Part Five. The Internet election challenge: Perspective and recommendations

Monitoring Internet openness during elections: A slippery challenge

This report marks the second occasion ONI has examined the openness of the Internet during national elections. In both cases -- during the 2005 Kyrgyz parliamentary elections and the 2006 Belarus presidential elections -- we found evidence that the Internet was becoming part of the electoral campaign and that civic and political groups were expressing increasing concerns about Internet openness. In neither case did we find black-and-white cases of deliberate filtering using standard techniques, such as those employed by China, Iran and Saudi Arabia. We did, however, find "greyer" evidence that suggested more subtle, less attributable techniques were at play, such as DoS attacks to take out certain websites at critical times. These initial findings suggest we may be looking at the start of a pattern of "below-the-parapet" Internet tampering during elections in democratically-challenged countries.

Arguably, a preference for subtle pressure on the Net may stem from the nature of elections themselves. Any government -- no matter how authoritarian -- that decides an election is needed to renew claims of legitimacy, risks losing that legitimacy if its attempts to "shape" the outcome are too obvious or heavy handed. Thus, Chinese-style "filtering out" to eliminate access to legitimate opposition parties in their entirety would be immediately obvious, and the finger of blame easy to point at the state.

We can also speculate that indirect methods (such as DoS attacks, hacking, or simply allegations thereof) are preferred because of their effectiveness. In elections, timing matters. Tampering with access to political websites or alternative news sources need not be long-lasting or comprehensive. Sites need not be blocked for weeks. All that is really required is a well-targeted disruption, to reduce or "confuse" message flows at a critical time -- say before a rally or after a major government announcement or on voting day when last minute information could play a role in changing how people vote.

Indirect filtering is also hard to prove, which makes it attractive in a politically charged environment. Interruption of Internet services that occurs during an election period is often viewed with more suspicion than disruptions at other times. These suspicions – combined with the potential political advantage that could be gained by levelling accusations of "censorship" against one's opponents – can make it difficult to distinguish between alleged cases of censorship, and actual verifiable cases. In these circumstances indirect techniques can yield valuable political advantage to whomever can "spin" and defend their story more effectively. Governments can interfere and interrupt opposition groups at critical times while retaining "plausible deniability." Similarly, opposition groups can claim government interference, regardless of whether they have evidence to support these claims.

Overall, it is fair to suppose that the "openness" of the Internet is likely to come under increasingly indirect and sophisticated forms of information control during election periods, with methods that squeeze access rather than filter content, and which mimic network timeouts or other plausible errors.

All of this makes monitoring the Internet during elections especially difficult, and fraught with methodological challenges. Passive testing techniques that rely on header returns and are used by ONI to test for the presence and absence of "filtering" are simply not sufficient to detect and verify indirect methods and techniques. As noted in Part 2, proving that sites have been hacked or subject to DoS attacks, for example, requires access to server log files, which can only be obtained from the website owners or hosting services. Even then, in the case of sophisticated techniques, other more specialized tests would be necessary to positively identify that a server was under a DoS attack. Besides, website owners are justifiably reluctant to share logfile information, which contains the source address for legitimate users of their websites as well as the "bots" used in DoS attacks. In the wrong hands, this information could be used to identify individual users and lead to harassment or other forms of prosecution. Beyond this, owners of political websites may have other motives for protecting log files from inspection. Thus, allegations of DoS attacks may be as effective as actual attacks, a convenient way to gain political capital out of normally occurring network anomalies or other technical failures. It is better to claim your website is inaccessible due to deliberate hacking, than to admit to poor design or maintenance.

The Internet is fast becoming an important component of the democratic and electoral process. There are signs it may eventually surpass the importance of other mass media as a means for grass roots campaigning. Ignoring the Internet during elections leaves the door open to possible abuses. And yet, monitoring the Internet during elections is a slippery business. It urgently requires the development of new testing methodologies and monitoring capabilities. It is to these issues we now turn.

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

1) **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, throughout the election period.

2) **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 whose task is 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

The Internet is fast becoming a strategic informational space, one which until recently has remained largely uncontested. This is changing rapidly. The importance of the Internet to the 'Colour Revolutions" and its increasing penetration world-wide means that is only a matter of time before governments, particularly those with less than transparent agendas recognize the advantages of indirect methods of strangling access to Internet informational resources – as opposed to blunt filtering which unambiguously identifies the perpetrator.

The contested nature of the Internet has become more visible through the US-led "war on terror," which has been stretching global norms to accept the use of "computer network operations" (CNO) as a means for combatting "illegal and terrorist organizations" on a global scale. In 2003, the US Department of Defense's *Information Operations Roadmap*, clearly stated that the US would prepare to "fight in the Net," that is, to unambiguously contest "terrorists" and their supporters in cyberspace, regardless of where they are located. Taken together with the shift in US strategic policy towards preemption of threats "before they are fully formed," this stance has effectively opened the door for states to use CNO as a means to act unilaterally and extraterritorially to combat self-defined threats to national security. As a consequence, CNO and Information Warfare (IW) are amongst the most secretive and fastest growing areas of investment for military, security and signals intelligence organizations worldwide. Moreover, as the recent revelation concerning the US National Security Agency's extralegal tapping of domestic communications (including the Internet) suggest, even open and democratic societies are undertaking covert Internet surveillance. If the United States does not require transparent legal standards for Internet surveillance, then what are the implications for states with less robust legal cultures and institutions?

It is imperative that civil society groups start to take information security seriously, and prepare to operate in a more contested and less secure informational environment. With respect to elections, it is important to advocate for an open Internet that is accessible to all. Therefore civil society groups should:

1. **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.

2. **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 using server farms (where one IP address is shared by numerous sites) and virtual hosting. Intelligent firewalls that capture possible attacks should also be used on primary server sites, so as to validate and possibly counteract attempts at hacking or DoS attacks, while still preserving the privacy of site visitors.

3. **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 the "contested" Internet environment.

*   *   *