Executive Summary

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

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

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

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

- 37 opposition and media websites were inaccessible from the state-owned Beltelecom network on 19 March (election day), although they were accessible within Belarus from a different ISP network as well as from the external control location;

- the Internet was inaccessible to subscribers using Minsk Telephone access numbers on March 25 (the day of a major demonstration, when riot police were used to disperse and arrest protesters);

- the website of the main opposition candidate Aleksandr Milinkevich was “dead” on 19 March and experienced access issues on the 21-22, (the post-election protest period); and,

- an opposition website (Charter 97) was only partially accessible between 19 to 25 March.

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

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

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

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