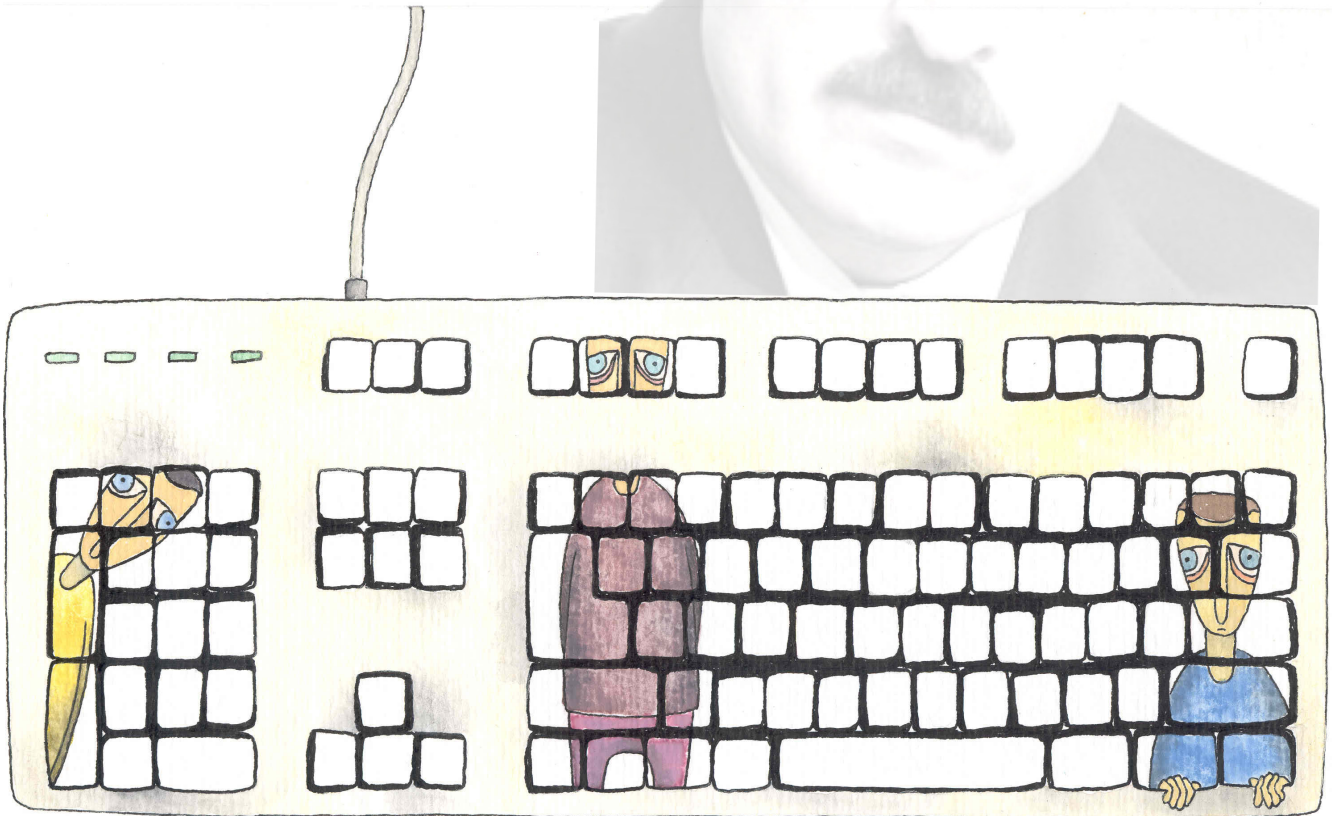
OpenNet Initiative

Internet Watch

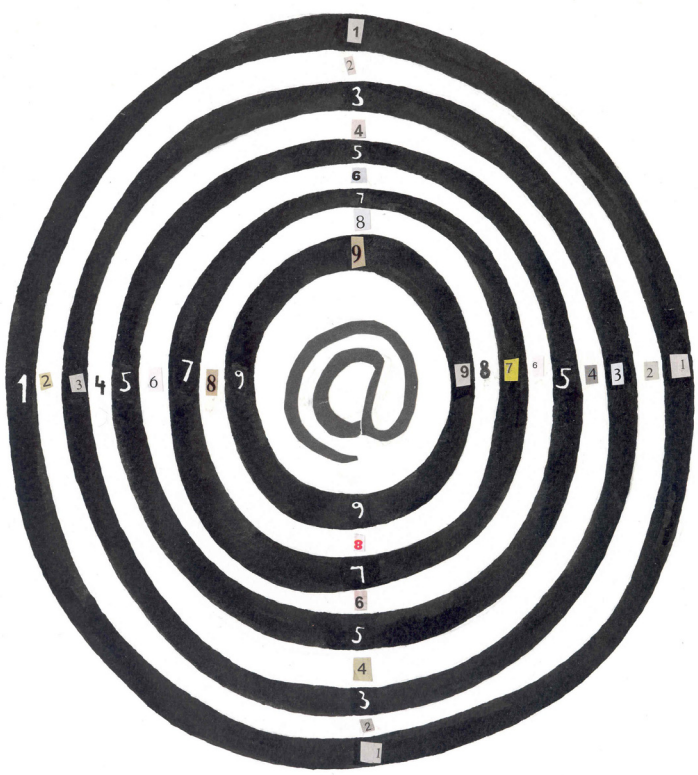
001

The Internet and Elections:

The 2006 Presidential Election in Belarus (and its implications)



April 2006



About OpenNet Initiative's Internet Watch Reports

Internet Watch reports investigate emerging trends in Internet filtering and control. These occasional reports take a detailed look at events, policies, technologies and countries where filtering and content controls are occurring in new and unexpected ways, or where filtering has been alleged but undetected using conventional ONI testing methodologies. They are designed to test hypotheses, refine monitoring techniques, and report on the cutting edge of the global informational battle space.

Internet Watch reports are available in download or hard copy from the ONI.

Executive Summary

As Internet penetration increases globally, so too does its importance to political contests. Both the Internet and cell phones were used to mobilize the masses during the recent "colour revolutions" in the former Soviet republics of Ukraine, Georgia and Kyrgyzstan, which brought down long-standing authoritarian regimes.

This first Internet Watch report, which focuses on election monitoring, represents a pilot venture for the OpenNet Initiative. The motivating hypothesis is that in democratically-challenged countries, the openness of the Net is likely to come under increasing pressure at key political times. One key conclusion thus far is that state tampering with the Internet during election periods is likely to be multi-faceted, elusive, less direct, and more difficult to prove than outright filtering and blocking. A second conclusion, based on the first, is that monitoring the Internet for openness during elections is an extremely slippery task that requires the development of new testing methodologies and monitoring capabilities.

This report presents the findings of ONI's efforts to monitor the Internet during the March 2006 presidential elections in Belarus. Advance preparation included ONI baseline testing and research conducted between June 2005 - January 2006, which revealed that the regime was *not* filtering political websites at that time but that it also had the technical capability to do so, as well as broader infield research which helped to piece together the architecture of control being put in place to control the informational space in Belarus, including the Internet.

ONI's election testing took place amidst many allegations by opposition groups that the regime was actively filtering or disabling independent websites during the election period. ONI testing results indicated that some allegations were misguided; however, others were not, as some politically sensitive websites were inaccessible or "dead" at different times. The main suspect results included:

- 37 opposition and media websites were inaccessible from the state-owned Beltelecom network on 19 March (election day), although they were accessible within Belarus from a different ISP network as well as from the external control location;
- the Internet was inaccessible to subscribers using Minsk Telephone access numbers on March 25 (the day of a major demonstration, when riot police were used to disperse and arrest protesters);
- the website of the main opposition candidate Aleksandr Milinkevich was "dead" on 19 March and experienced access issues on the 21-22, (the post-election protest period); and,
- an opposition website (Charter 97) was only partially accessible between 19 to 25 March.

The testing was unable to prove – conclusively – that the regime was behind these anomalies, although the problems centering on the state-owned Beltelecom network are unlikely to have been simply coincidental. The "dead" websites may have been victims of deliberate Denial of Service attacks (as the site owners claimed), but ONI cannot confirm this without access to the log server files.

Overall, however, ONI found no evidence of systematic and comprehensive interference with the Net. Any regime-directed tampering that may have taken place was fairly subtle, causing disruptions to access, but never completely turning off the alternative information tap.

And yet, this Internet Watch report does not argue that Internet openness in Belarus is robust and guaranteed. Rather, analysis of the political and legal context suggests that the Belarus' regime has both the will and capability to clamp down on Internet openness, and that its capacities to do so are more pervasive and subtle than outright filtering and blocking. The openness of the Internet in Belarus is likely to come under increasing threat both from pending legislation that promises to legalize more active state monitoring, content regulation and blocking of the Net, as well as from increased pressures for self-censorship.

The report ends with a broader call to raise awareness of the importance of monitoring the Internet for openness during election periods, offering reflections on the technical and organizational challenges involved, as well as specific recommendations for election monitoring groups and civil society activists.

Table of Contents

List of Boxes

List of Figures

List of Tables

About the OpenNet Initiative

The OpenNet Initiative is a partnership between the Advanced Network Research Group at the University of Cambridge, the Citizen Lab at the Munk Centre for International Studies, University of Toronto, the Berkman Center for Internet & Society at Harvard Law School, and the Oxford Internet Institute at the University of Oxford. Rafal Rohozinski’s and Deirdre Collings’ work on this ONI Internet Watch report was supported through grants from the Ford Foundation and the Open Society Institute. The ONI project is generously supported by a grant from the John D. and Catherine T. MacArthur Foundation. For more information about the OpenNet Initiative, please visit ONI's website:

http://www.opennetinitiative.org

Acknowledgments

The research presented in this report could not have been completed without the time and effort of our dedicated ONI researchers at Cambridge, Toronto, Harvard and Oxford, as well as our team of in-field researchers based in Warsaw and Minsk, Joanna Rohozinska and others who cannot be named for reasons of personal safety. The field team was responsible for much of the background research and analysis of the political, legal and telecommunications environment in Belarus that informs this report. The ONI is grateful to the Eurasia i-Policy Network which provided invaluable support for understanding and documenting the emerging "matrix of control" in Belarus. Thanks also to Vesselina Haralampieva (Berkman Centre, Harvard Law School) for her work on documenting Belarus' opposition websites, and to Steven J. Murdoch (Security Group, University of Cambridge, Computer Laboratory) who was responsible for much of the detailed technical detective work. ONI testing and list processing was coordinated by Nart Villeneuve at the Citizen Lab (Munk Centre, University of Toronto). The research effort was directed and managed by Rafal Rohozinski (Advanced Network Research Group, University of Cambridge), and the report was pulled together by Deirdre Collings (ANRG, University of Cambridge) whose sound editorial judgment shaped and sharpened the analysis. Special appreciation goes out to Maciej Michalski for the cover illustrations. The ONI is solely responsible for any errors or omissions in this report.

Introduction

In recent years, people-based "colour revolutions" in the former Soviet republics of Ukraine, Georgia and Kyrgyzstan have brought down long-standing authoritarian regimes. These revolutions were effective in part because civil society leaders, armed with cell phones and the Internet, were able to route around the authorities' control of the media to mobilize mass support. The relative ease with which the strong-man regimes were outmaneuvered by agile oppositional actors signaled the growing importance of the Internet throughout the Commonwealth of Independent States (CIS) and the potential challenge it represents to authoritarian powers.[1]

As Internet penetration increases globally, so too does its importance to political contests. This is especially true in the developing world, where the access of opposition actors to mass media tends to be tightly controlled. In more authoritarian countries, the Internet is sometimes seen as the "final frontier" of free informational space because it is less vulnerable to the kinds of state controls that gag traditional media. In some cases, the Internet may be the only channel available to opposition groups contesting entrenched ruling parties. This is true even in countries where Internet penetration is limited, as key political messages carried on the Net are magnified by mouth-to-mouth social networks, rather than by direct access to the Internet itself.

A key hypothesis underpinning the ONI's interest in election periods is this: In democratically-challenged countries, we are likely to see increasing constraints on the "openness" of the Internet during election periods, and these constraints may be more subtle than outright filtering and blocking. For this reason ONI has begun to undertake pilot investigations of the Internet during elections, with Belarus as our second effort.

The February 2005 elections in Kyrgyzstan marked the ONI's first foray into election monitoring.[2] During the Kyrgyz elections ONI researchers were able to document two major Denial of Service (DoS) attacks directed against ISPs hosting major opposition newspapers.[3] The attacks were commissioned from a commercial "bot herder" and traced back to a group of Ukrainian hackers-for-hire. ONI was not able to identify who was ultimately responsible for these attacks. Direct links to the Kyrgyz authorities could not be established. Thus, while no *direct* filtering took place, the DoS attack resulted in the *indirect* censorship of websites while exonerating the Kyrgyz authorities of any direct responsibility. The Kyrgyz case also raised the issue of who benefits most from this kind of indirect filtering. In Kyrgyzstan, the target of the DoS attacks – opposition newspaper websites -- continued to publish print editions while claiming that they were being "censored" by the government. The absence of proof concerning who ordered the attacks, and the fact that the story could have been "spun" to benefit either side (government or the newspapers) meant that both sides were using the incident as a form of "information warfare."

The Kyrgyz case suggests that this kind of "grey" phenomenon – indirect and intermittent filtering as a form of information warfare -- may be more relevant to how the Internet is manipulated during election

---

1 See: *Breaking Down the Great Firewall,* BBC 30 April 2005 available on http://news.bbc.co.uk/2/hi/asia-pacific/4496163.stm ; and *Wireless World: The 'Orange Revolution'* http://www.bestkeptsimple.org/archives/0003820.php.

2 In fact, the *very* first effort was during the 2004 US presidential campaign, when ONI testing found that during the final days preceding the vote, the George W Bush Website was not available to users outside of the US. However the filtering did not prejudice the ability of most US citizens resident in the US - the electorate - to access the site. See, http://www.opennetinitiative.net/bulletins/007/

3 http://www.opennetinitiative.net/special/kg/

periods than outright political filtering itself. It also shows that developing a robust and reliable methodology for monitoring the "openness" of the Internet during election periods is a complex and difficult task. Standard ONI tests detect the presence or absence of filtering as well as the mechanism being used to block specific material (see Annex B). These standard tests have proven robust and reliable when investigating blanket filtering such as that pursued in China, Myanmar and Saudi Arabia.[4] However, they are less suited to deal with the myriad of network "anomalies" that we have seen during our monitoring of the Net during election periods. To date, observed "anomalies" have included intermittent and partial inaccessibility of websites (which may be indicative of filtering), accidental or deliberate server configuration errors, DNS failures, network congestion, and deliberate denial of service attacks against ISPs and specific web servers. A second set of observations, based on our Kyrgyz and Belarus experience, is that independent and opposition groups are quick to allege deliberate regime-inspired filtering, while the regime in question denies all charges. The terrain is grey indeed.

Evidence-based reports of outright "filtering" of opposition websites during elections are rare, and mere accusations – even in the face of a "dead" website[5] – are difficult to verify as direct tampering. For example, the confirmed Kyrgyz DoS attacks did not conclusively reveal the regime's involvement, nor did the other observed network "anomalies" yield conclusive evidence that websites were systematically and comprehensively filtered (as happens in China, for example). We will return to these issues, and the methodological challenges that they raise, in the final section of this report.

In this Internet Watch, we report on ONI's efforts to monitor the March 2006 presidential election in Belarus, as well as earlier baseline testing conducted in 2005 and more qualitative research undertaken to investigate the architecture of control being put in place by Belarus authorities aimed at controlling the country's informational space, including the Internet. This report is presented in five parts:

Part 1 details the reasons why Belarus was a leading candidate for ONI investigation of Internet openness during the elections, given the regime's authoritarian nature, tight control over Belarus' informational space and traditional media, past allegations of Internet tampering, and earlier ONI baseline testing which established the regime's technical capability for potential filtering.

Part 2 reports on the 2006 ONI Internet testing and findings during the presidential election period. The testing confirmed that some websites were inaccessible or "dead" at different times. However, the testing was unable to prove – conclusively — that the regime was behind these anomalies. The testing found no evidence of systematic and comprehensive interference with the Net.

Part 3 builds out the findings, and considers why the regime did not systematically target the Internet during the elections. It also argues that the openness of the Internet in Belarus is likely to come under increasing threat both from pending legislation that promises to legalize more active state monitoring and blocking of the Net, as well as from increased pressures for self-censorship.

