Introduction

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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