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.