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.

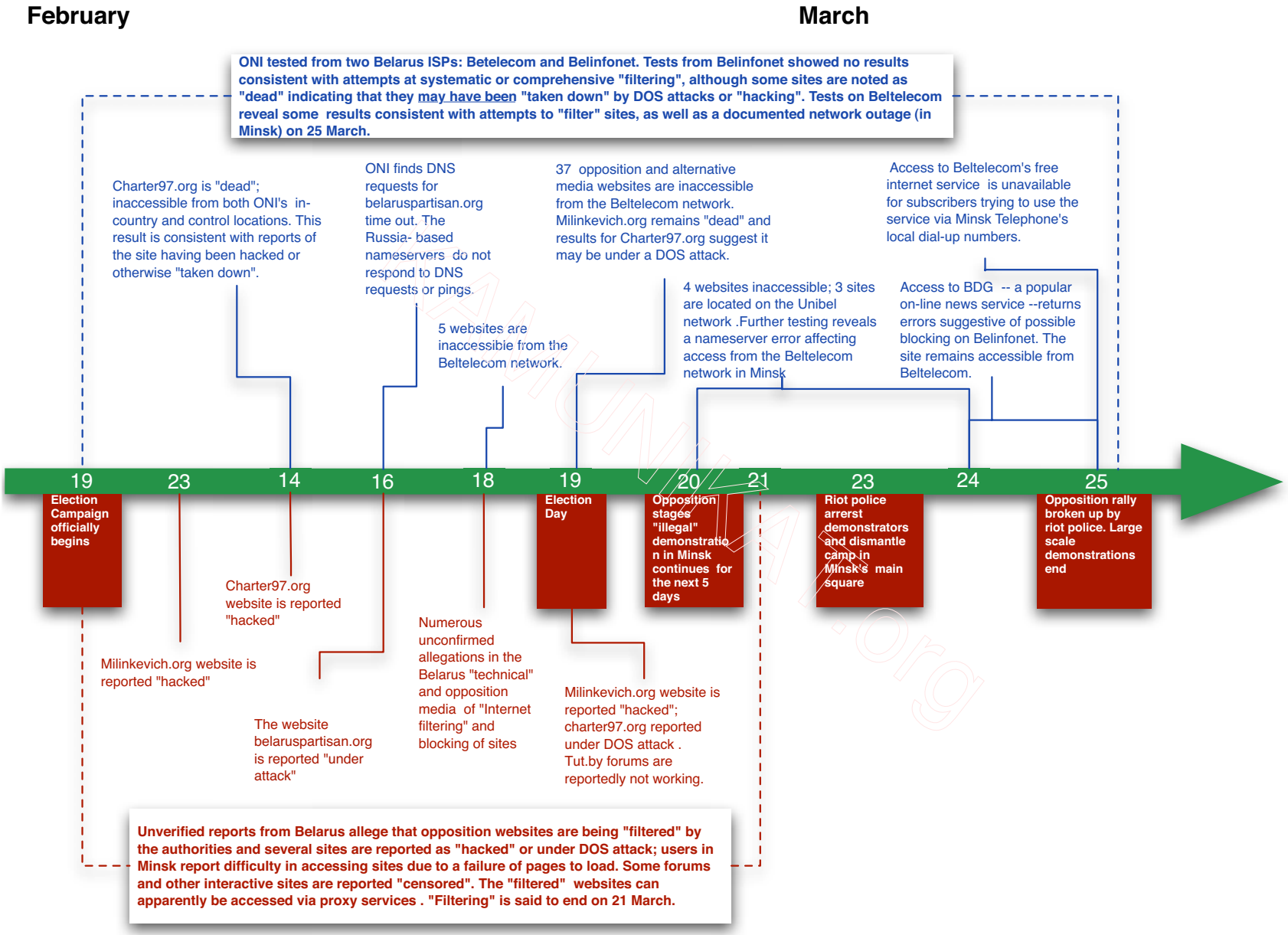

February
March
ONI tested from two Belarus ISPs: Betelecom and Belinfonet. Tests from Belinfonet showed no results consistent with attempts at systematic or comprehensive "filtering", although some sites are noted as "dead" indicating that they may have been "taken down" by DOS attacks or "hacking". 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 BDG -- a popular on-line news service --returns errors suggestive of possible blocking on Belinfonet. The site remains accessible from Beltelecom.
Access to Beltelecom's free internet service is unavailable for subscribers trying to use the service via Minsk Telephone's local dial-up numbers.
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
Charter97.org website is reported "hacked"
Milinkevich.org website is reported "hacked"
The website belaruspartisan.org is reported "under attack"
Numerous unconfirmed allegations in the Belarus "technical" and opposition media of "Internet filtering" and blocking of sites
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

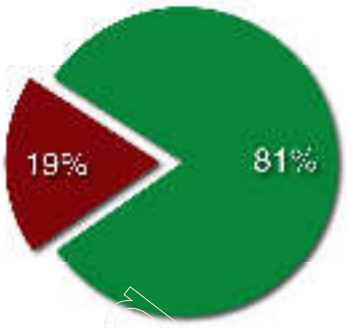
42 http://www.e-belarus.org/news/200603201.html

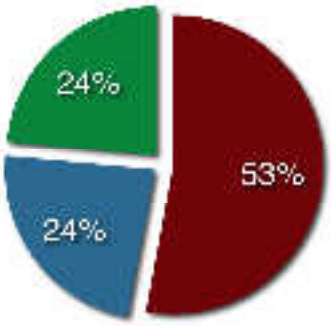
43 http://bybanner.com/show.php3?id=1816

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.

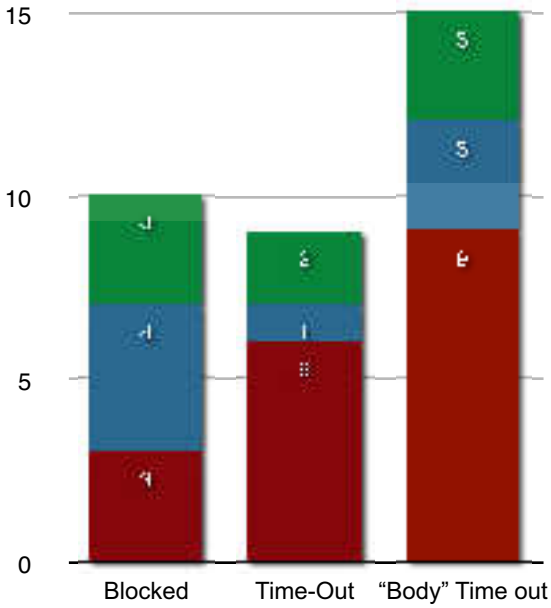




Of the 19% inaccessible from Beltelecom, 53% were sites belonging to opposition political parties (or movements), 24% were independent media sites, and 24% included blog sites and other informational content sites.

- 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.