instead of paper and broadcast frequencies, Internet access cost is determined by cost of users' hardware, speed and frequency of access, or other. The general belief is that costs of information should go down with greater availability on the Internet, but we are already starting to realize that with increased quantity of information, the task of evaluation and selection becomes costly for a consumer. Finally, the timing factor is crucial for the Internet. The online media have not yet fully taken advantage of the realtime possibilities of the Internet, but one-to-one communication that is now almost always in realtime (AOL, ICQ, chat rooms) or with little delay (e-mail and chat rooms). Each of these five factors can be built into the general model proposed above, and one can analyze how these different characteristics of the Internet (most unique and in combination definitely unique) affect governments' behaviour and individuals' choices.

5 Government Learning and Freedom to Control

The above game theoretic model helped us explain a story of Russian government's increasingly sophisticated modes of Internet content control. The historical narrative showed a trend from failed attempts at Soviet-style bureaucratic oversight to Yeltsin government's crude monitoring practices to Putin's more subtle ways of influencing online content. By the beginning of 2002, President Putin had started to appreciate the significance of the Internet as a public medium and has moved to integrate government regulatory efforts in the Internet sector into his overall ambition to control all of the Russian media. The evolving Russian Internet policy sheds some important light on Russian President's strategy of political and economic reform.

Most Western observers of Russia agree that Putin's policies have moved Russia away from democracy that only started to take shape, quite problematically, under former President Boris Yeltsin. Huskey (2001) identified Putin's attempts to revive "a disciplined and centralized state machinery" instead of "relying on the institutions associated with integrative politics in democratic countries, such as political parties or social movements." (83) Dunlop (2001) called Putin's reforms nothing less than "authoritarian tendencies," fearing that any progress Putin might make on his highly publicized campaign to reform and enforce a solid legal system would pale in comparison to the damage he could cause by failing to maintain political plurality achieved in the Yeltsin years. Hughes (2001) has compared Putin's center-periphery relations reform with the Tsarist policy of using military gover-

nors to rule the provinces (140). ¹⁹ Brown (2001) argued that the re-centralization policies have brought the regional practice of "guided" or "manipulated democracy" to the federal level.

The building pessimism about the future of Russian democracy (Brown, 2001; Brzezinski, 2001; McFaul, 2001; Odom, 2001) is accompanied by a growing scholarly consensus that the Russian "transition" experience has been one of sometimes-violent competition for power among political and economic elites, both in absence of durable state institutions and in appeal to pragmatically-selected Western political and economic values. To date, President Vladmir Putin has fared well in this world of power competition. In contrast to Yeltsin, whose strategy was to de-centralize the power and give both oligarchs and regional politicians as much power as they could handle, Putin's strategy has been to undo Yeltsin's reforms in this area. Ultimately, it is this strategy, more than any other specific action of Putin's, that brands him an authoritarian leader of a sort. In this context, his use of the Internet policy for increasing the state's control over the information space could have detrimental effects both on individual freedom and on the future of democratic culture and institutions in Russia.

6 Conclusion

Despite its disproportionately small degree of penetration, Internet in Russia has expanded fast and has captured attention of politicians, policy-makers, and the regulatory agencies. The first-round of Russian government's response consisted of legislation that drew heavily on the Soviet bureaucratic experience and fore-shadowed the emerging concern for security and national identity. The second stage was marked by the rise of online news providers and emergence of political campaign web sites. Upon Putin's poorly-contested election as the President, the Russian Internet policy became more aggressive; as government started to promote use of the Internet while expanding its control over Internet content through effective commercial competition against independent content providers.

Traditionally, authoritarian governments have responded to the IT revolution by censoring sources of free and unbiased information (China, Singapore, Middle East), while democratic governments focused on public concerns such as protection of minors and hate speech (United States, European Union). The game theoretic model introduced to explain the Russian case formally showed that governments have a third choice: to promote Internet access and ICP proliferation, and then use the Internet for direct and indirect propaganda. Realizing this danger – even if in the long run the government's ability to overpower independent ICPs dimin-

¹⁹The most important part of reforming what Huskey (2001) called centralized state machinery was Putin's re-centralization of executive power through dividing the country into seven administrative regions, run by Putin's loyal representatives appointed to reign in on the numerous regions' governors and presidents. See President Putin' May 13, 2000 Presidential Decree establishing the seven regions.

6 CONCLUSION 24

ishes – is important if we are to understand the role of both the Internet and free information space in democratization.

The simplicity of the game theoretic model introduced also allowed us to see that introduction of new technologies such as the Internet may open up possibilities of control that were otherwise unavailable to a post-totalitarian authoritarian regime (one that is forced to allow some freedoms in the public and private space, while leaders maintain power and political control through un-democratic means that exclude blunt propaganda, censorship, and terror). In these cases, what may seem more freedom could mean less freedom in the short run and a danger of yet-to-beconceived opportunities for control in the long run. Further, when non-democratic governments show signs of learning which control mechanisms work and which ones do not, we should be especially concerned.