Part 4 provides a short summary of the overall findings of ONI testing and research in Belarus.

Part 5 offers broader reflections on the challenges of monitoring the Internet for openness during election periods, and provides recommendations for election monitoring groups and civil society.

---

4 http://opennetinitiative.net/modules.php?op=modload&name=Archive&file=index&req=viewarticle&artid=1.

5 See Annex B for a typology of ONI test results.

Part 1. Why test in Belarus?

The ONI considered Belarus to be an important test-case for monitoring the Internet during elections for four reasons: 1) apparent regime motive; 2) the growing importance of the Internet as a "last frontier" of free informational space in the country; 3) past allegations of regime-directed political filtering; and, 4) previous ONI baseline testing and research which proved that the regime has the technical capability to filter the Net. Let us look at each in turn.

In March 2006, Belarus President Aleksandr Lukashenka sought to continue his 12-year reign amidst rumours that a "denim revolution" was about to unfold.[6] The backdrop to these elections was the President's increasingly authoritarian regime. Since coming to power, Lukashenka has put in place a pervasive edifice to reinforce his rule, while keeping competitors contained and silenced. On paper, Belarus' legal and administrative framework appears democratic. Indeed, the regime is characterized by a hyper-legalism wherein all actions – including civilian repression -- require a legal pretext. In practice however, all state bodies function to service the control of the Presidential Administration (PA), and it is the President's office that determines when laws are to be enforced, and which illegalities are to be prosecuted.

Lukashenka's architecture of authoritarian control has three key dimensions: political/security, legislative/administrative, and economic. The scope and reach of these elements has expanded in lock-step with the entrenchment of the regime, from the 2001 presidential elections through to the rigged referendum in 2004 (which lifted the constitutional limit allowing Lukashenaka to run for a third term), through to this year's presidential elections (March 2006). Together the troika works to diversify pressure points on both government administrators and ordinary citizens, ensuring compliance with regime interests while maintaining the illusion of legality. (See Annex A for a more comprehensive discussion of Lukashenka's "matrix of control" with specific reference to the informational sphere and the Internet).

Politically, all key decisions, in all spheres, are made by the President, either in the form of official Decrees or "unofficial" (oral) statements that carry the same weight, and are implemented

Box 1. "Father" knows best

"Batka" – or "father" as President Lukashenka is called by his supporters -- has brought stability, continuity, and economic security to the lives of the some 55% of Belarus citizens who genuinely support him,* namely the rural, middle-aged workers and elderly. Lukashenka was swept to power in 1994, on the strength of his promises to eradicate rampant corruption and redress the large drop in living standards, which had fallen by half during the country's first four years of independence. Once voted in, Lukashenka delivered on his promises, rooting out corruption and "normalizing" the economy by redirecting millions of dollars into obsolete industries and collective farms. This both resuscitated livelihoods and secured Lukashenka the lasting loyalty of the workers. He also "stabilized" government by destroying the old elites (mostly the Soviet-era *nomenklatura*) and replacing them with cadres more loyal to himself. And then he embarked on an ever-more-authoritarian project to ensure his continued political rule. He disbanded the Parliament, creating a rubber-stamp institution in its stead, and proceeded to rule by Presidential Decree. He created a "healthier" society by introducing pervasive ideology in support of his policies in schools and workplaces, forcing young people to join the BRSM (*Belaruskii Respublikanskii Sojuz Molodzhezhi* - Belarusan Republican Youth League), and limiting foreign travel and contact.

* Statistic comes from a January 2006 Gallup/Baltic Survey

[6] Insiders suggest that the term "denim revolution" has far more resonance in the Western media than within Belarus itself. Indeed, there was little belief inside Belarus that a "revolution" would follow the election, and the size and persistence of the post-election demonstrations -- with tents set up in October Square -- took many by surprise.

even if they contravene or conflict with existing legislation.[7] Legislative and administrative bodies, from the National Assembly through to the Ministries on down, function to sanction presidential decisions – either by "proposing" legislation that the PA has "suggested" or rubber-stamping pre-approved legislation. The subsequent enforcement is also subject to presidential directives. Presidential power is underpinned by a solid array of security bodies. In the informational sphere, these include the Committee for State Security (KGB), the Ministry of Internal Affairs (especially Department "K" responsible for computer crime), and the State Center for Information Security. All have wide latitude to investigate, surveil and interrogate citizens (or request same), including the monitoring of any and all communications to "safeguard security."[8]

Legally, all organizational entities – including political parties, NGOs, television and newspapers, and Internet Service Providers (ISPs) -- are subject to strict rules for registration and licensing, the technicalities of which have often been used to shut down or stifle independent or oppositional organizations, news media, and those who dare to criticize the President in any way. Articles 367 and 368 of the Criminal Code, which make it a crime to "defame" or "slander" the President, are often used in this respect. Beyond this, new amendments to the Code in December 2005 further restrict the public's capacity to gather, organize and speak. Among other things, the amendments criminalize any activities that "discredit the Republic of Belarus."[9]

Economically, the formal financial regulative bodies[10] have extensive

Box 2. Economic compellence: The Velcom case

Velcom is Belarus' first private GSM operator, established in 1999. Initial control of Velcom was split as follows: the Cypriot-owned SB Telecom (49%), the state-owned Beltelecom (31%), and the state-owned Beltechexport (20%). However, Beltelecom was unable to contribute its portion of the statutory capital obligations. The parties signed a new agreement, reducing Beltelecom's capital obligations to 1%, while increasing the obligations of the foreign founder to 69% (SB Telecom-69%; Beltechexport-30%; and Beltelecom-1%). The agreement further stipulated that Beltelecom would retain 31% share of votes and profits, and that it had the right to "buy back" its extra 30% of shares at a later date.

Within a few years the market value of Velcom rose to several hundred million dollars, and share prices rose accordingly. As Beltelecom continued to be unable to buy back its 30%, the President of Belarus ordered that Beltelecom's shares would be 31%, to guarantee 'real state control of company activity,' (even though it de facto controlled 51% of votes and profits). Velcom partners were requested to "present" a portion of their shares to Beltelecom to raise its official shares to 31%. The state-owned Beltechexport presented 10%. The foreign founder, however, refused to hand over the remaining 20% without compensation.

Suddenly Velcom started to have problems. The MCI threatened to cancel Velcom's license, due to a licensing "violation" which the Ministry, itself, had previously allowed to occur. The managers of Velcom, including the Cypriot owners, were slapped with a criminal case, accused of abusing custom privileges some years previously. Despite the lack of evidence, the Cypriot owners were arrested and placed in KGB detention. SB Telecom capitulated, handing over 20% of its shares to Beltelecom. The criminal case was closed, and Velcom's licensing problems disappeared.

Source: *Tomaszevskaya* (2003) on http://www.ucpb.org/bel/showart.shtml?no=3305

7 For example, during a meeting devoted to the development of cellular communication the President gave the order to cancel the international tender for a third GSM license and instead, to create a completely state-owned GSM operator, BeST. See also Footnote 14.

8 Although the privacy of personal communications is enshrined in the Constitution, other laws override this right when it comes to issues of "security." See Annex A, as well as discussion in Part 3.

9 According to recent statements by the Minister of the Interior (Uladzimer Navumau), this law will be used to track down regime dissenters in cyberpace. This discussion is picked up in Part 3 of the report.

10 That is, the National Bank, State Customs Committee, Tax Ministry, and State Control Committee.

powers to supervise all economic activity and financial transactions in the country. These powers are often used to harass independent entities – from civic groups and organizations, through to newspapers and other information producers as well as businesses -- to pressure them to conform to state ideology and directives. Many critics and businesses have been effectively curbed after being charged with "tax irregularities" or other "economic crimes." (See Box 2 above. For more details, see Annex A).

From the perspective of this report, one critical result of the regime's political, legal and economic machinations has been the gagging or shutting down of independently-minded political parties, non-governmental organizations and media.

When it comes to the traditional channels of Belarus informational space (press, radio, television), the independent press are rendered particularly vulnerable because of the state monopoly on printing and distribution facilities, which is controlled directly by the Presidential Administration. These facilities can and do suspend the production and distribution of publications that chose to carry "inappropriate" information, and many independent papers have been forced to close. Television and radio are dominated by state-run media, with the remaining independent outlets "choosing" to carry mostly entertainment programmes or local events. International media is limited and declining (See Box 3, next page).

Thus by 2005, a host of foreign and independent observers were expressing grave concern about Belarus' restrictions on freedom of speech, press, assembly, and association, and the intensified pressure on independent media and NGOs, many of which were forced out of existence through legal technicalities compelling de-registration, or throughfrequent tax investigations and other state-sanctioned allegations and harassment.[11]

Against this backdrop, the Internet, whose content remains relatively unfettered for now, is seen by many as the last breach in Lukashenka's informational blockade on free speech.[12]

11 See, for example *Country Reports on Human Rights Practices - 2004*. U.S. Department of State, released by the Bureau of Democracy, Human Rights, and Labor. February 28, 2005. http://www.state.gov/g/drl/rls/hrrpt/2004/41671.htm. Human Rights Watch, 2005, Belarus available on http://hrw.org/english/docs/2006/01/18/belaru12217.htm .

12 See, for example, Valentinas Mite, *Belarus Opposition Politicians Embrace Internet, Despite Digital Divide*, RFE/RL, 07.02.2006.

Box 3. Discipline and punish: Keeping the opposition and media in line

Civic organizations, political parties, trade unions and the independent media form the backbone of the political opposition in Belarus. It is not coincidental, then, that the Lukashenka regime "disciplines" them collectively. Rather than a frontal assault to ban independent organizations and publications, the authorities use multiple legal, economic and administrative methods to limit activities, prevent public gatherings, outlaw funding sources, gag public communication efforts, and shut down communication channels and spaces. Control is achieved through legislation (via an ever expanding array of strict financial, administrative and content regulations), administrative harassment amounting to a "persecution by permits" (with "re-registration" being a proven method to thin out the ranks), hounding by tax authorities, and the threat of being accused of "economic crimes." More "hands on" tactics like phone-tapping, regular monitoring by the KGB, and other forms of intimidation are also wide-spread but difficult to document. Arrests of opposition activists, and their confinement to "administrative detention," have increased but charges are rarely overtly "political." Rather the offenses are classified as "economic" or "hooliganism." At the most extreme, political opponents -- including a journalist -- have "disappeared."

For traditional media, the State Press Committee implements state information policy (e.g., ensuring no criticism of the regime) and is empowered to suspend the activity of media outlets, and slap large fines on publications or individuals. A common reason for State Press Committee intervention is to combat so-called "honor and dignity" offenses, that is, any statement that "defames the honor and dignity" of state officials.

The independent press is attacked administratively through restrictive registration and accreditation policies, unfair taxation. And, as noted in the main text, is vulnerable because of the state's monopoly on printing and distribution facilities. According to Reporters Without Borders, the Lukashenka regime has "… *systematically shut down the country's few struggling independent newspapers by throttling them financially with huge fines or using ridiculous bureaucratic pretexts."*

As for television and radio the Belarus Broadcasting Company is subordinate to the President. Remaining independent radio and television outlets operate on shoestring budgets, avoid news programming (so as not to risk license loss) and focus on entertainment and local events.. Licenses are issued on the basis of "political loyalty" and thus can be easily withdrawn.

The penetration of international media is limited and declining. Like domestic media, international publications must be registered (vetted) by the central authorities before being distributed in Belarus. Most individual cable operators, who are responsible for the materials they re-broadcast, have stopped rebroadcasting BBC and CNN, leaving Euronews as the only major international service available to some 30% of cable subscribers. Russian channels, which used to be a source of alternative information, have been fully or partially suspended with Belarus' content taking their place. The authorities have been known to charge Russian correspondents in Belarus with "honour and dignity" offenses, to prevent them from transmitting (to Russia) materials viewed as unfavorable to the Lukashenka regime.

Sources: "Viasna '96" monthly reports catalogue cases of intimidation, harassment and persecution, see: www.spring96.org ; Belarus Helsinki Committee's Annual and Monthly Reports (bhc.unibel.by); *Reporters without Borders, Worldwide Press Freedom Index 2005;* IREX, *Media Sustainability Index 2004 and 2006;* Jan Maksymiuk, *How Lukashenka has dealt with independent media,* RFE/RL Reports, 26 December 2000, Vol.2, No.48.

Internet: Lukashenka's "Trojan Horse"?

As traditional media have become either state-run, state-sanctioned, or shut down in Belarus, the Internet as a medium for information has grown in importance.[13] Given that some see the Internet as Lukashenka's "Trojan horse," it is not without irony that his regime has made significant effort to expand Belarus' telecommunications capacities as part of the plan to modernize the state. State policies also demonstrate Lukashenka's desire to get telecommunications capacities into the hands of his rural supporters. Beltelecom's cross-subsidization of local telephone calls is one example of this, as are the aggressive policies for universal access.[14]

Although Internet penetration in Belarus remains amongst the lowest in Europe, the user-base is on the rise. Estimates suggest that the number of Internet users doubled between 2002 and 2005, and now reaches close to some 2 million or 20% of the population, although only some 5% are thought to be "permanent" users due to the high cost of access.[15] Surveys suggest that most users are young, educated and urban, based in Minsk or the regional centers.[16] 40% of users are also government employees, which has important implications for constraining their civic or oppositional cyberactivism.[17]

In this respect, the majority of Lukashenka's core constituency – the rural workers, middle-aged and elderly – are not active Internet users as of yet. A 2003 survey on the political attitudes of Internet users and non-users found Internet users were more likely to be skeptical of the Lukashenka regime's policies and propaganda, trust independent news sources more than state-run organs, and were more inclined to actively support the opposition.[18]

The opposition takes to the web…

Even three years ago, most "independent" websites in Belarus – of oppositional political parties, human rights groups, non-governmental organizations – offered little more than slogans, basic contact information or "wire service" information without analysis. During the October 2004 parliamentary election campaign, for example, the websites of non-regime candidates offered a few oppositional slogans and minimal information on some of the hopeful contenders.

---

13 For example, Reporters without Borders asserts: "*The Internet is an efficient source of independent news in a country where traditional media are under constant government pressure and online material is not censored much.*" See also: "*Belarus Protesters turn to the Internet*," http://i-policy.typepad.com/informationpolicy/2006/03/belarus_protest.html

14 See discussion of the state-owned Beltelecom monopoly below. BeST is a fully state-owned mobile phone operator enacted in 2004 to ensure a roll-out of mobile services to rural and poorer regions of the country, which would not be encumbered by market considerations.. According to the license terms, the new GSM operator must provide special pricing for low-income subscribers and cover remote rural areas. The government expects the BeST network to cover 90% of the population by 2008/9.

15 See "*Internet Users in Belarus*" at http://www.e-belarus.org/news/200506021.html. Estimates of users vary considerably. Non-regime sources suggest a significant rise in Internet users since 2002, from 809,000 users in 2002 (Reporters without Borders, *Internet under Surveillance 2004*) to 1,391,900 in 2003 (CIA World Factbook 2006). Based on the official estimate of 2 million in 2005, it would seem the user-base has doubled in the space of three years.

16 A 2003 survey found that 33% of active users were aged between 20-24, 50% were university graduates, 23% lived in Minsk and a further 46% lived in regional centers.

17 In 2004, all government employees in Belarus (which represent 80% of all employed people) became "contract employees," with contracts renewable annually. As such, they are now much more vulnerable to job dismissal, which discourages participation in non-state sanctioned activities, including critical commentary. See Annex A.

18 Source: Belarus Independent Institute of Socio-Economic and Political Research, 2003 Survey.

The contrast with 2006 is stark. In the run-up to the elections, the main opposition candidates signalled their intent to leverage the Internet's communicative and organizational power.[19] Aleksandr Milinkevich had a site up and running almost immediately following his nomination[20] and the United Civic Party began distributing a regular e-mail bulletin, while dramatically improving the informational content and appeal of its website.[21] Beyond this, websites concerned with human rights in Belarus carry an abundance of news and analysis (see, for example, Annex C and D), and some independent papers and oppositional publications have moved on-line.[22] Certainly, the information and commentary contained on the websites of opposition groups and independent news sources throughout the election and post-election protest period would not have been allowed to appear in the strictly controlled Belarus' newspapers, radio or television.[23]

Moreover, the 2006 election period saw new and spontaneous uses of the net for political organization -- as forums and blogs were used by "ordinary" people to connect and coordinate action. There was a rash of "flash mob" political gatherings in Minsk and other centres that were not organized by the official opposition, but by young people who coordinated their gatherings via the Internet and text messaging (see Part 3).

