Fair and free

Internet and elections in 2006

This text is based on the Internet Watch report on Belarus, a project by Open Net Initiative. It was the result of ONI monitoring of the Belarusian Internet during the March 2006 presidential elections.

The testing was unable to prove 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 in Belarus. 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. The government has the 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 cyber-self-censorship.

* * *

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."[1]

Economically, the formal financial regulative bodies 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 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."

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

Based upon the Internet Watch report on Belarus

[1] According to recent statements by the Minister of the Interior (Uladzimer Navumau), this law will be used to track down regime dissenters in cyperpace

Hackers put a caricature on the web-page of the State-owned channel ANT.

"inappropriate information, and many independent papers have been forced to close. Television and radio is dominated by state-run media, with the remaining independent outlets "choosing" to carry mostly entertainment programmes or local events.

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

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 Łukašenka 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, organizational 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 "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 Łukašenka 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 (the channels jammed) with Belarus content taking their place. The authorities have been known to charge Russian correspondents in Belarus with "honour and dignity" offences, to prevent them from transmitting (to Russia) materials viewed as unfavorable to the Łukašenka regime.

Internet

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.

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.[2] Surveys suggest that most users are young, educated and urban, based in Minsk or the regional centers.[3]

In this respect, the majority of Łukašenka'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 Łukašenka regime's policies and propaganda, trust independent news sources more than state-run organs, and were more inclined to actively support the opposition.

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 Łukašenka regime was deliberately blocking access. In June 2003, the www.batke.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 Łukašenka to amend the constitution so he could continue his reign), oppositional websites again reported access problems, albeit on a lesser scale.4 In 2005, various websites claimed they were victims of deliberate blocking by state authorities or DOS attacks.5 However, none of these accusations has been independently verified on the basis of testing. And in the absence of this, the Łukašenka 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 websites being filtered in Belarus at that time were Russian gay 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.[6] 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).

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). 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

[2] 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 (RWB "*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.

[3] A 2003 survey found the 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.

[4] 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 naviny.by, had their phones turned off for the day. See Freedom House, Nations in Transition 2005.

[5] For example, in August 2005 a site with cartoons about President Łukašenka was reportedly blocked, and the two youths who had placed the cartoons online were charged with the criminal offence of slandering the President.

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

by the Ministry of Communications. 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.[7] Thus, all 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 registered in domains outside of the .by domain – like .com, .net or .org. 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.[8] 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.

The third level for potential filtering of websites is at the level of the non-state owned ISPs themselves.[9] 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. 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.

What we tested, and what we found…

ONI testing during the 2006 Presidential elections revealed a generally open and accessible Internet throughout the entire election period, including election day (19 March) and the next week when the opposition attempted to challenge the results by staging demonstrations (20-25 March). ONI 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 were inaccessible. On one occasion Internet connectivity in Belarus failed, apparently for technical reasons, 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 "high impact" websites on two Belarus' ISPs.[10] Tests were run from Belinfonet between 12 to 25 March, and on Beltelecom from 17 to 25 March.

16 March: several opposition and independent websites allegedly come under unspecified network-based attacks causing them to fail.

16 March: The website belaruspartisan.org was also 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.

18 March: Five sites accessed through the Beltelecom network returned results consistent with those for "blocked sites". 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,

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

[8] 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.

[9] 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 totaled 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.

[10] 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.

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.

18 March, 23:00hrs: 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." 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.

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

Numerous opposition and independent media sites are reported as "blocked." Two rounds of ONI testing on 19 March found that 37 sites – mostly opposition and independent media sites – were inaccessible from the Beltelecom network in Minsk, even though they were accessible from the control location. However, the tests did not yield conclusive evidence of comprehensive filtering. The reasons for failure differed from site to site, and the same sites remained accessible from the Belinfonet network. As a consequence it is conceivable that the results obtained from tests on Beltelecom may have been caused by other factors. For example, network congestion could be one explanation, as our tests indicated high levels of latency and "dropped packets" on the Beltelecom network on 19 March. This is consistent with reports from users that sites failed to load, or only partially loaded before timing out. However, this explanation is unlikely as testing confirmed that other less political sites remained fully accessible for subscribers of the Beltelecom network. "Congestion" should have affected all sites, and not just the 37. Furthermore, we can exclude that the "failures to load" were a consequence of high demand for the affected website servers, as these servers remained accessible from Belinfonet and the ONI control location. Taking all evidence under consideration, the 37 sites may well have been tampered with on the Beltelecom network.