References

Anderson, Robert, Tora Bikson, Sally Ann Law and Bridger Mitchell. 1995. "Universal Access to E-mail: Feasibility and Societal Implications." Rand Corporations Paper.

- Arnold, R. Douglas. 1992. The Logic of Congressional Action. New Haven: Yale University Press.
- Bimber, Bruce. 2000. "Measuring the Gender Gap on the Internet." Social Science Quaterly 81:868–876.
- Boreiko, Aleksander and Pavel Nefedov. 2001. "Cabinet Approves E-Russia Plan." *The Moscow Times*. July 2001.
- Boreiko, Alexander. 2001. "Law Change May Put RuNet Names in Peril." *The Moscow Times*. December 19.
- Brown, Archie. 2001. "From Democratization to 'Guided Democracy'." *Journal of Democracy* 12(4):35–41. Part of the symposium "Ten Years After the Soviet Breakup".
- Brown, Nancy and Jeff Wright. 1997. "Information Technology in the Russian Federation." www.american.edu/initeb/nb2224a/russia.html.
- Brzezinski, Zbignew. 2001. "The Primacy of History and Culture." *Journal of Democracy* 12(4):20–26. Part of the symposium "Ten Years After the Soviet Breakup".
- Bucy, Erik. 2000. "Social Access to the Internet." Harvard International Journal of Press and Politics 5:50–61.
- Clemente, Peter C. 1998. State of the Net: The New Frontier. New York: McGraw Hill.
- Dahl, Robert. 1956. A Preface to Democratic Theory. Chicago: University of Chicago Press.
- Dahl, Robert. 1971. Polyarchy: Participation and Opposition. New Haven: Yale University Press.
- Davis, Richard. 1999. The Web of Politics. New York: Oxford University Press.
- Dertouzos, Michael. 1997. What Will Be: How the New Information Marketplace Will Change Our Lives. San Francisco: Harper.
- Diamond, Larry. 1999. Developing Democracy. Toward Consolidation. Baltimore: The Johns Hopkins University Press.
- Diamond, Larry, Juan J. Linz and Seymour Martin Lipset. 1990. *Politics in Developing Countries: Comparing Experiences with Democracy*. Boulder, Colo.: Lynne Rienner Publishers.

DiMaggio, Paul, Eszter Hargittai, W. Russell Neuman and John P. Robinson. 2001. "Social Implications of the Internet." *Annual Review of Sociology* 27:307–336.

- Dunlop, John B. 2001. Sifting through the Rubble of the Yeltsin Years. In *Contemporary Russian Politics: A Reader*, ed. Archie Brown address =. Oxford University Press.
- Ellis, Frank. 1999. From Glasnost to the Internet: Russia's New Infosphere. London: Macmillan.
- Fishkin, James. 1991. Democracy and Deliberation: New Directions for Democratic Reform. New Haven: Yale University Press.
- Foster, Frances H. 1996. "Information and the Problem of Democracy: The Russian Experience." *American Journal of Comparative Law* 44:243. Reprinted in Russian Media Law and Policy in the Yeltsin Decade: Essays and Documents, edited by Monroe E. Price, Andrei Richter and Peter K. Yu (The Hague: Kluwer Law International, 2002), pp 95-118.
- Gibbons, Robert. 1992. Game Theory for Applied Economists. Princeton, N.J.: Princeton University Press.
- GILC, Global Internet Liberty Campaign. 2000. "Bridging the Digital Divide: Internet Access in Central & Eastern Europe.".
- Gutmann, Amy and Dennis Thompson. 1996. *Democracy and Disagreement*. Cambridge, Mass.: Belknap.
- Habermas, Jurgen. 1989. The Public Sphere. In *Jurgen Habermas on Society and Politics*, ed. Steven Seidman. Boston: Beacon Press.
- Habermas, Jurgen. 1996. Between Facts and Norms: Contributions to a Discourse Theory of Democracy. Cambridge, Mass.: The MIT Press.
- Hammersley, Ben. 1999. "Niet to Net Freedom." The Times. June 23.
- Hoffman, Donna L., Thomas P. Novak and Ann E. Schlosser. 2002. "The Evolution of the Digital Divide: How Gaps in Internet Access May Impact Electronic Commerce." *Journal of Computer-Mediated Communication*.
- Hughes, James. 2001. From Federlisation to Recentralisation. In *Developments in Russian Politics 5*, ed. Stephen White, Alex Pravda and Zvi Gitelman. Carnegie Endowment for International Peace.
- Huntington, Samuel P. 1991. The Third Wave: Democratization in the Late Twentieth Century. Norman: University of Oklahoma Press.
- Huskey, Eugene. 2001. Overcoming the Yeltsin Legacy: Vladimir Putin and Russian Political Reform. In *Contemporary Russian Politics: A Reader*, ed. Archie Brown. Oxford: Oxford University Press.
- Mansbridge, Jane J. 1980. Beyond Adversary Democracy. New York: Basic Books.