...and anticipates the spider

Given the Internet's growing importance to the opposition, a significant subplot of the 2006 elections was whether or not the regime would seek to "shut down" the websites of oppositional candidates and independent news sources. Indeed, the loudly critical "Charter 97" website – an opposition site that is particularly popular with Western audiences because it also carries English -- anticipated that the authorities would seek to filter it, and posted information on how users could find alternative access routes.[24]

In the event, however, Internet freedom did not alter the election results. On the 19th of March, Lukashenka won, claiming some 82.5% of the vote, with Milinkevich garnering a mere 3%. Protests erupted as the opposition called foul-play, and carried on for the following week. While these rallies at times reached some 10-15,000 demonstrators, the "denim revolution" did not ignite.[25] By week's end, momentum had flagged, and the police were sent in to root out the diehards.

---

19 Milinkevich told Radio Svodboda: *"There is no equal access to the media [in Belarus]. We bank on the remaining independent newspapers, samizdat [underground press], and the Internet."* (RFE/RL—25.01.2006).

20 http://by.milinkevich.org/.

21 www.ucpb.org.

22 In December 2005, for example, the opposition newspaper Salidarnasc ceased printing and became an exclusively on-line newspaper. See: Belapan,14.02.2006, www.gazetaby.com .

23 Although observers noted the extraordinary appearance of opposition candidate Kozulin on television prior to the elections, where he delivered a highly critical speech, which later found its way to Internet sites. See: "*Daring to crticise Belarus' President,"* on http://news.bbc.co.uk/go/pr/fr/-/2/hi/programmes/from_our_own_correspondent/4790912.stm See also "*Belarus stifles critical media*" on http://news.bbc.co.uk/go/pr/fr/-/2/hi/europe/4818050.stm .

24 See: www.charter97.org. The site provides news, commentary, and an active opposition blog. During the elections, the blog provided up-to-the minute information on election protests and events. Charter 97 has made various allegations in the past of being disabled by way of regime-directed "denial of service" (DoS) attacks (e.g., February 2005). A DoS attack involves flooding the server with packets (requests) to overwhelm its capacity and thereby causing it or its network connection to fail.

25 These figures are cited by most independent media accounts. Opposition sources claim higher figures of 20-40,000.

Past allegations

Allegations of Internet blocking in Belarus are not new. During the 2001 presidential elections, various independent or oppositional groups claimed that their sites were inaccessible, and that the Lukashenka regime was deliberately blocking access. By contrast, the authorities issued the entirely plausible counter-claim that Internet problems were caused by access overload: too many people were trying to access the sites all at once during the elections.[26] In June 2003, the www.bakte.net site was allegedly blocked on the order of the secret police (KGB) because it had posted the text of a book criticizing the President, which the Ministry of Foreign Affairs had called "political pornography." During the 2004 parliamentary elections and referendum (which allowed President Lukashenka to amend the constitution so he could continue his reign), oppositional websites again reported access problems, albeit on a lesser scale.[27] In 2005, various websites claimed they were victims of deliberate blocking by state authorities or DoS attacks.[28] However, none of these accusations has been independently verified on the basis of testing. And in the absence of this, the Lukashenka regime's claim that any Internet problems stem from overloaded servers is at least conceivable.

ONI baseline testing in 2005

To explore allegations of politically-motivated regime blocking of sites, ONI undertook baseline testing between June 2005-January 2006. The results confirmed that filtering was taking place -- but *not* of political or independent sites, which remained up and unfettered. Rather, the only "high impact" websites[29] being filtered in Belarus at that time were Russian gay porn sites: ONI attempts to access these "gay" sites from within Belarus consistently resulted in a "connection refused" error, even though the sites could be reached from a control location outside Belarus.

In fact, the authorities have formally admitted to the filtering of the Russian sites, which they said were "legally" and openly blocked because of their deemed unacceptable pornographic nature.[30] What is of note here is that the regime felt obliged to make the legal case for this action, which was put together in 2004. As noted above, the government is characterized by a hyper-legalism, with all state actions requiring a legal basis (even if this stems from a Presidential decree and laws are applied in a highly selective manner). Non-lawful blocking of the Internet could be considered a violation of the Belarusan constitution which on paper "guarantees" free speech. As of yet, there is no law on the books that specifically addresses the right of the state to regulate or block websites, although, as we shall see in Part 3 below, this law is probably on its way.

---

26 No official documents confirm that the government blocked any sites. However, on 10 September 2001, Letvinskiy Zubr – the "code name" for an anonymous but well-known commentator on the Internet in Belarus -- wrote a letter to Belarus Media claiming insider knowledge that the decision to block the Internet was "made on the highest level" with the First Deputy Head of the Presidential Administration giving orders to the Ministry of Communication to "fix the Internet and anti-president and anti-national slander…".

27 Some sites which claimed vote rigging on the referendum were allegedly blocked for most of election day. However, no testing was conducted to confirm this was the case. By way of analogy, it is interesting to note that several online newspapers, such as www.naviny.by, had their phones turned off for the day. See Freedom House, *Nations in Transition 2005*.

28 For example, in August 2005 a site with cartoons about President Lukashenka was reportedly blocked, and the two youths who had placed the cartoons online were charged with the criminal offense of slandering the President (see Part 3 below).

29 The ONI "high impact" test list is one that is tailored specifically for the country being tested, and is comprised of sites that are likely to be a potential target of state action because of their sensitive or critical (political) nature (See Annex B).

30 A senior figure from the Ministry of Communications officially acknowledged the blocking in an interview with Radio Svaboda. For information on how the legal case for blocking the sites was built up in 2004, see: Belnet, 12.10.2004.

They have the technology

ONI testing in 2005 confirmed that the Belarus authorities have the technical capacity to filter websites. The testing revealed that Russian sites were filtered by ISPs configuring their routers to reject requests for the offending sites' IP address (a method called IP address blocking or null routing). Further infield investigation by the ONI team revealed that the state's capacity to control the physical functioning of the Internet lies at three levels:

The first level is the State Center for Information Security (GCBI), a body that used to be part of the KGB but now reports directly to the President and is roughly equivalent to the US National Security Agency although its focus is domestic rather than international. Among other things, the GCBI controls the top level Internet domain (.by), meaning it is in charge of registering all sites within that domain. This also means the GCBI is in a position to tamper with the DNS records of any website within its registry to render it unaccessible, should this be of interest. Indeed, during the 2001 presidential elections, the opposition accused the GCBI of just such tampering when some of their websites went down.

The second level is by way of the state-owned Beltelecom telecommunications monopoly, which is controlled by the Ministry of Communications (See Box 4). Beltelecom's monopoly extends over all external communication lines, and as such functions as Belarus' central ISP. The thirty or so local ISPs have been granted licenses to connect through Beltelecom facilities, and no operators have fully independent external links to the Net, with the exception of the academic and research network (BasNet), which comes under a different set of controls.[31] Thus, most Internet traffic within Belarus flows through one state-owned choke point, making for an ideal monitoring or filtering set-up. A filter installed on the main router of Beltelecom can block IP-addresses of external sites that are hosted outside of Belarus regardless of their

Box 4. Beltelecom monopoly: Revenue, power and control

Beltelecom is the main source of revenue for the Ministry of Communications (MIC). Various MIC regulations suggest that protecting Beltelecom's market hegemony is a priority. One such example is the ban on transceiver satellite antennas for commercial providers. Another is the essential prohibition of IP-telephony services by commercial providers, which, if this were allowed, would undercut Beltelecom's lucrative earnings from international telephone communications. Currently, Beltelecom provides IP-telephony services at a substantial profit, (charging only 30% less than regular telephone costs). Some clandestine IP-telephony operators tried to provide services at vastly reduced rates, and generated some $200,000 USD worth of business before caught by the KGB, fined, charged and shut down (See Annex A).

Formally, the monopoly exists only in relation to external communication lines, as any operator may provide services for local telephone calls. However, in practice, Beltelecom operates a cross subsidizing system, using profits from the very high charges for international phone calls and Internet to subsidize local call costs, which means that commercial operators cannot compete. In addition, extra profits from Beletelcom subsidize the otherwise unsustainable collective farms and outmoded industries which provide essential jobs to Lukashenka's main powerbase (rural workers).

The state's financial interests in the telecommunications 'market are substantial. In 2004 the market totalled USD 700 million with mobile communications accounting for 39% of the market, and fixed telephony, Internet access and data transmission equalling 61%. The growth of the stationary communications segment totalled 40%, and the mobile communications market had doubled. The government, which has controlling shares in all mobile operators, has been the single greatest beneficiary.

31 Basnet is effectively a government network – see Annex A. Note also that the major wireless service operators -- Velcom, MTS, and BelCel -- are obliged to use Beltelecom hardware facilities for all international traffic.

domain name. This means, for example, that an opposition site hosted in the United States and registered as .org can be rendered inaccessible to anyone trying to access the site from within Belarus. At various times, the opposition has accused GCBI of installing filters at Beltelecom.[32] Beyond this, there is official acknowledgment that other state security organs like the Ministry of the Interior have comprehensively surveilled and intercepted Internet traffic to catch a variety of "cybercriminals" (See Annex A and Part 3).

The third level for potential filtering of websites is at the level of the non-state owned ISPs themselves.[33] In some ways this capacity is superfluous, given Beltelecom's overarching control. However, any ISP could install filters to block Internet sites, and no doubt would do so if directly requested by a state security body. ISPs, like all non-state organizations in Belarus, are inherently vulnerable to state persecution by permits, fines or criminal charges (See Part 3 below). During the 2001 presidential elections, the ISP "Open Contact," which also administers the central database for the .by domain (on behalf of GCBI), was accused by the opposition of blocking various websites within Belarus by way of DNS tampering.

But are they using it?

Just because the regime has the capability to shut down the Net and there have been allegations that it has, does not prove the reality of active filtering for political purposes. With this question in mind, ONI commenced its monitoring of the Internet during the 2006 elections.

32 There have also been persistent rumours, reported in the Polish press that the authorities have procured technology for filtering from China. See: http://www.bybanner.com/show.php3?id=1295; http://www.charter97.org/2005/11/25/filtr . Note, however, that ONI has not verified any patterns of filtering consistent with those used in China. See the ONI report on China.

33 As of 2005, a total of 32 providers are connected to Internet access nodes through Beltelecom. According to ISP assessments, the dial-up services market totalled some USD 24 million in 2004, which was up USD 17 million from 2003. Beltelecom has established 187 Internet access points with 732 'work places'. It is planned to put into operation 92 more 'work places' in 2005 and 115 in 2006-2007.

Part 2. Monitoring Belarus

ONI conducted extensive monitoring and testing of the Belarus Internet throughout the 2006 presidential election and post-election protest period (March 18-25 to check for disruptions to access. This testing was undertaken amidst allegations that the regime was actively filtering "independent" Internet websites, or rendering them unreachable by way of Denial of Service (DoS) attacks.[34] In preparation for the monitoring, ONI modified its testing protocol to allow for a more refined look at the Net and enable greater precision with follow-up investigation of any "anomalous" results. ONI increased the frequency of its regular testing protocol, and broadened the testing to include a second Belarus ISP. In addition, new methods were developed to measure network latency on the interconnection points between the Belarus Internet and its upstream providers. We also paid close attention to nameserver errors (as this was a problem reported in previous elections) and aggressively followed-up reports on website access outages as well as alleged DoS attacks.

What we tested, and what we found…

ONI testing did not detect *comprehensive* or *systematic* filtering of the Internet using known filtering techniques during the election period. However, the quality and consistency of access to some sites varied considerably, and on critical days, up to 37 opposition and independent sites across 25 different ISPs were inaccessible from within the state-owned Beltelecom network. On election day and after the website of the main opposition candidate (Aleksandr Milinkevich) was "dead," as was another opposition site -- Charter 97. On the day that the police cleared the last remaining protesters from October Square (25 March) Internet connectivity by way of Minsk telephone dial-up services failed. And, there were three instances of confirmed "odd DNS errors" affecting opposition websites. While no case yielded conclusive evidence of government inspired tampering, the pattern of failures as well as the fact that mostly opposition and independent media sites were affected, suggests that something other than chance was afoot.

A closer look…

Between 12-25 March 2006, ONI monitored access to a list of 197 "high impact" websites on two Belarus' ISPs.[35] Tests were run from Belinfonet between 12 to 25 March, and on Beltelecom from 17 to 25 March. The "high impact" list, which had been developed by our field research team in prior testing cycles, contained websites of opposition parties, human rights groups, on-line forums, and other sites that had a political character or could be perceived as sympathetic to the opposition movement.[36] Figure 1 (next page) summarizes ONI testing results in chronological order, along with the major events that took place.

---

34 See partial listing of 2006 Internet-related allegations in Part 2, Figure 1 below and Annex D.

35 In both cases, the testing was carried out from Minsk, which may mean that the results obtained do not reflect the access available from other parts of Belarus. However, as Beletelcom is the top tier ISP, and the one though which most ordinary subscribers as well as other ISPs get their connectivity, we consider the results to be robust.