Hacking reported against main opposition websites, and that of the main opposition candidate.

www.milinkevich.org – Opposition media sources reported that the site had come under a denial of service attack. 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. A "dead" site is consistent with the results of a DOS attack. However, ONI cannot confirm that an attack took place without access to the server logs. ONI was unable to access the server logs, despite requests to the hosting company in the United States as well as the site owners.

www.charter97.org – Belarus sources reported that outages experienced by this site were a result of various forms of electronic attack (DOS and hacking). 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 conducted by ONI investigators found that the domain charter97.org resolves to two distinct IP addresses. One of these IP addresses behaved erratically and was inaccessible at times. It is possible that that this IP address was subject to a DOS attack. However, as ONI was not able to obtain log files from the charter97.org it was impossible to verify this possibility. Nonetheless, the fact remains that one of the two IP addresses associated with this site was effectively "inaccessible." 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.

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

21-22 March: www.milinkevich.org experiences irregular access. The results may indicate the site was under a DOS attack.

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 was caused by a misconfigured nameserver on the Beltelecom network.

23-24 March: forum site for charter97.org returned anomalous "inaccessible" errors. Two rounds of test-

ing 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, (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.

25 March: dial-up Internet services in Minsk fails. Beltelecom's webpage 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)

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. The 25th is the day Belarus riot police broke up demonstrations by the opposition in Minsk.

Did the government tamper with the Internet?

Despite considerable evidence of suspicious problems with the Belarus Internet during the election period, ONI testing did not yield conclusive proof that the authorities engaged in systematic and comprehensive filtering of opposition and independent media websites.

However, ONI testing did return evidence of inaccessible or partially disabled sites on certain days at certain times from certain locations. And follow-up testing and investigation cannot rule out the possibility that some Internet tampering took place during the election period:

- 37 opposition and media websites were inaccessible from Beltelecom 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 Milinkievič was "dead" on 19 March and experienced problems on the 21-22, (the post-election protest period); and,
- the main website of the opposition movement (Charter'97) was only partially accessible between 19 to 25 March.

The 37 sites

ONI testing evidence, in combination with user field reports, does suggest 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 Belinfocom network inside Belarus on the 19th, meaning that any filtering that may have taken place was only partial in effect. 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.

And yet even the confirmed problems with these sites on the Beltelecom network do not yield an iron-clad case for filtering. The evidence in favour is two-fold: the analysis of message headers whose returns were consistent with those found in cases of filtering; and, our users in Minsk who 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. So what are the other possible explanations for such selective difficulties?

It is possible that the 37 sites had excessive loads on the servers themselves, causing failures or time-outs. However, this is unlikely given that the same servers remained accessible for our test runs from Belinfonet and the ONI control collocations, meaning that the severs were behaving normally when dealing with requests. Another explanation could be a combination of intermittent network problems and sever loads that 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.

The "dead" websites

ONI cannot verify the claims that two major opposition sites were taken down by way of DOS attacks or hacking (as claimed). In the absence of log files, ONI investigation can only confirm that the website of the main opposition candidate was "dead" on election day. With

respect to the other site – the main opposition movement website charter97.org – ONI investigation found the site to have remained partially accessible because the domain resolved to two separate IP addresses. One of the IP addresses provided uninterrupted access throughout the elections. The other IP address returned an error of "body time out" which could be indicative of a DOS attack (but we didn't have the logs to prove it), but could also have been caused by high demand, or a misconfiguration of the web-server located on that IP address. Overall, however, the fact remains that both the Milinkevich.org and Charter '97 sites were down during election day. At the very least this suggests 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?

Taking into account all evidence above, we cannot say for sure whether the Internet in Belarus was deliberately restricted during the elections.

For now, we can say that ONI results suggest that the opposition reports of extensive and outright filtering during the elections are likely overstated. Websites that were down on Beltelecom remained accessible from 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 implemented a comprehensive "filtering system".

At the same time, it is clear that suspicious irregularities did affect access to opposition and independent media websites before, during and after the elections, although the level of interference was erratic. The effect was information disruption, not blockade. It also seems that the problems were mostly occurring state-owned monopoly provider – Beltelecom.

Overall we are left with a puzzle. Given the authorities' proven intolerance for oppositional and critical information, and given their known technical capability for potentially and comprehensively filtering, the Net, why didn't they?

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 large-

Andrej Lankievič

Young activists use the Internet to organize flash mobs like this one, of solidarity with political prisoners.

ly unfettered during the 2006 election period. 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 still-born "denim revolution." Third, despite vociferous accusations that Belarus' websites were "taken down," 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.

And yet 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. So why was the Internet relatively untouched?

photo.bymedia.net

Śviatłana Kalinkina (center) and Paviel Šaramiet (right).

Not now, darling. We've got company

There are four plausible answers. First, it could be that Łukašenka 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.

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 cyberspace in its effective fight against cybercriminals.

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.

Summary: Wither Belarus?

Given the regime's efforts to shut down independent informational and organizational space in Belarus, the Internet is likely in its "sights." This is especially so as independent and oppositional voices are increasingly taking to the web to organize and get their message out, as the 2006 elections have shown.

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 outright blocked.