Margolis, Michael and David Resnick. 2000. *Politics as Usual: The Cyberspace "Revolution"*. Thousand Oaks: Sage Publications.

- McFaul, Michael. 2001. Russia's Unfinished Revolution: Political Change from Gorbachev to Putin. Ithaca and London: Cornell University Press.
- MMLPC, Moscow Media Law Policy Center. 2000. "Is the Internet Independent of the Law on Elections?" Commentary by the Moscow Media Law and Policy Center. February.
- Mulvey, Stephen. 2001. "Russian Internet Politics." BBC News. March 5, news.bbc.co.uk.
- Norris, Pippa. 1999. Who Surfs? New Technology, Old Voters and Virtual Democracy. In *democracy.com: Governance in a Networked World*, ed. Elaine Ciulla Kamarck and Jr. Joseph S. Nye. Hollis, NH:: Hollis Publishing.
- Norris, Pippa. 2001. Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide. Cambridge: Cambridge University Press.
- NTIA. 2000. Falling Through the Net: Toward Digital Inclusion. Washington, D.C.: U.S. Department of Commerce.
- Odom, William E. 2001. "Realism about Russia." The National Interest (65):56. Fall.
- Palma, Giuseppe Di. 1990. To Craft Democracies: An Essay on Democratic Transitions. Berkeley: University of California Press.
- Price, Monroe E. 1995. "Law, Force, and the Russian Media." *Cardozo Arts & Entertainment Law Journal* 13:795. Reprinted in Russian Media Law and Policy in the Yeltsin Decade: Essays and Documents, edited by Monroe E. Price, Andrei Richter and Peter K. Yu (The Hague: Kluwer Law International, 2002), pp 31-46.
- Price, Monroe E. and Peter Krug. 2000. Enabling Environment for Free and Independent Media. University of Oxford: Programme in Comparative Media Law & Policy.
- Przeworski, Adam. 1991. Democracy and the Market: Political and Economic Reforms in Eastern Europe and Latin America. Cambridge: Cambridge University Press.
- Przeworski, Adam. 1999. Minimalist Conception of Democracy: A Defence. In *Democracy's Value*, ed. Ian Shapiro and Casiano Hacker-Cordon. Cambridge: Cambridge University Press.
- Putnam, Robert D. 1993. Making Democracy Work: Civic Traditions in Modern Italy. Princeton: Princeton University Press.
- Putnam, Robert D. 2000. Bowling Alone: The Collapse and Rivaval of American Community. New York: Simon and Schuster.

Rheingold, Howard. 1993. The Virtual Community: Homesteading on the Electronic Frontier. Reading, Mass.: Addison Wesley.

- ROCIT, Russian Non-Profit Center For Internet Technologies. 1999. "How many on line.".
- Rozumilowicz, Beata. 2002. Democratic Change: A Theoretical Perspective. In *Media Reform: Democratizing the Media, Democratizing the State*, ed. Monore E. Price, Beata Rozumilowicz and Stefaan G. Verhulst. London and New York: Routledge pp. 9–26.
- Schumpeter, Joseph. 1942. Capitalism, Socialism, and Democracy. New York: Harper.
- Selnow, Gary W. 1998. Electronic Whistle-Stops: The Impact of the Internet on American Politics. Westport, Conn.: Praeger Publishers.
- Seregina, Yelena. 2001. "Reiman Wrestles With Communication Goals." *The Moscow Times*. May 15.
- Shanetskaya, Natasha. 2001. "Duma to Mull Over 15 Internet Bills." *The Moscow Times*. January 31.
- Smetko, Holli A. and Natalya Krasnoboka. Forthcoming. "The Political Role of the Internet in Societies in Transition." *Party Politics*. Draft copy of the paper on file with the authors.
- Warren, Marcus. 1998. "Connected: Russian Spies Target Web." The Daily Telegraph. August 6.
- Wilhelm, Anthony G. 2000. Democracy in the Digital Age: Challenges to Political Life in Cyberspace. Oxford: Routledge.
- Wolfe, Elizabeth. 2001. "Ministries Vie for E-Russia Control." *The Moscow Times* . September.
- Wresch, William. 1996. Disconnected: Haves and Have-Nots in the Information Age. Rutgers: Rutgers University Press.