36 Site languages included: Belarus, Russian and English. Some sites were in two or all three languages.

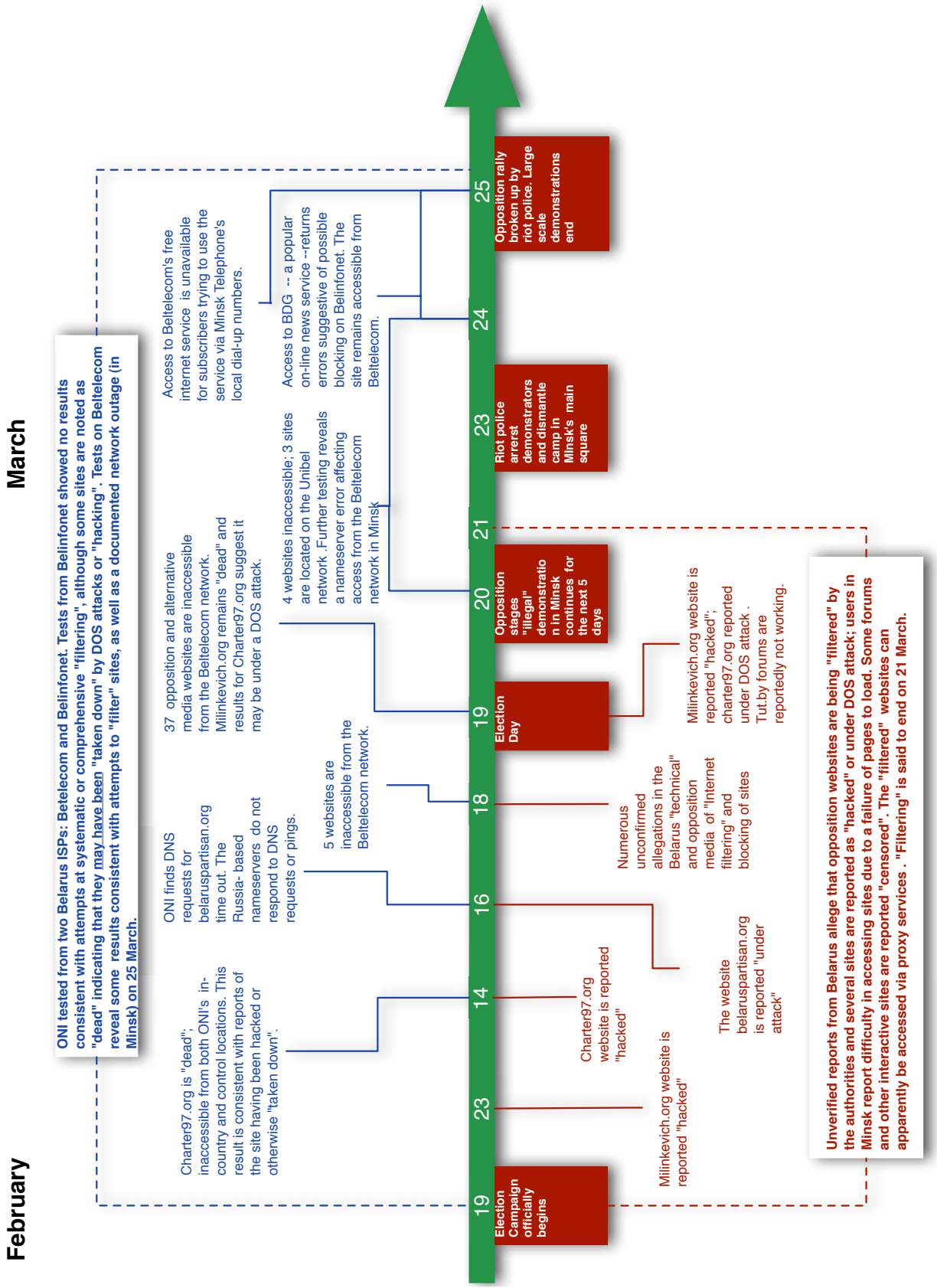

February
March
19
23
14
16
18
19
20
21
23
24
25
Election Campaign officially begins
Election Day
Opposition stages "illegal" demonstratio n in Minsk continues for the next 5 days
Riot police arrerst demonstrators and dismantle camp in Minsk's main square
Opposition rally broken up by riot police. Large scale demonstrations end
ONI tested from two Belarus ISPs: Betelecom and Belinfonet. Tests from Belinfonet showed no results consistent with attempts at systematic or comprehensive "filtering", although some sites are noted as "dead" indicating that they may have been "taken down" by DOS attacks or "hacking". Tests on Beltelecom reveal some results consistent with attempts to "filter" sites, as well as a documented network outage (in Minsk) on 25 March.
Charter97.org is "dead", inaccessible from both ONI's in-country and control locations. This result is consistent with reports of the site having been hacked or otherwise "taken down".
ONI finds DNS requests for belaruspartisan.org time out. The Russia- based nameservers do not respond to DNS requests or pings.
5 websites are inaccessible from the Beltelecom network.
37 opposition and alternative media websites are inaccessible from the Beltelecom network. Milinkevich.org remains "dead" and results for Charter97.org suggest it may be under a DOS attack.
4 websites inaccessible; 3 sites are located on the Unibel network .Further testing reveals a nameserver error affecting access from the Beltelecom network in Minsk
Access to Beltelecom's free internet service is unavailable for subscribers trying to use the service via Minsk Telephone's local dial-up numbers.
Access to BDG -- a popular on-line news service --returns errors suggestive of possible blocking on Belinfonet. The site remains accessible from Beltelecom.
Milinkevich.org website is reported "hacked"
Charter97.org website is reported "hacked"
Numerous unconfirmed allegations in the Belarus "technical" and opposition media of "internet filtering" and blocking of sites
The website belaruspartisan.org is reported "under attack"
Milinkevich.org website is reported "hacked"; charter97.org reported under DOS attack . Tut.by forums are reportedly not working.
Unverified reports from Belarus allege that opposition websites are being "filtered" by the authorities and several sites are reported as "hacked" or under DOS attack; users in Minsk report difficulty in accessing sites due to a failure of pages to load. Some forums and other interactive sites are reported "censored". The "filtered" websites can apparently be accessed via proxy services. , "Filtering" is said to end on 21 March.

Figure 1. Chronology of Belarus testing and results (March 2006)
Pre-election reports and testing (12-18 March 2006)

1) **14 March: the main opposition website Charter 97.org was reported as "hacked."**[37] ONI testing confirmed that this site was "dead" on the morning of 14 March (inaccessible from Belinfonet as well as our control location). This result is consistent with a site having been taken down by its owner, or coming under a successful DoS attack. Full access to the site was restored by the afternoon of 14 March.

2) **16 March: several opposition and independent websites allegedly come under unspecified network-based attacks causing them to fail.** The Belarus opposition and "technology" media reported that the server hosting the website of the main opposition leader www.milikevich.org came under an unspecified attack causing it to fail "for a few hours." Other allegedly affected sites included: charter97.org, grodno.net, lida.info, bybanner.com, it-belarus.net, svaboda.org, tut.by, kozylin.com.[38] For these sites on this date, ONI testing could not confirm that the sites were down. All sites were accessible, according to our tests, although some anomalies were noted (see discussion below). ONI did not detect any filtering on this date. (Although note that the absence of filtering does not rule out the possibility of a network based attack).

3) **16 March: The website belaruspartisan.org was reported "under attack."** ONI testing found that DNS requests for belaruspartisan.org timed out. The site's primary nameservers -- ns1.agava.net.ru (195.161.118.36) and ns2.agava.net.ru (81.176.64.2) -- are based in Russia. Both failed to respond to DNS requests or pings. However, the namesevers also failed to resolve the Russian site, agava.net.ru, which suggests that the problems were coincidental and not a deliberate attempt to "attack" the belaruspartisan.org site.

4) **18 March: Five sites accessed through the Beltelecom network returned results consistent with those for "blocked sites".** On 18 March, the Belarus site bybanner.by reported that "opposition sites" failed to load, and alleged that authorities "may be blocking the Internet."[39] ONI testing indicated that five sites tested from the Beltelecom server returned results typically associated with attempts to filter access. Two kinds of error were observed: two instances of "connection refused" errors typically associated with IP based blocking, and three instances of "Socket connection" errors typical to network time outs (which can be associated with filtering). However, the results were inconclusive as they could have been the result of problems on the server, or high network latency. (During this period the ONI was not testing for latency on the network). Moreover, ONI testing also indicted that these sites were accessible from the ISP Belinfonet, suggesting that if this were an attempt at filtering, it was not comprehensive.

---

37 http://www.e-belarus.org/news/200603021.html

38 http://community.livejournal.com/by/386690.html?thread=2673026#t2673026; http://bybanner.com/show.php3?id=1706; and, http://active.by/company/press/news/2006/02/23/21.html

39 http://bybanner.com/show.php3?id=1814. See Annex C and D for description of sites.

5) **18 March, 23:00: User forums on the popular site Tut.by are reported to have ceased functioning.** Unverified reports in the Belarus "technical press" reported that access to the forums on Tut.by, a popular forum site with over 20,000 subscribers had failed. The report claimed that users received an error indicating that the desired forum was not working, and to "repeat their request in a few minutes."[40] In an e-mail exchange with ONI researchers, Tut.by CEO Kirill Voloshin, stated TUT.by had not experienced any problems before, during or after the elections. It is perhaps of interest to note, however, that other sources told ONI that Tut.by was no longer a completely "independent" site, as it had earlier yielded to government pressure to monitor and censor its forum discussions for inappropriate political content (see discussion in Part 3 below).

Election day reports and testing (19th March, 2006)

1) **Numerous opposition and independent media sites are reported as "blocked."[41]** Opposition groups reported that the authorities were "blocking" access to political and news sites. Two rounds of ONI testing on 19 March found that 37 of the 197 "high impact" sites -- mostly opposition and independent media sites -- were inaccessible from the Beltelecom network in Minsk, even though they were accessible from the control location. (see Figure 2).

2) **Hacking reported against main opposition websites, and that of the main opposition candidate.** [42]

   1. www.milikevich.org – Opposition media sources reported that the site had come under a denial of service attack.[43] ONI tests indicate that the site was "dead" from 17:45 on 19 March until 11:45 on 20 March, 2006 -- inaccessible from both of our testing locations in Belarus as well as our control location.

   2. www.charter97.org – Belarus sources reported that outages experienced by this site were a result of various forms of electronic attack (DoS and hacking).[44] On 19 March ONI tests revealed a mixed picture. Testing from Belinfonet showed erratic levels of accessibility throughout the day. Three connections from Belinfonet to the site returned "inaccessible" errors, while connections made at the same time from our control location showed the site as accessible. On average the site was 66% accessible from Belinfonet. However, testing from Beltelecom found the site to be fully accessible. Follow-up testing found that the domain charter97.org resolves to two distinct IP addresses. One of these IP addresses behaved erratically and was inaccessible at times. This means that users whose nameserver resolved to the affected IP address found that the site failed to load, or loaded only partially (this is consistent with what users in Minsk reported). This may also explain why ONI tests showed the site as mostly accessible, while some users reported difficulties in accessing the site.

40 http://bybanner.com/show.php3?id=1815

41 http://naviny.by/ru/content/rubriki/2-ya_gruppa/kompyuter/19-03-06-1/; and, http://www.e-belarus.org/news/200603201.html

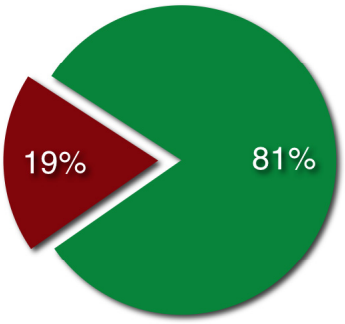
42 http://www.e-belarus.org/news/200603201.html

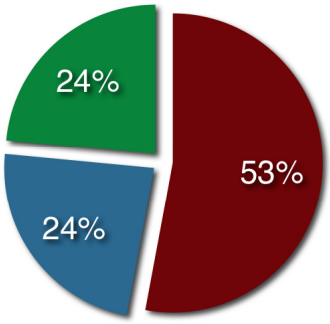
43 http://bybanner.com/show.php3?id=1816

44 http://bybanner.com/show.php3?id=1816

Figure 2. Results of testing 10 March 2006 (Election Day)

On 19 March, 2006, ONI testing revealed errors in accessing 19% (37 of 197 sites) on our "high impact list" from the Beltelecom Network. These errors affected access from Beltelecom only; all sites (except for two*) remained accessible from Belinfonet. The sites were also accessible from our control location.

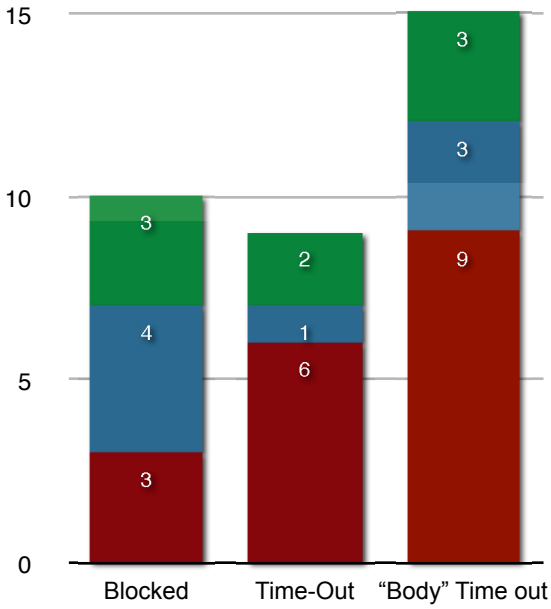




Of the 19% inaccessible from Beltelecom, 53% were sites belonging to opposition political parties (or movements), 24% were independent media sites, and 24% included blog sites and other informational content sites.

- Opposition Political Parties or Movements
- Independent media
- Other (inlcuding blogs, religious and gay sites)

Our tests recorded three distinct types of error messages: "Blocked" - indicating a connection was refused; "Socket time out" - indicating that a connection to the site could not be made as the maximum amount of time allowed to make a connection was exceeded; and, "Error reading body" -- where we connected to the site, but the body (or content) failed to load due to the connection timing out.



* The two sites concerned were charter97.or and milinkevich.org. Charter97.org was partially accessible (possibly due to a DoS attack); milinkevich.org was "dead" (reportedly hacked).

Post-election Testing (20-25 March, 2006)

1) **21-22 March: www.milikevich.org experiences irregular access**. ONI testing revealed erratic access to the milikevich.org website on 21-22 March. On the 21st, the site showed only 50% of requests as successful from ONI's in-county and control testing locations. By mid-day on the 22nd the site was fully accessible. The results may indicate the site was under a DoS attack. However, ONI was unable to access sever log files and therefore cannot confirm that this was the case (see discussion below).

2) **22-25 March: some websites continue to experience irregular access, returning error messages consistent to those found in instances of "blocking."** Between 22 and 25 March, some five sites from our high impact list continued to return a variety of unusual access errors, which could have been indicative of blocking. However, the low number of affected sites suggests that factors other than blocking may have been responsible for the observed faults. In one case (unibel.by) the errors were caused by a misconfigured nameserver on the Beltelecom network (see discussion below).

3) **23-24 March: forum site for charter97.org returned anomalous "inaccessible" errors.** Two rounds of testing by ONI on the 23 March (from Beltelecom) returned "inaccessible" errors. A further seven tests on the 24th yielded the same result. The types of error received, (http 502, and 503), as well as the patterns observed, suggests that these errors were due to problems with the server rather than the result of attempted blocking.

4) **25 March: dial-up Internet services in Minsk fails**. On 25 March, the Belarus-based Financial News Agency reported that the Minsk telephone network "turned off "access to Beltelecom's free dial-up Internet services.[45] Beltelecom's webage announced that the problems were due to a technical failure. ONI contacted Minsk telephone help desk staff who likewise blamed the outage on a technical fault. The "outage" affected Minsk telephone dial-up numbers only. It was still possible to connect by calling the main Beltelecom access numbers (ie , not through Minsk Telephone). The timing of this error coincided with the day riot police broke up demonstrations in Minsk, ending the opposition's week-long protest against the results of the elections. It was also the second time that "access" issues affected the Beltelecom network in the week following the elections. (The first being the inaccessibility of 37 sites on 19 March)

5) **24-25 March: the on-line news paper BGD returned "connection refused" errors for on Belinfonet.** ONI testing on the evening of 24 March, and all day 25 March returned a "connection refused" error, which was consistent with IP blocking. The site remained accessible from our control location. ONI did not test for accessibility from the Betelecom network as access in Minsk was "down" for most of the day.

Tampering with nameservers

As noted in Part 1, during previous elections several Belarus' sources made strong allegations that authorities were tampering with the local nameservers of opposition and independent media sites

45 http://afn.by/news/default.asp?newsid=72596#data

(rendering them inaccessible). During the 2006 election period, ONI investigations revealed only two cases of DNS irregularities affecting the domains of our "high impact" websites. The first case involved two domains hosting NGOs sites -- home.by and NGO.by -- which returned results from the primary nameservers that indicated the domains had been deregistered. ONI researchers confirmed that both sites had been removed by their owners prior to the elections, but for different reasons.[46]

The second case occurred four days after the elections (24 March) and affected access to sites located within the unibel.by domain for subscribers of the Beltelecom network. Unibel, a Belarus ISP that services the educational community, maintains one of its two nameservers at Beltelcom (srv.bsf.minsk.by). On the 24th, this nameserver stopped processing requests for the unibel.by domain for all subscribers using the Beltelecom nameserver. This affected all subscribers in Minsk, and may have also affected other Beltelecom subscribers throughout the country. The second nameserver, ns.unibel.by (195.50.0.161) located on the Unibel network, continued to operate normally, and any subscriber (including those in Belarus) using the unibel nameserver directly[47] would have been able to access the sites. As a result, while the domain was inaccessible from our Belarus testing locations, it remained fully accessible from our control location. The error affecting the Beltelecom-based nameserver may have been caused by misconfiguration. However, the error was suspect because the affected namesever continued to process requests for other domains correctly – only the unibel.by domain failed to resolve properly. The Unibel domain hosts the domain bhc.unibel.by which is the site of the Belarus Helsinki Committee, a human rights group critical of the Lukashenka government. However, it should be noted that this site has not been updated since November 2005, and thus was not a conduit for active information during the current election period.

Did the government tamper with the Internet?

ONI testing did not yield conclusive proof that the authorities engaged in systematic and comprehensive filtering, or tampering with the domain names, of opposition and independent media websites using known or previously documented techniques during the 2006 election period. However, ONI testing did return evidence of inaccessible or partially disabled sites on certain days at certain times from certain locations. Follow-up testing and investigation cannot rule out the possibility that some Internet tampering took place during the election period.

Of the main results reported above, the most suspicious are:

- 37 of 197 opposition and media websites being monitored were inaccessible from the Beltelecom network on 19 March (election day), although they were accessible from the Belinfonet;
- the Internet was inaccessible to subscribers using Minsk Telephone access numbers on March 25 (the day of a major demonstration,when riot police were used to disperse and arrest protesters);
- the website of the main opposition candidate Aleksandr Milinkevich was “dead” on 19 March and experienced problems on the 21-22, (the post-election protest period); and,
- the opposition website Charter 97 was only partially accessible between 19 to 25 March.