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

- **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, are accessible throughout the election period.
- **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 empowered 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:

- **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
- **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 collocating copies on server farms (where one IP address is shared by numerous sites). Intelligent firewalls that capture possible attacks should also be used on primary servers sites, so as to validate and possibly counteract attempts at hacking or DOS attacks.
- **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 "contested" Internet environment.

Beltelecom monopoly: Revenue, power and control

Beltelecom is the main source of revenue for the Ministry of Communications and Informatization (MCI). Various MCI 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 commu-

nications. 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 worth of business before caught by the KGB, fined, charged and shut down.

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 Łukašenka's main powerbase (rural workers).

The state's financial interests in the telecommunications 'market are not unsubstantial. In 2004 the market totaled $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.

The most popular Belarusian web-sites

(listed according to the rating by www.akavita.by counter)

General

www.tut.by	information, mail and service portal
www.akavita.by	reliable web-counter
www.date.by	information and search system
www.kosht.com	shopping and pricing site
www.realt.by	realty site

Media, news & analysis

www.charter97.org	independent news service, available in Belarusian, Russian, English
www.naviny.by	independent news service of Belapan information agency, available in Russian, English
www.belaruspartisan.org	Russian-language, Russian-oriented independent news-service
www.kp.belkp.by	"Komsomolskaya Pravda v Belarusi" newspaper web-site; the newspaper is affiliated to the Russian "Komsomolskaja Pravda"
www.bdg.by	web news service, made by the editors of the former newspaper "Beloruskaja Delovaja Gazeta"
www.afn.by	independent agency of financial news site
www.svaboda.org	Radio Liberty Belarusian service site
www.nn.by	"Nasha Niva" newspaper web site
www.gazetaby.com	web news service, made by the editors of the former newspaper "Salidarnaść"
www.belta.by	state owned news agency
www.sb.by	"Sovetskaya Belorussiya", official presidential newspaper web site
www.nv-online.info	"Narodnaja vola" newspaper web site
www.nmnby.org	analytical Russian language web site
www.tvr.by	"Belarusian TV Channel 1" site
www.tube.by	video portal
www.belradio.fm	"European Radio for Belarus" site
www.belmarket.by	"Belorusy i Rynok" business newspaper web site
www.belapan.com	Belapan information agency web site, available in Belarusian, Russian, and English versions
www.racyja.by	Radio "Racyja" site
www.camarade.biz	"Tovarishch", communist newspaper site
www.zvyazda.minsk.by	"Zviazda", Belarusian-language official newspaper web site
www.belarustoday.info	Minsk English-language newspaper web site
www.arche.bymedia.net	"Arche" intellectual monthly magazine

State institutions

www.president.gov.by	President of Belarus official site
www.minsk.gov.by	Minsk City Executive Committee site
www.pravo.by	national legislation portal
www.government.by	Council of Ministers site
www.mfa.gov.by	Ministry of Foreign Affairs site
www.mod.mil.by	Ministry of Defense site

Politics, NGOs and communities

www.uspb.org	United Civic Party site
www.minsk_by.livejournal.com	independent LJ-community uniting people sharing political information as well
www.kozylin.com	personal site of Alaksandr Kazulin
www.milinkevich.org	personal site of Alaksandr Milinkievič
www.mfront.net	Małady Front, most persecuted opposition youth organization site
www.generation.by	site for students close to the underground Association of Belarusian Students
www.pbnf.org	Belarusian Popular Front Party site
www.baj.by	Belarusian association of journalists site
www.bielarus.net	Conservative-Christian Party BNF (Zianon Pazniak) site
www.bchd.info	Belarusian Christian Democracy forming party site
www.pozirk.org	Blogging community

Education

www.bsu.by	Belarusian State University on-line
www.bseu.by	Belarusian State Economic University site
www.bsuir.unibel.by	Belarusian State University of Informatics and Radio-Electronics site
www.baj.by/belkalehium	Belarusian College, independent educational initiative

Society, culture & arts

www.music.fromby.net	independent musical site
www.photoclub.by	photo portal
www.belzhaba.com	satirical site, publishing political caricatures and collages
www.catholic.by	Catholic Church site
www.radzima.org	historical heritage independent site
www.church.by	Belarusian Orthodox Church site

Libraries & bookshops

www.nlb.by	National Library of Belarus
www.knihi.com	Belarusian independent electronic library
www.kamunikat.org	another Belarusian independent electronic library
www.knihi.net	books and disks by post on-line

Regions

www.blog.grodno.net	Hrodna blog
www.news.vitebsk.cc	Viciebsk people, news, services
www.gs.by	Gazeta Slonimskaja, Hrodna region local newspaper site
www.homiel.org	Homiel Hart unregistered youth initiative site
www.hrodna.by	Hrodna independent web portal
www.dzedzich.org	Brest youth initiative site