---

46 The two domains were associated with a United Nations Development Programme (UNDP) sponsored project – Internet2 – which was formally closed at the end of 2005. In the case of home.by,, UNDP, decided to shut it down due to outdated content. In the case of NGO.by, the sponsoring organization (United Way Belarus) was unable to register as a local NGO, and as a result was unable to financially support the operation of its service. The inability of United Way Belarus to register as an NGO points to the broader mechanism the authorities are employing to silence critical civil society voices (as noted in Part 1 above).

47 Meaning, those users whose ISP's recursive chose the unibel nameserver. An ISP provided recursive nameserver will choose randomly between the minsk.by and unibel.by nameserver, but stick with this choice for some time.

The 37 sites--partially filtered

ONI evidence, in combination with user field reports, suggests that the 37 "inaccessible" oppositional and news sites were partially filtered on 19 March. We say "partial" because the 37 sites remained accessible from the Belinfonet network inside Belarus on the 19th, meaning that any filtering that may have taken place was only partial in effect.[48] At present, ONI does not have sufficient knowledge of the technical configuration of Belinfonet to explain why this was the case. Some sources suggest that the owners of Belinfonet are well connected, and hence its satellite-based downlink is not routed through the Beltelecom network, which would insulate it from a filter placed on Beltelecom's central server. Certainly ONI tests seem to support this hypothesis, as even the Russian gay sites officially banned by the Belarus government are accessible via Belinfonet.[49]

And yet the confirmed problems with the 37 sites on the Beltelecom network do not yield an iron-clad case for filtering. One could argue that the sites' problems were due to technical faults, such as excessive server loads that caused failures or timeouts; or that some combination of intermittent network problems and sever loads combined to create local conditions on Beltelecom which made these sites inaccessible in a random and unpredictable manner, while giving the appearance of being blocked to users in Minsk. While ONI testing was not robust enough to rule out these possibilities, the counter-evidence in favour of partial filtering is four-fold:

- the analysis of message headers revealed returns consistent with those found in cases of filtering;
- the servers for the affected sites remained accessible for our test runs from Belinfonet and the ONI control collocations, meaning that the servers did not appear to be unduly overloaded and were behaving normally when dealing with requests;
- the inaccessible sites were distributed across 25 different ISPs, making it highly unlikely that the problems could have been caused by 25 simultaneous technical faults (See Annex E);
- our users in Minsk reported that the opposition websites were only partially loading, while other Internet websites (including others on our high impact list) loaded without any difficulty. This latter evidence rules out the possibility that the 37 sites sites were inaccessible due to network congestion alone. Indeed, ONI measurements of network latency on Beltelecom during that day indicated a significant packet loss -- but this problem would have affected all sites, not just the 37 that were experiencing the consistent and sustained problems.

On 30 March a senior Beltelecom official responsible for network services, stated publicly that the network did not experience any irregularities before, during or after the elections, nor that Beltelecom filtered access to opposition sites.[50] If taken at face value, the first assertion denies that access errors were caused by heavily congested channels, while the second denies filtering. Given ONI test results and verified user reports from Minsk that prove accessibility problems for some sites from the Beltelecom network, both statements cannot be true. Taking all evidence under consideration, it would seem that the 37 sites may well have been partially filtered by way of the Beltelecom network.

---

48 Only one site was inaccessible from Belinfonet (www.belarusy.com), and this site was accessible from the Beltelecom network.

49 ONI sources in Minsk indicate that the management of Belinfonet is protected through its connection with the KGB and the Presidential Administration, which grants it a special concession. While this is impossible to verify at this time, ONI has observed similar arguments in other CIS countries, where exemptions are provided to favored companies. In Uzbekistan, for example, despite a systematic approach to Internet filtering, a "favored ISP" is allowed to carry political and pornographic content that is banned on all other ISPs. (See, ONI Uzbekistan Study, forthcoming, 2007).

50 Yuri Galyakevich, the senior Beltelecom official responsible for the network services publicly denied allegations that Beltelecom filtered opposition sites on 19 March, or that the network suffered from technical problems (see, http://naviny.by/ru/content/rubriki/2-ya_gruppa/kompyuter/30-03-06-1/).

The Minsk outage

The technical failure which affected Internet access for users of free dial-service through the Minsk Telephone Company was suspicious, as the service is the primary means of free access to the Internet for citizens of Minsk and the failure coincided with the day that riot police cleared away a major opposition demonstration (25 March). However, Internet access was not cut off completely. Users in Minsk could still connect to the free service if they called Beltelecom numbers directly. Other service providers, including Belinfonet remained open and accessible and did not report any access issues. Our tests on Belinfonet for 25 March show almost all sites on the high impact list were accessible.

The "dead" websites

ONI confirmed that there were significant problems with two major opposition sites on certain dates: the website of the main opposition candidate Aleksandr Milinkevich was "dead" on 19 March (election day), with additional access problems later; and the Charter 97 site was also experiencing significant verifiable problems on one of its IP addresses. The observed problems of both sites could be indicative of a DoS attack, as the site owners claimed. However, the problems could have been caused by high demand or a misconfiguration of the webserver located on the particular IP address.[51] The only way ONI can confirm a DoS attack is through analysis of the server log files. However, ONI was unable to obtain copies of the log files for analysis, despite a number of requests to the website owners and one of the hosting companies in the United States.[52]

Overall, the fact remains that both the Milinkevich and Charter 97 sites were down or disrupted during the election day and after. This is suggestive of deliberate action, even if ONI is not in a position to prove by whom, and in what manner.

So what can we say for sure?

ONI evidence does not confirm that the regime was engaged in systematic and comprehensive filtering of independent websites during the election period. The results imply that the opposition reports of extensive and outright filtering during the elections are likely overstated. Websites that were down on the Beltelecom network remained accessible from the Belinfonet ISP. At the very least, this suggests the absence of a centrally enforced filtering regime, and casts doubt on newspaper reports that Belarus has benefited from Chinese technical assistance and has implemented a comprehensive "filtering system"(See Part 1 above).

At the same time, ONI found suspicious irregularities that affected access to opposition and independent media websites before, during and after the elections, although the level of interference was erratic. The testing was unable to prove – conclusively – that the regime was behind these anomalies, although the problems centering on the state-owned Beltelecom network are unlikely to have been simply coincidental. In part, this ambiguity reflects weaknesses within the ONI testing methodology

[51] For example, a maximum transmission unit (MTU) problem. This occurs when a server's MTU is set higher than the connection allows and the Internet Control Messaging Protocol (ICMP) messages that signal this error are blocked, making a timeout during loading of the body likely.

[52] Note that website owners are often reluctant to share access to their logfiles. Amongst other reasons, the files could endanger the privacy and security of their website users if they fell into the wrong hands. See Part 4.

which is not yet well adapted to dealing with filtering that may be irregular or sporadic.[53]. We return to these issues in Part 4.

Overall, ONI can confirm that any regime-directed tampering which took place was fairly subtle, causing disruptions to access, but never completely turning off the alternative information tap. This does present a puzzle: Given the authorities' intolerance for oppositional and critical information, and given their technical capabilities for filtering the Net, why did they not do so?

53 ONI testing depends on statistical methods, which allow us to average results, and verify patterns. This means repeating testing over an extended period of time in order to minimize the impact of anomalous results. As a result, the smaller the sample, as in cases where filtering may be irregular, the less accurate ONI methods become.

Part 3. And so? Is the Internet under threat in Belarus?

ONI monitoring of the Internet in Belarus revealed three things. First, the Internet was the only information-rich mass media channel that was largely unfettered during the 2006 election period.[54] Second, independent voices, including the political opposition, were actively leveraging the Internet, sporting web-sites for independent news and analysis, the main oppositional candidates, critical commentary including the banned speeches of political opposition leaders, and close coverage of the post-election demonstrations. Third, despite vociferous accusations that Belarus' websites were "taken down,"[55] ONI investigation showed that the regime did not engage in comprehensive tactics to blockade offending web-sites, although it may have "squeezed" the Internet pipe to make certain web-sites more difficult to access for a couple of days or at certain times from within Belarus. Any regime-directed tampering that took place during the election period was fairly subtle, and never resulted in the complete turning off of the alternative information tap.

And yet, as noted in Part 1 of this report, the state has the technical capacity to constrict and even shut down the Internet to users within Belarus because all ISPs must flow through the state-owned Beltelecom, which has exclusive rights to external connections (see Box 4 above). As such, the regime's relatively "light hand" on the Internet tap during the election period may seem somewhat at odds with its concerted efforts to suppress all other independent or oppositional informational space in Belarus. So why was the Internet relatively untouched?

Not now, darling. We've got company

There are four plausible answers. First, it could be that Lukashenka simply didn't consider the Internet to be much of a threat in early 2006. After all, the Internet reaches less than 20% of the population in Belarus. And certainly, its incendiary messages were not reaching the vast majority of "unplugged" rural voters who are also Lukashenka's main constituency and would likely have guaranteed his victory even if the elections had been free of irregularities. Second, given the Internet's limited "threat," why mess with it when all eyes are on Belarus? Better perhaps to let it be, to deal with it later in a more measured and effective manner after the foreign correspondents have gone home. Third, why shut down a great source of intelligence? By letting those oppositional packets flow, any number of the regime's security organs may have been collecting intelligence on just whom to pressure next, by way of Internet monitoring and surveillance. The Ministry of the Interior, has proven its capability to monitor and track down users of cyperspace in its effective fight against cybercriminals. (See Box 5 below). And just prior to the elections, the Interior Minister (Uladzimer Navumau) signaled his intention to uphold the December 2005 changes to the Criminal Code that outlaw the "discrediting of Belarus": "*Recently there are more incidents of dissemination on the Internet of patently false information, which in fact is aimed at*

54 As noted in Part 1, newspapers, radio and television are effectively gagged inside Belarus, with only those servicing the regime in operation. Cellphones were also used during the elections, to send out mass SMS text messages to both support and intimidate the opposition.

55 See, for example, Timothy Garton Ash, 2006. *Spinning Belarus: Can hyping a peoples' 'revolution' in Minsk make it so?* Los Angeles Times, March 23.

discrediting the state. Thanks to this law we [police] will be able to prosecute those who place this information."[56]

Fourth, ONI researchers on the ground suspect that the regime's own hyper-legalism may have tempered its comprehensive filtering of websites. These insiders note that the formal legal architecture for regime blocking of the Internet – which would allow the regime to require all ISPs to also block – is not formally in place... yet.[57]

Just like the others

In fact, Internet-related legislation is poised to thicken in Belarus, pending the anticipated adoption of amendments to the 1994 Law on the Press and Other Media (See Table 2 below). These amendments promise to classify the Internet as a "mass media outlet," rendering it subject to the same regulations that have effectively gagged the traditional media in Belarus.

The draft bill establishes, among other things, the obligatory registration of websites, and possibly other forms of Internet communication, if they fall under the bill's notion of "network media," which seems likely. As for the regular media, registration will not be a "right" but a "privilege," which is granted provided state prerogatives on content are followed. Likewise, if a website is located on a "foreign" server outside of Belarus, the website must conform to national legislation on content and also acquire a license (in much the same way that foreign newspapers require state sanction). Any website that violates content or licensing requirements will be rendered "illegitimate" within Belarus, which would then give the regime the legal right to shut it down. Under such a scenario, "blocking" would become fully legalized, and the regime can also legally demand that all ISPs follow suit.[58]

Box 5. State eyes on the Net

The 1994 Belarus' Constitution guarantees the privacy of personal communications. However, other laws override these rights (See Table 1, and Annex A). A 1999 law allows for the interception of traffic to track "criminal" suspects, and to prevent "cybercrimes" or threats to national security. The Ministry of Internal Affairs has demonstrated its prowess for intercepting and analyzing Internet traffic in the fight against cybercrime. For the past five years, its "Department K," has scored impressive victories in tracking down hackers, cracking Internet-based credit-card scams, and helping Interpol break the world's biggest child pornography network, which involved extensive money-laundering operations on Belarus soil. As noted in the text, the Minister now intends to enforce new changes to the Criminal Code by going after all those who "discredit the state of Belarus."

A 1997 law vastly expanded the KGB's authority to acquire all forms of information from any state or non-state body, including unfettered access to databases and information systems. The law also requires ISPs to install equipment that will shunt traffic flow directly to the KGB for real time processing, in a way similar to that which is done in Russia by SORM.** ISP owners have declared that they do not have such equipment installed. However, allegedly there is an unofficial request that ISPs store all monthly logs, in case law enforcement bodies demand them.

** In Russia, SORM legislation or "System of Ensuring Investigative Activity" requires ISPs to install a "black box" rerouting device that tracks every transaction made over the Net and sends it directly to the secret police (FSB) without users knowing.

---

56 See: I*nterior Minister of Belarus promises to see into a matter of false information on Internet*'; 8 December 2005 on www.charter97.org.

57 Outright blocking of Internet sites by the government could be considered a violation of the constitution. As such, theoretically at least, an ISP could challenge a regime directive to block certain sites. In practice, however, it is likely that most ISPs are too vulnerable to take such an audacious stance. See discussion below.

58 See analysis of advance draft of the Law in *Man and Internet*, 2001. The draft has, in fact, been pending for some time, but observers anticipate that it will finally be tabled soon. As noted, technical blocking of sites is possible because Beltelecom is the central tethering point for Internet access.

But Lukashenka need not be so blatant in order to bring the Internet to heel in Belarus. He has more pervasive and subtle levers to pull, where the focus will be to encourage "self-policing" and "self-censorship" amongst information transmitters, producers and receivers.

ISP Inspection: Father may be watching

As in all good police states, it is best to share the burden for maintaining the integrity of the Republic. With respect to Internet content, ISPs are well-placed to help with the task, if sufficiently motivated. In Belarus, ISP motivation is helped along by way of "inspections" mounted by the State Inspectorate on Telecommunications (BelGIE). The stated legal purpose of BelGIE inspections is to ensure that all equipment is properly certified, operating in compliance with the license requirements, and in satisfactory working order. Any violations can result in fines, disconnection from Beltelecom, or a revoking of the operator's license. According to insider observers, ISPs are "terrified" of BelGIE inspections, mainly because the legal parameters of work for ISPs are not clearly specified by the Ministry of Communications. This means that BelGIE has a wide degree of interpretive latitude for finding "violations."[59] There have already been accusations in Belarus that ISPs have come under pressure to monitor Internet content, and that some have aided and abetted filtering on behalf of the regime (See, for example, Box 5 above).

The spider and his flies

Another effective means for closing down the Net's informational space is through pressure on web-site administrators, moderators and posters. A series of incidents over the past year suggests that this tactic is on the rise:

In March 2005 a popular Internet forum (forum.grodno.by) hosted on a local Beltelecom platform, which was home to discussions about President Lukashenka's policies and the upcoming parliamentary elections, was suddenly closed. The system administrator, Alexei Rads, was forced to resign albeit "at his own wish."[60]

In April 2005, the largest Belarus portal www.tut.by introduced compulsory registration for its 20,000 forum users. The administrators informed forum users that all discussions must comply with Criminal Code regulations, and in particular, those that prohibit "slander of the President."[61] Forum moderators are responsible for checking political discussions (allegedly at the request of the authorities), and the forum pages feature citations from the applicable parts of the Criminal Code.

In August 2005, the Minsk office of the US International Research and Exchange Board (IREX-Promedia) was de-registered and thereby closed. IREX had been providing free access to the Internet, and hosted the websites of some 30 independent newspapers, as well as extensive media archives. The legal basis for closing the office was found in the charge of "irregular" activities.

In August 2005, an "honor and dignity" criminal suit was filed against two students, Alexei Obozov and Pavel Morozov, for posting cartoons about the President on the Internet site "Multclub" (http://mult.

59 This is all the moreso because a fair few ISPs, frustrated by unduly long waits to receive certification for equipment like WIFI or ASDL, simply go ahead and buy uncertified equipment. These ISPs are automatically vulnerable to BelGIE sanctions, should the Government choose to do a targeted inspection.

60 Belnet, 11.3.2005. See also Pazdnhak, 2005. *A one-window democracy? The shaping of e-Government in Belarus*, Wider Europe Review, Vol.2,No.1. Retrieved from http://review.w-europe.org/4/4.html

61 Belnet 23.6.2005. See also Pazdnyak, 2004. *Democracy and foreign policy: Belarusian intersections*,Wider Europe Review. Retrieved from http://review.w-europe.org/3/2.html

3dway.org). The KGB searched their apartments and seized all computer-related equipment. On 17 August, access to information on the 'Multclub' site was allegedly blocked.[62] This case has not yet gone to trial, but if it does no doubt it will serve as an example to others.

In April 2006, a "flash-mob" political demonstration was announced over the Internet, with participants to gather in downtown Minsk. The 12 young people who gathered in response were promptly arrested by the waiting policemen.[63]

As the regime turns its gaze more closely to Internet content, pressures on administrators, moderators and posters will likely increase, in lock-step with enhanced regime surveillance.

In sum, closer analysis of the political and legal context suggests that the Belarus' regime has both the will and capability to clamp down on Internet openness, and that its capacities to do so are more pervasive and subtle than outright filtering and blocking. The regime has well-honed means for encouraging "self-censorship" amongst its citizens. It is also poised to thicken the legal architecture that will enable more active state monitoring and blocking of the Net, while bringing Internet content under the same strictures that have stifled the traditional media in Belarus.

Table 1. Legal groundwork for control of the Internet: Legislation in force

Type of Law	Full Title	Significance for Internet Openness
Government Regulation № 551 (16.08.1993)	On the Concept of Communication Development in the Republic of Belarus	Enshrined State Monopoly over External Communication Channels
Constitution of the Republic of Belarus (30.03.1994; amended 24.11.1996)	Constitution of the Republic of Belarus	1996 amendments empowered the President to issue Decrees that override all other legislation, and eliminated the separation of state powers and judicial independence. The 1994 Constitution was considered by international experts to be thoroughly "democratic." Among other things it established freedom of access to, and distribution of, information, as well as the right to personal privacy and inviolability of personal data.
Regulations № 427 (27.06.1996) AND No. 215 of the Ministry of Communication (14.11.1997)	On the State Supervision Of Telecommunication in the Republic of Belarus AND Statute on the Order of the Control over the Building and Condition of Telecommunication Networks which have Access to the Communication Network of Common Use	Empowered the State Inspectorate on Telecommunication (BelGIE) to inspect telecommunications providers –including ISPs -- and issue fines or revoke licenses if anomalies are found. The stated inspection purpose is to ensure all equipment and activities are properly licensed, certified and operational. In practice, however, BelGIE inspections can be used as a form of intimidation or punishment against "unreliable operators," meaning those who allow activities/information that may threaten the regime.
Law of the Republic of Belarus (03.12.1997)	On State Security Bodies of the Republic of Belarus	Vastly expanded KGB authority to violate individual privacy through wire-tapping and other forms of communication interception and monitoring. The law covers all forms of communication, and so applies to the Internet.

62 Belnet, 17.8.2005. Apparently, access to several other sites hosted on the webserver were blocked as well: '3d Way' movement site http://kniga.3dway.org;; Limon project http://limon.3dway.org; Gomel youth center 'Gart' http://hart.3dway.org; Information page http://gazeta.3dway.org; Project 'For Ours' http://za.nashih.org; Project StudGomel.Com http://studgomel.3dway.org.

63 Source: RFE/RL Newsline Vol 10:69, Part II April 2006.

Law of the Republic of Belarus (09.07.1999)	On Retrieval Activity (Intercepting and monitoring)	Expanded authority for state-interception and monitoring of private correspondence (including electronic). The Ministry of the Interior has used this law to combat a wide array of cybercrimes including hacking, money laundering, child pornography and credit card fraud. There are fears however, that the state's proven capabilities for interception and monitoring of Internet traffic maybe used to crack down on the political use of the Internet in the future.
Amendments to the Criminal Code of the Republic of Belarus (08.12.2005)	Amendments to the Criminal Code	Among other things, establishes criminal liability for any activities that "Discredit the Republic of Belarus". Following the law's release, the Minister of the Interior noted that the Internet carries considerable false information that "discredits Belarus" and that now his ministry can "prosecute" the perpetrators; (Note this is the same Ministry that deals with cybercrime through effective Internet surveillance).

Table 2. Legal groundwork for control of the Internet: Pending legislation

Type of Law	Full Title	Significance for Internet Openness
Not yet tabled: update to the Law of the Republic of Belarus (13.01.1995)	*Press and Other Mass Media*	The new draft law will include the Internet, and will likely impose significant regulations and restrictions on website owners. The new draft law will likely classify the Internet as a "mass media outlet" thereby subjecting it to the existing legal framework that has effectively gagged traditional media in Belarus. The new law could require all websites to officially register with the authorities, thereby outlawing any unregistered foreign websites (in the same way the foreign press is treated). Any site not officially registered could be subject to "blocking" by Beltelecom (which controls the Internet connections in Belarus). All sites that register will be subject to content laws, including the expanded criminal code which prohibits the "discrediting of the Republic."
Not yet tabled	*On Fundamentals of Information Security*	This draft law, which is not yet available publicly, is expected to enact even stronger controls over information content and distribution, including information on the Internet.

Part Four. Summary: Wither Belarus?

This ONI Internet Watch has shown that the Belarus regime has the technical capability to filter and block the Internet. However, ONI testing during the 2006 election period did not yield conclusive proof that the regime chose to fully exercise this capability. ONI confirmed that some 37 important political and independent news websites experienced access problems at certain times, and also found other suspicious access anomalies.

ONI was unable to verify unequivocally whether the confirmed Internet problems were due to deliberate regime interference, although the problems centering on the Beltelecom network are highly suspicious. The one firm conclusion is that any regime filtering or interference that took place was neither comprehensive nor systematic. Websites on the Internet may have been "squeezed" at times, but were never under full blockade.

This report, however, does not argue that Internet openness in Belarus is robust and guaranteed. Rather, analysis of the political and legal context revealed that the regime has both the will and capability to clamp down on Internet openness, and that its capacities to do so are more pervasive and subtle than outright filtering and blocking, with growing pressures for self-censorship. Regime surveillance of the Net's informational space is likely to grow as more independent and oppositional voices take to the web to organize and get their message out, as the 2006 elections showed.

When it comes to outright Internet filtering, the formal legal architecture that would enable the state to lawfully block and filter Internet sites is not yet fully in place. Perhaps this explains why the regime, always careful to have a legal basis to pursue its actions, has not pursued overt and sustained political filtering to date. But there are new laws in the works which promise to bring websites and website content into the same regulatory framework that have been used to effectively stifle the traditional media in Belarus – both domestic and foreign. As such, the day may be approaching when Belarus' cyberspace will be legally and overtly restricted and monitored, with any potentially offending sites being blocked outright. And in the meantime, the precedent has been set to apprehend and prosecute those who choose to slander the President or his regime in cyberspace.

Part Five. The Internet election challenge: Perspective and recommendations

Monitoring Internet openness during elections: A slippery challenge

This report marks the second occasion ONI has examined the openness of the Internet during national elections. In both cases -- during the 2005 Kyrgyz parliamentary elections and the 2006 Belarus presidential elections -- we found evidence that the Internet was becoming part of the electoral campaign and that civic and political groups were expressing increasing concerns about Internet openness. In neither case did we find black-and-white cases of deliberate filtering using standard techniques, such as those employed by China, Iran and Saudi Arabia. We did, however, find "greyer" evidence that suggested more subtle, less attributable techniques were at play, such as DoS attacks to take out certain websites at critical times. These initial findings suggest we may be looking at the start of a pattern of "below-the-parapet" Internet tampering during elections in democratically-challenged countries.

Arguably, a preference for subtle pressure on the Net may stem from the nature of elections themselves. Any government -- no matter how authoritarian -- that decides an election is needed to renew claims of legitimacy, risks losing that legitimacy if its attempts to "shape" the outcome are too obvious or heavy handed. Thus, Chinese-style "filtering out" to eliminate access to legitimate opposition parties in their entirety would be immediately obvious, and the finger of blame easy to point at the state.

We can also speculate that indirect methods (such as DoS attacks, hacking, or simply allegations thereof) are preferred because of their effectiveness. In elections, timing matters. Tampering with access to political websites or alternative news sources need not be long-lasting or comprehensive. Sites need not be blocked for weeks. All that is really required is a well-targeted disruption, to reduce or "confuse" message flows at a critical time -- say before a rally or after a major government announcement or on voting day when last minute information could play a role in changing how people vote.

Indirect filtering is also hard to prove, which makes it attractive in a politically charged environment. Interruption of Internet services that occurs during an election period is often viewed with more suspicion than disruptions at other times. These suspicions – combined with the potential political advantage that could be gained by levelling accusations of "censorship" against one's opponents – can make it difficult to distinguish between alleged cases of censorship, and actual verifiable cases. In these circumstances indirect techniques can yield valuable political advantage to whomever can "spin" and defend their story more effectively. Governments can interfere and interrupt opposition groups at critical times while retaining "plausible deniability." Similarly, opposition groups can claim government interference, regardless of whether they have evidence to support these claims.

Overall, it is fair to suppose that the "openness" of the Internet is likely to come under increasingly indirect and sophisticated forms of information control during election periods, with methods that squeeze access rather than filter content, and which mimic network timeouts or other plausible errors.

All of this makes monitoring the Internet during elections especially difficult, and fraught with methodological challenges. Passive testing techniques that rely on header returns and are used by ONI to test for the presence and absence of "filtering" are simply not sufficient to detect and verify indirect

methods and techniques. As noted in Part 2, proving that sites have been hacked or subject to DoS attacks, for example, requires access to server log files, which can only be obtained from the website owners or hosting services. Even then, in the case of sophisticated techniques, other more specialized tests would be necessary to positively identify that a server was under a DoS attack. Besides, website owners are justifiably reluctant to share logfile information, which contains the source address for legitimate users of their websites as well as the "bots" used in DoS attacks. In the wrong hands, this information could be used to identify individual users and lead to harassment or other forms of prosecution. Beyond this, owners of political websites may have other motives for protecting log files from inspection. Thus, allegations of DoS attacks may be as effective as actual attacks, a convenient way to gain political capital out of normally occurring network anomalies or other technical failures. It is better to claim your website is inaccessible due to deliberate hacking, than to admit to poor design or maintenance.

The Internet is fast becoming an important component of the democratic and electoral process. There are signs it may eventually surpass the importance of other mass media as a means for grass roots campaigning. Ignoring the Internet during elections leaves the door open to possible abuses. And yet, monitoring the Internet during elections is a slippery business. It urgently requires the development of new testing methodologies and monitoring capabilities. It is to these issues we now turn.

Recommendations and areas for further investigation

Established election monitoring groups need to be sensitized to the growing importance of the Internet. For this reason, we end this report with two sets of recommendations for: elections monitoring groups; and, civil society or political groups who will be contesting elections in the coming years.

Recommendations for Election Monitoring Groups

1) **Election monitoring should be extended to include the Internet.** Measures of openness and access need to be developed and incorporated into overall assessments of the fairness and transparency of electoral campaigns and outcomes. First and foremost this should include the development of methods and indicators to track the accessibility and "openness" of websites belonging to political parties, independent media, watchdog groups and electoral authorities, throughout the election period.

2) **Appropriate monitoring techniques need to be developed, specifically to investigate allegations of DNS tampering, hacking and DoS attacks in "real time."** Technical testing will need to to encompass a boarder range of network metrics, so as to be able to identify other plausible causes for website failures, and identify and investigate "anomalies" with greater precision and detail. Beyond this, election monitoring missions should include an independent technical investigations team whose task is to examine log files and conduct other tests to determine the veracity of claims that websites have been attacked or otherwise made unavailable. Consideration should be given to setting up an on-line facility where the public can record complaints, and where a "real time" projection showing the status of on-line resources could be found.

For its part, ONI will work to expand its technical methods, while exploring other opportunities and partnerships to refine and implement these two recommendations. However, implementation will be challenging, for the reasons outlined in the discussion above, and will require work on the following:

- Base-lining the importance of the Internet. An overall baseline for the relative importance of the Internet needs to be established as its relevance to the electoral process may vary between countries, depending on its penetration and uptake.
- Jurisdictional issues. Relevant websites are often not located in the country in which an election is being contested. Should websites located outside of a country's jurisdiction be monitored for accessibility during an election period, and under what conditions?
- Whom to include. Should election monitoring extend only to official registered political parties and media, or should unofficial movements, international media as well as civil society groups and individuals also be included? Should monitoring include websites belonging to expatriate or diaspora communities?
- Does the Internet include mobile services? Increasingly the Internet can be accessed through a variety of means, including cell phones, whose growth and penetration in societies is higher than that of PCs. Should access to text messaging, multimedia messaging, GPRS and WAP be included in the monitoring methodology?
- Monitoring interactive services. E-mail, chat rooms, on-line forums and Internet Relay Chat are also important channels for mobilizing supporters and conducting "grassroots" political campaigns. New methods for detecting deliberate interruptions in these services are also necessary.
- Over the horizon issues. New developments and trends in the industry –protocols, routing, services – as well as governance and regulation will prompt new opportunities for indirect informational control. These need to be tracked and assessed for the relevance and impact on election monitoring.

Recommendations for civil society and groups contesting elections

The Internet is fast becoming a strategic informational space, one which until recently has remained largely uncontested. This is changing rapidly. The importance of the Internet to the 'Colour Revolutions" and its increasing penetration world-wide means that is only a matter of time before governments, particularly those with less than transparent agendas recognize the advantages of indirect methods of strangling access to Internet informational resources – as opposed to blunt filtering which unambiguously identifies the perpetrator.

The contested nature of the Internet has become more visible through the US-led "war on terror," which has been stretching global norms to accept the use of "computer network operations" (CNO) as a means for combatting "illegal and terrorist organizations" on a global scale. In 2003, the US Department of Defense's *Information Operations Roadmap*, clearly stated that the US would prepare to "fight in the Net," that is, to unambiguously contest "terrorists" and their supporters in cyberspace, regardless of where they are located. Taken together with the shift in US strategic policy towards preemption of threats "before they are fully formed," this stance has effectively opened the door for states to use CNO as a means to act unilaterally and extraterritorially to combat self-defined threats to national security. As a consequence, CNO and Information Warfare (IW) are amongst the most secretive and fastest growing areas of investment for military, security and signals intelligence organizations worldwide. Moreover, as the recent revelation concerning the US National Security Agency's extralegal tapping of domestic communications (including the Internet) suggest, even open and democratic societies are undertaking covert Internet surveillance. If the United States does not require transparent legal

standards for Internet surveillance, then what are the implications for states with less robust legal cultures and institutions?

It is imperative that civil society groups start to take information security seriously, and prepare to operate in a more contested and less secure informational environment. With respect to elections, it is important to advocate for an open Internet that is accessible to all. Therefore civil society groups should:

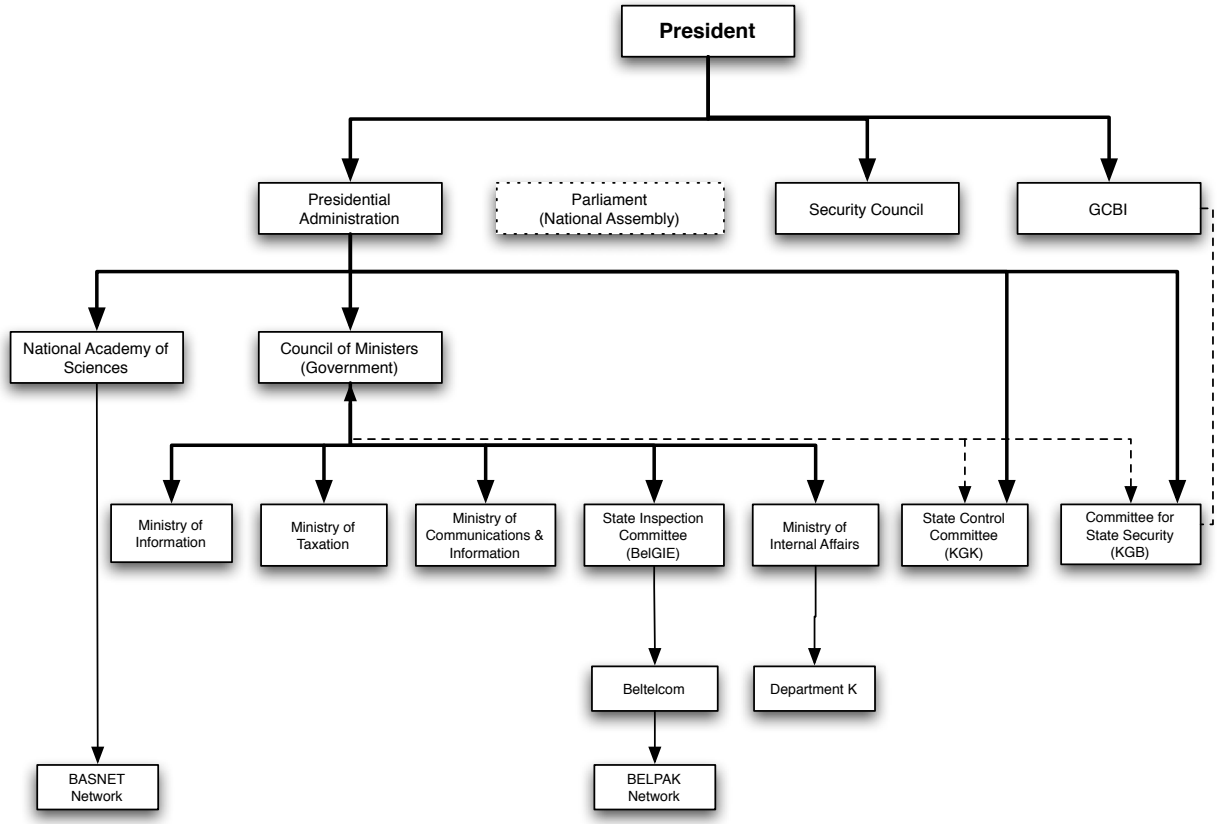
1. **Draw attention to the possibility that the Internet can be tampered with, and ensure / insist that election monitoring groups include the Internet in their assessment of the "free and fair" nature of elections.** Civil society should encourage watchdog groups to put in place a credible system for monitoring the "openness" of the Internet, as well as means to document and verify abuses or restrictions.

2. **Prepare contingency plans for their websites being filtered or otherwise blocked.** This can be accomplished by putting in place a mirroring strategy prior to the elections, distributing copies of sites on multiple servers and domains, as well as using server farms (where one IP address is shared by numerous sites) and virtual hosting. Intelligent firewalls that capture possible attacks should also be used on primary server sites, so as to validate and possibly counteract attempts at hacking or DoS attacks, while still preserving the privacy of site visitors.

3. **Increase training and awareness raising**. Civil society needs to increase its awareness of information security and train to anticipate and react to filtering, hacking and DoS type attacks. Civil society needs to become capable of competing in the "contested" Internet environment.

* * *

Annex A. Belarus' informational sphere: The matrix of control



On paper, Belarus' legal and administrative framework appears democratic. In practice, however, all state bodies and agencies function to service the control of the Presidential Administration.

The above diagram illustrates the stringent top-down nature of control and decision-making in Belarus as it relates to the informational environment, a pattern which is replicated in all other spheres in Belarus. ONI researchers on the ground have pieced together the different components of this "matrix of control" and suggest it has three basic components: political/security, legislative/administrative, and economic. Together this troika works to diversify pressure points on both government administrators and ordinary citizens, to ensure compliance with regime interests while maintaining the illusion of legality:

Political Power and the Secret Police

All key decisions, in all spheres, are made by the President, either in the form of official Decrees or "unofficial" (oral) statements. Statements get passed down the "vertical" levels for elaboration, legitimization and implementation. The legitimization process "from below" – whereby the President's statements are turned into draft legislation, policies or programmes -- is important for maintaining a veneer of regime "legitimacy" and the illusion of democratic functioning. However, the Presidential

Administration (PA) must approve all government decisions, including legislative matters, before they are submitted to the National Assembly. The PA also often intervenes in the activities of ministries and departments by issuing direct instructions.

Presidential power, including control over critical opponents and information, is further buttressed by the KGB and other special security bodies (State Center for Information Security, Ministry of Internal Affairs and Public Prosecutor) who have special investigative functions (invigilation of citizens including monitoring of communications) to "safeguard security" through covert, extralegal, intervention.

KGB

The KGB has a special technical department that investigates crimes related to communications technologies and allegedly engages in covert Computer Network Operations. The Belarus' opposition claims that the KGB has hacked and eliminated opposition web sites (using DoS attacks), but there are no documented evidence of such actions. The KGB has also investigated ICT related crimes, participated in a crackdown against "underground" mobile communication operators, and IP telephony-based office centers, and investigated a case of "on-line Hooliganism," allegedly perpetrated by the Belarus People's Liberation Army (which is thought to be a non-existent organization).

State Center for Information Security (GCBI)

The State Center for Information Security (GCBI) used to be part of the KGB but is now directly controlled by the President. The GCBI is roughly equivalent to the US National Security Agency although its focus is domestic rather than international. Among other things, it controls the top level Internet domain (.by), and is therefore in a position to fiddle with the second level DNS records of any website registered in the .by domain, to render them inaccessible. As noted in the main text, the opposition accused the GCBI of such tampering during the 2001 Presidential elections when some of their websites went down. It has also been accused of installing filters at the Beltelecom central Internet exchange.

Ministry of the Interior

Another security-enforcement body – Department K under the Ministry of Internal Affairs – has demonstrated its prowess at intercepting and analyzing Internet traffic, which it has done to successfully fight cybercrime. As the main text of this report notes, the Minister of the Interior has signaled his intent to go after all those who "discredit the state of Belarus" on the Internet (See Part 3 of main text).

Legal and Administrative Control

As noted in the main text, the regime is characterized by a hyper-legalism wherein all actions require a legal pretext and strict regulations govern all forms of activity, most notoriously those dealing with financial regulations. However, it is the President's office that determines where, when and which laws are to be enforced, and illegalities are to be prosecuted. The legislative and administrative bodies (e.g., the National Assembly,[64] Security Council,[65] Council of Ministers,[66] Central Election Commission, Ministries, and Commissions) function to sanction Presidential decisions – either by "proposing"

64 The National Assembly (NA) is controlled by the President, and as of the October 2004 elections, contains no members of the formal or informal political opposition. The NA automatically adopts laws introduced by the Ministries or the PA.

65 The Security Council elaborates the national security policy. The head of the SC is President Lukashenka.

66 Another rubber-stamp institution. The Council of Minister (CM) only approves programs that are proposed or agreed to by the President and the PA.

legislation (based on "suggestions" from the PA) or rubber stamping pre-approved legislation. The subsequent enforcement of legislation is then distributed among relevant ministries according to jurisdiction, but subject to Presidential directives. With respect to the Internet, several administrative bodies "shape" and discipline the ISP sector:

Ministry of Communication and Informatization (MCI).

MCI has a regulatory (licensing, certification, inspection) function over telecommunications services, but is also the dominant telecommunications operator given its ownership of Beltelecom (the state run telecommunications monopoly). As a matter of course, the MCI makes policy based on serving the interests of Beltelecom. For example, Beltelecom enjoys a legally enforced monopoly over all international communication services including the Internet, as all commercial ISPs must rent external channels from it. Beyond this, everything from the use of wireless equipment through to the operation of a Local Area Network (LAN) and videoconferencing requires state permissions and permits.[67] Only Beltelecom is permitted to provide IP Telephony, which it does at high rates for considerable profit.[68] The Beltelecom monopoly serves other important political and financial functions for the regime. For example, its high charges for international calls and ISP leasing of lines yield substantial profits that are used to subsidize the costs for local calls, which expands its monopoly – defacto – over local telecommunications provision as well (as competitors cannot compete). Profits are also used to subsidize the otherwise unsustainable industries, providing livelihoods for the mass of workers who are Lukashenka's main powerbase.

Anyone that uses communications technologies without the required permit – or for "inappropriate" communications -- can be charged with "illegal" activities under the criminal code. The Ministry of Communications has been known to refuse licenses for LANs in apartment buildings. Indeed, in February 2006, the Ministry announced its intention to "liquidate" unregistered domestic computer networks, which are thought to number around 1,300 in Belarus, and provide affordable Internet access to some 45,000 users. Experts commented that the move was motivated by the need to remove threats to Beltelcom's monopoly as well as to de facto cut Internet access for several thousand people.[69]

Finally, because most Internet traffic in Belarus flows through Beltelecom's "hands," it enjoys a significant capacity to monitor or filter Internet traffic, should this be of interest (see discussion in Part 1).

State Inspectorate of Telecommunication (BelGIE)

The State Inspectorate of Telecommunication (BelGIE), acts as the MCI's main oversight body with significant powers to supervise the activity of telecommunication operators (including ISPs) in the areas of network licensing, functioning and facilities, and is empowered to impose fines and initiate license withdrawal (see main text, Part 3).

---

67 Activities liable to licensing are listed in Presidential Decree 1387 "On licensing of separate kinds of activity" (14.07.2003).

68 See also Box 2 in main text.

69 PAP (Polska Agencja Prasowa), 20.2.2006 and Bybanner.com, AFN news agency, Belarusy i Rynok, 20.2.2006. An ADSL connection can range from $95 – $385 per month plus $28 – $70 for every two hours of on-line time. The average monthly salary in Belarus is about 385 USD. Networks that encompass several apartments or the entire building allow for sharing of Internet costs.

Ministry of Information

The Ministry of Information does not yet have formal responsibility for the ICT sphere, however representatives of the Ministry have repeatedly declared the need to filter access to inappropriate Internet resources. The Ministry has elaborated a new draft law "On Media" that seeks to classify the Internet as a "mass media outlet" in order to bring it under the same controls that govern the press, radio and television in Belarus. This could mean measures stemming from the required registration of websites – both domestic and foreign -- through to control over content.

Box 5. Legal control over Internet content

As detailed in Part 3 of the main text, direct political control of the Internet in terms of what websites and content are allowed to be accessed inside Belarus is still in its infancy. Criminal code legislation prohibiting slandering of the President has already been used to charge Internet offenders, and the December 2005 changes to the criminal code (prohibiting discrediting of the state) will also apply to information carried on the Net. Beyond this, pending legislation "On the Media" promises to define the Internet as a "mass media outlet" subjecting to the same highly restrictive set of laws that have effectively stifled the independent "traditional" media in Belarus (e.g., registration of all websites "broadcasting" inside Belarus, content regulations etc).

National Academy of Sciences and BasNet

One other body with independent access to the Internet is the National Academy of Sciences of Belarus whose computer network – BasNet -- has a license for autonomous satellite access. The "independence" of this channel, however, is tempered by the Academy's direct supervision by the Presidential Administration.

Economic and Financial Control

In the early days of Lukashenka's regime, his fight against corruption and the still-entrenched *nomenklatura*, helped to consolidate Presidential control over all aspects of the economy. The formal financial regulative bodies (National Bank, State Customs Committee, Tax Ministry, State Control Committee) have extensive powers to supervise all economic activity and financial transactions in the country. These powers are often used to harass independent entities – from civic groups and organizations, through to newspapers and other information producers -- to pressure them to conform to state directives and ideology. Economic control has yielded numerous critical financial and political benefits for the regime, including:

1) **A proliferation of lucrative state monopolies**, particularly in the telecommunications banking, and gas sectors. The generous income from these enterprises allows the state to "re-invest" in more political goals, such as maintaining non-viable collective farms and industries, which provide stable employment for key constituents.[70] As noted above, the Beltelecom monopoly has additional benefits in terms of controlling Belarus' informational environment.

A maintenance of the balance of power within state structures. Charges of mismanagement, corruption and embezzlement against heads of companies and industries are used to ensure obedience to the President. Frequently, individuals who have built-up some authority within regime structures are accused of corruption, and thereby removed.[71]

---

70 Heritage Foundation, 2005, *Index of Economic Freedom*. The monopolies also close out opportunities for the rise of an independent middle (business) class, which in turn increases the population's financial dependence on state structures.

71 For example, in 2003, the regime arrested some 150 directors of state enterprises and launched 440 lawsuits for large-scale theft and embezzlement against 1,638 individuals. See: The Observatory for the Protection of Human Rights Defenders, 2004. Belarus: The "liquidation" of the independent civil society, No. 388 (April).

2) **The obedience of Small and Medium Businesses,** which are subject to a host of administrative regulations that compel support for the regime. Personal economic pressures in the form of petty fines and taxation, which can be frequently made to disappear with a small donation to the right official, effectively stifle small and medium enterprise – including, independent media. Short suspensions of newspapers are frequently a death sentence as they lose crucial advertising revenue.

3) **The enlistment of big (international business) in the service of state interests**, as financial levers are used to compel independent entities to conform to state interests.

4) Control over civic groups and organizations. In addition to cutting NGOs off from external financial resources the state uses the pretext of 'economic crimes', ranging from tax evasion to irregularities in tax declarations, to pressure NGOs and individual civil actors. These carry substantial penalties, including fines and prison terms.

When it comes to the Internet in particular, financial control of ISPs and telecommunication operators are achieved mostly by way of items number 1, 3, and 5 above, and generally consisting of fine-grained control over all financial operations. The State Control Committee (KGK) is directly responsible for inspecting the economic activities of communication operators. Significantly the KGK is controlled by the Security Council.

Annex B. ONI methodology and test results June 2005--January 2006

General Methods

ONI performs technical testing across multiple levels of access at multiple time intervals. The team analyzes results within the contextual framework of the target state's filtering technology and regulations. To obtain meaningful, accurate results we:

- generate lists of domain names and URLs that have been or are likely to be blocked;
- enumerate ISPs and national routing topography;
- determine the type, location, and behavior of the filtering technology;
- deploy network interrogation and enumeration software at multiple access points; and
- conduct a thorough statistical analysis of results.

Determining which URLs to test is a vital component of ONI research, as it reveals the filtering system's technical capacity and content areas subject to blocking. ONI employs two types of lists:

1. "**High impact" sites**, reported to be blocked or likely to be blocked in the state of concern due to their content (for example, political opposition); and
2. **A "global list,"** containing a control list of manually categorized Web sites reflecting a range of Internet content (for example, news and hacking sites).

To explore Internet filtering, ONI deploys network interrogation devices and applications, which perform the censorship enumeration, at various Internet access levels. These tools download the ONI testing lists and check whether specific URLs and domains are accessible from that point on the network. Interrogation devices are designed to run inside a state (i.e., behind its firewall) to perform specific, sensitive functions with varying degrees of stealth. Similarly, ONI distributes interrogation applications to trusted volunteers who run the software inside the state. For testing, ONI obtains network access at multiple levels through:

- Proxy servers
- Long distance dial-up
- Distributed applications
- Dedicated servers

During initial testing, ONI uses remote computers located in countries that filter. These remote computers are located behind the state's firewalls yet allow access to clients connecting from the wider Internet. ONI attempts to access the URL and domain name lists through these computers to reveal what content is filtered, and how consistently it is blocked. ONI also tests these lists from control locations in non-filtered states. The testing system flags all URLs and domains that are accessible from the control location, but inaccessible from ones inside the target state, as potentially blocked.

General Results Analysis

The standard ONI testing methodology yields results along a graduated scale based upon the HTTP header returns obtained during the testing period.

We classify our results into one of four categories that range from the absence of any filtering through to the unambiguous presence of filtering indicated by a "block page" generated by the filtering software (see ONI Test Result Typology, below). A fifth special category of "dead sites" can either be indicative of sites that are "dead" because they no longer exist or of sites that are not responding because they are under a sustained DoS attack.

In between the clear absence or presence of filtering, are several gradients of returns which require further investigation, but which can also provide conclusive evidence of filtering. In some of these cases, filtering is accomplished though blocking IP addresses on backbone routers; in others, by introducing long "time outs" on requests to specific IP addresses. In both cases, ONI's follow-up methods generally allow us to generate enough evidence to confirm whether "filtering" is taking place. This ONI methodology is robust and proven for detecting the presence of filtering as well as the specific content that is being blocked.

ONI Test Result Typology

- **Not filtered** - URL is accessible from the control location and the in-country testing location.
- **Possible Filtering** - URL is accessible from the control location but inaccessible from the in-country testing location due to a network connection error. This result is inconclusive. The inability to access a URL could be a consequence of network failure, error or failure of ISP name servers, or blocking of IP addresses (for example). Without additional testing the cause of the loss of access cannot be determined with any certainty.
- **Probable Filtering** - URL is accessible from the control location but inaccessible from the in-country testing location, which returned a different HTTP response code. Filtering can usually be identified by http header returns. For example, some filtering systems return a "403 Forbidden" error.
- **Filtered** - URL is accessible from the control location but inaccessible from the in-country testing location and the in-country testing connection returns a block page.
- **"Dead"**- URL is inaccessible through both the local connection and the remote computer. In most cases the URL can be "extinct". However, this can also be indicative of a site which has been taken down" by a "Denial of Service" (DoS) attack.

However, in situations where blocking occurs in a dynamic, high demand environment – such as elections -- elevated user expectations and large traffic volumes can often cause network congestion and failure that renders leads sites "inaccessible". In these cases the effectiveness of the ONI testing protocol declines as error messages are often inconsistent and each case must be investigated to rule out the possibility of either network congestion or other transmission faults (rather than filtering).

Methods Specific to Belarus

To analyze Belarus' Internet filtering system, ONI initially tested three ISPs in Belarus to determine blocking patterns and identify any differences in filtering between providers. We conducted tests between June 2005 and January 2006 from within Belarus on the networks of the ISPs AtlantTelecom, Belinfonet, and Beltelecom. The tests included our global list and a high impact list of sites specific to Belarus.

Results and Analysis for Initial Belarus Testing (June 2005-January 2006)

Summary

In total, ONI tested 624 URLs on each ISP. Results showed minimal filtering; less than 1% of sites tested were inaccessible from the ISPs AtlantTelecom (1 URL), and Beltelecom (2 URLs). None of the sites tested were inaccessible from Belinfonet. The inaccessible sites were Russian gay pornographic sites.

Topics Tested

ONI tested the standardized global list, which contains high-profile Web sites in 31 categories, as well as a list of "high impact" sites selected specifically for testing in Belarus. The high impact list contained sites known or likely to be blocked, or sites that were alleged to have been blocked in Belarus for hosting sensitive content.

Filtering Methods

ONI testing indicated that the blocked sites were being filtered by way of IP address blocking. ISPs were preventing access to the targeted sites (gay porn sites) by configuring their routers to reject requests for the site's IP address. This method blocks access to all web sites hosted on the targeted IP address.

Global List Results

ONI's testing in Belarus included our new global list comprised of 458 sites in 28 categories. All these sites were are accessible from all ISPs.

High-Impact List Results (sites specific for Belarus)

AtlantTelecom and Beltelecom blocked www.gayly.ru. Beltelecom also blocked www.gay.ru.

Annex C. "Inaccessible" websites from the Beltelecom network on 19 March 2006

ONI testing on 19 March 2006 found that 37 of the 197 websites tested were inaccessible when accessed from the Beltelecom network in Belarus but were accessible when connections were made at the same time from the external control location. In addition, all 37 affected websites were accessible from the Belinfonet network (inside Belarus).[72] The tables below offer a breakdown and description of the inaccessible sites, grouped by error type.

Table C.1. "Connection Refused" Errors

A connection refused error suggests a TCP/IP connectivity issue between the requesting computer and the remote server -- either the remote server or a computer on the path between it and the requester has actively refused the connection. This error is indicative of IP-based blocking.[73]

Type of Site	URL	Description of Site
Opposition political party	http://www.ucpb.info/	The official website of the United Civic Party, which offers alternative news, critical commentary of the Belarus regime and links to other opposition sites. The site also lists the Milinkevich supporters who have been detained for "petty hooliganism. The sections on party structure, documents, photo archive, forum and library have been inactive.
Opposition political party	http://www.bsdp.org/	The site of the Belarus Social Democratic Party, containing opposition leader Kozulin's political platform, a video of his address to the public and recent news including a joint statement of the opposition for continued protest against the result of the elections.
Independent media site	http://www.belmarket.by/	The online version of a newspaper, which is also available in paper format. It provides updated independent news on politics, international relations, and economics, among other topics.
Independent media	http://www.bdg.by/	The Belarus Business Gazette, which covers politics, international matters, culture, and economics among other topics. It had a separate section for election coverage. Its archive dates from 1997 and includes special reports such as monitoring of the 2001 elections, and the disappearance of high profile individuals in 2001. The site posted information on how to access news provided by BelaPAN in case the site was blocked during elections. The site has a link to the Fund for Support of the Free Press, which itself hosts a "who's who in Belarus" listing of pubic figures and their biographies
Media site (web portal)	http://www.svaboda2006.org/	A web news portal supporting links to other online news sources on politics and economics.
Opposition movement	http://www.studenty.alternativy.net/	A student site against Lukashenka's regime. It advertised the petition that was collecting signatures to protest the election result.
Independent media	http://www.svaboda.org/	The website of radio station Svaboda (Freedom), the Belarus service of Radio Free Europe/Radio Liberty (RFE/RL), transmitting both current and archived programmes. News is updated several times per hour.
Minority faiths	http://www.islam.by/	An Islamic religious site, with articles and analysis of the Koran etc.
	http://www.mfront.net/	Only the main page is active. I had problems accessing other sections with links provide on the main page (archive, history of the movement, etc.)
Gay	http://www.gay.ru/	Russian site of interest to the homosexual community.

72 Belinfonet had a connection issue with only one site: http://www.belarusy.com/. This site was accessible from Beltelecom throughout the testing period.

73 However, it could also be that the webserver is down or has incorrect information in DNS. This would not be expected from IP blocking (null routing) which would result in a timeout.

Table C2. "Timeout when reading Body" Errors

"Timeout when reading body" errors indicate that although the connection to the site was successful, the content of the site was being transferred so slowly that the connection eventually timed out.

Type of Site	URL	Description of Site
Opposition unity	http://www.belngo.info/	Assembly of Belarus Pro-Democratic NGOs, offering comprehensive news on the results of election, acts of solidarity, links to opposition movements, etc.
Independent media	http://www.belintellectuals.com/	Intellectual society site, providing analysis on current issues, encouraging blogging, etc.
Independent movement	http://www.prizyv2005.alternativy.net/	Youth Initiative site, against the civil war and military resolution of political problems. (does not support Lukashenka)
Opposition political party	http://www.ucpb.org/	Official website of the United Civic Party (but on different IP address than in Table 1).
Opposition movement	http://www.zubr-belarus.com/	Youth movement "Zubr". Site provides information on missing politicians and arrested and sentenced activists, along with press releases, and also documents international actions of solidarity with Belarus. Users can print out "Zubr" logo, stickers, etc.
Independent media	http://www.naviny.by/	Belarus News, an Internet newspaper run by BelaPAN (a news gathering agency), which provides independent political news and commentary, as well as financial, cultural and sports coverage. News service is available by email (which circumvents blocking). In preparation for the election, the site provided several web addresses in case the primary one was blocked.
Independent movement	http://pahonia.promedia.by/ http://www.pahonia.promedia.by/	Online newspaper
Informative	http://www.livejournal.com/	Internet-diaries created and modified by the users.
Opposition movement	http://www.a-klimov.com/	Andrei Klimov's democratic movement, which is strongly anti-Lukashenka.
Informative	http://www.plyn.org/	Provides services to help users create and manage their own website (but most of the information is not legible).
Opposition party	http://www.bchd.info/	Belarus Christian Democrats' site, which is critical of both the regime and the opposition. The site incorporates news from other online news sources
Independent media	http://www.vybor.org/	Civil Initiative for free and fair elections.
Opposition movement	http://www.pbnf.org/	Belarus People's Front
Independent/ opposition monitoring site	http://www.wolnabialorus.org	Democratic association focused on promoting democracy in Belarus created by Polish youths, and including representatives of Belarus opposition.
Opposition political party	http://pkb.promedia.by/	The Communist Party
Opposition political party	http://www.kozylin.com/	The official website of Kozulin, the second most popular opposition candidate, providing biographic information, political platform, names of organizations/movements that support him, etc. His highly critical political address made during the elections on TV and radio stations is recorded and available online.

Table C3. "Socket Timeout" Errors

A "Socket Timeout" is the maximum amount of time the testing client will wait for a response from a remote server before terminating the connection. The "Socket Timeout" prevents the testing client from hanging indefinitely. This error is indicative of network problems, routing failures or IP blocking (null routing).

Type of Site	URL	Description of Site
Independent media	http://www.nn.by/	Media site, containing news, analysis, etc.
Independent Observation Mission	http://www.elections2006.ws/	A domestic organization monitoring the elections. The participants present themselves as "independent" and concluded that the elections were not free and fair.
Opposition initiative	http://www.multclub.org/	Website posting cartoons, including of Lukashenka. Also contains forums and links to opposition sites.
Opposition	http://www.bielarus.net/	Site of Belarus Solidarity, denouncing Lukashenka's regime and his violation of the Election Laws.
Opposition movement	http://www.solidarity16.org/	An initiative of Charter 97, which advocates for silent protest by lighting a candle every month.
Opposition	http://www.vybar.org/	Site motivating people to vote on the election day; openly denounces Lukashenka and his support form Russia, and includes an article on youth protests.
Opposition movement	http://www.3dway.org/	Youth society site supporting the protesters against the election result, and offering election news, discussion, analysis, and information about solidarity expressed in other countries.
Discussion forum	http://www.byelarus.org/	Internet forum for expression of ideas, political views and other interests.
Discussion forum	http://www.voka.tk/	Chat forum for "young" Belarus, who are inclined towards "civic activism"

Annex D. Additional websites reported as blocked, hacked or DoSed during the elections by the opposition media

This list contains descriptions of additional websites (beyond those listed in Annex C above) that the opposition media reported as being blocked, hacked or under DoS attack during the election period.

Website	Description
www.milinkevich.org	The official website of Milinkevich, democratic opposition candidate. The site provides biographical information, the names of his staff, up-to date campaign information, links to his TV and radio statements, a photo gallery from his political meetings and emphasizes his large domestic and international support. Campaign news from the 15 and 17 March lists the names of his supporters detained by the police. The site is available in Belarus and Russian with some English translations of leading news, Milinkevich's bio, and interviews. The site is well organized, attractive and the information provided is easily accessible.
www.charter97.org	Charter 97, an oppositional, human rights monitoring site providing up-to-date information on mostly political issues. In the run-up to the elections it carried statements of opposition candidates, including the joint statements of Milinkevich and Kozulin concerning their lack of confidence in the central Election Committee, as well as the opinions of foreign officers and observers. The site has articles on political prisoners, journalists sentenced to prison for defaming the president, etc., as well as a large photo library of oppositional actions, like youth demonstrations and missing politicians. The site is available in Russian, Belarus and English. Chapter 97 organization has carried out several projects related to the Internet, such as the "Free Internet" project, which was prompted in response to the alleged obstructed access on Sept. 9, 2001 to the main on-line news resources, including Charter 97.
www.elections.belapan.com	An Internet newspaper (special project of Belapan) that provides up-to-date information on the elections, links to past elections, and information on the basic principles and conditions regulating elections and referenda. The site presents the profile of each candidate for presidency with his biography and links to his political address and website. The site is available in Russian, Belarus and English.
www.afn.by	AFN, the Financial News Agency, a Minsk-based operation that reports on the state of global financial markets in Belarus, Russia and Ukraine, and which also contains news about the elections and human rights abuses (mostly relating to journalists). News articles prior to the election covered the harassment of the opposition, a comparison of media coverage for Lukashenka and the opposition, and reports of Lukashenka's threats directed at those who oppose him. The site also published the text of various speeches by Milinkevich and Kozulin. speeches from events that took place and those that were cancelled. A subscription service offers access to more content on the site. On March 17, 2006, free subscriptions were temporarily disabled, but it was possible to sign up with a credit card.
www.belaruspartisan.org	Belarus Partisan, which is mostly devoted to election news with some 50 articles in Russian that proclaimed a German radio station would be broadcasting election results, and provided updates on the persecution of political opponents, and other political news. The articles do not have dates, but seem to be recent. The copyright on the site says 2005-2006.
www.tut.by	A popular site, started in 2000, that provides news, forums, online shopping, and email services, which claims 70,000 unique visitors per day, the most of any Belarus site. The site has some statistics about the age, family status and financial situation of its visitors. It appears that it is visited mostly by people age 20-40 and with at least some higher education. The site has a significant section for election coverage, but does not appear to be biased in favour of any side. The site hosts other websites and helps Belarus companies get online. Its primary goal is to increase Internet use among businesses and individuals in Belarus.
www.news.akavita.by	A web portal supported by opposition candidate Kozulin, providing links to other online political and economic news sources. The site also supports a well organized web dictionary, Internet shops, and dating directory. Most of the political news is related to the elections, abuses of state power, and statements made by the presidential candidates.
www.unibel.by/	Unibel.by is a site about computers. It lists the services the company provides, the conditions to access, means of payments, prices. The site provides information about Internet projects that have sought to improve Internet access for the educational sector.
www.by.ru	By.ru, started in 2001, provides free website hosting and now has over 250,000 clients. The customer agreement states that the user will be liable for all content he or she places online. It prohibits posting pornography, hate speech, libelous or insulting postings, and malware. It also forbids political parties and campaigns. The site is geared toward Russian speakers and therefore any site that uses by.ru as a host must provide Russian translations of any foreign language materials.
www.livejournal.com	An Internet-diaries service, popular in Belarus. Users create live journals that can be searched. Users can get a paid account to post their photos, record voice posts, and create communities. The site is available in many languages, including Russian, Belarus and English.
www.leader.ru	A site that provides a list of proxy-servers that allows users to circumvent domain-based filtering (mentioned on all Belarus oppositional sites as the proxy list). There are different categories, including basic information about the site, whois checkup, web privacy, proxy and NAT software, filtering programs etc. The site is available in Russian and English.

Annex E. Inaccessible sites (19 March) by ISP (and location)

On 19 March, 37 unique sites were inaccessible from the state-owned Beltelecom network in Minsk. The sites were hosted on 25 separate ISP, spread across 6 countries.

Website	IP Address	ISP	Country
http://www.svaboda.org/	193.111.134.85	RFERL-NET	CZ
http://www.naviny.by/	195.137.160.82	TUTBY-NET	BY
http://www.unibel.by/	195.50.0.161	UNIBEL	BY
http://bhc.unibel.by/	195.50.0.161	UNIBEL	BY
http://www.livejournal.com/	204.9.177.18	SIXAPART	US
http://www.belmarket.by/	217.16.28.138	Masterhost	RU
http://www.nn.by/	217.16.28.138	Masterhost	RU
http://pahonia.promedia.by/	217.16.28.138	Masterhost	RU
http://www.pahonia.promedia.by/	217.16.28.138	Masterhost	RU
http://pkb.promedia.by/	217.16.28.138	Masterhost	RU
http://www.bdg.by/	217.23.147.147	CARAVAN-HOSTING	RU
http://www.svaboda2006.org/	217.31.49.3	IGNUM-CZ	CZ
http://www.voka.tk/	62.129.131.38	VERZA	NL
http://www.zubr-mogilev.tk/	62.129.131.38	VERZA	NL
http://www.gay.ru/	62.205.161.8	Corbina Telecom	RU
http://www.mfront.net/	63.241.136.205	CERFnet	US
http://www.a-klimov.com/	64.21.117.97	Net Access Corporation	US
http://www.bchd.info/	66.135.33.237	ServerBeach	US
http://www.islam.by/	66.235.186.165	HopOne Internet Corporation	US
http://www.wolnabialorus.org/	66.244.251.19	Big Pipe Inc.	CA
http://www.bielarus.net/	66.45.228.135	Interserver	US
http://www.vybar.org/	66.45.228.135	Interserver	US
http://www.bsdp.org/	66.98.250.75	Everyones Internet	US
http://www.belngo.info/	69.50.196.170	ATJEU	US
http://www.plyn.org/	69.50.196.170	ATJEU	US
http://www.solidarity16.org/	69.93.4.245	ThePlanet.com	US
http://www.zubr-belarus.com/	69.93.4.245	ThePlanet.com	US
http://www.studenty.alternativy.net/	70.84.17.228	ThePlanet.com	US
http:www.prizyv2005.alternativy.net/	70.84.17.228	ThePlanet.com	US
http://www.belintellectuals.com/	70.85.182.2	ThePlanet.com	US
http://www.vybor.org/	72.29.73.91	HostDime.com	US
http://www.pbnf.org/	72.9.232.242	Global Net Access	US
http://www.gsu.unibel.by/	80.94.161.9	BAS-NET	BY
http://www.elections2006.ws/	81.177.10.242	AGAVA	RU
http://www.ucpb.info/	81.177.16.130	NETHOUSE-MOSCOW	RU
http://www.ucpb.org/	81.177.16.130	NETHOUSE-MOSCOW	RU
http://www.multclub.org/	81.222.134.156	SpaceWeb	RU
http://www.3dway.org/	81.222.134.156	SpaceWeb	RU
http://www.kozylin.com/	81.222.134.156	SpaceWeb	RU
http://www.byelarus.org/	82.165.193.206	SCHLUND-SHARED	US