



# **Political Organizing in Closed Societies**

*Building Support for Democratic Change in Belarus*

Lindsay Beck

Information and Communication Technology Programs

National Democratic Institute

## **Executive Summary**

In politically closed environments such as Belarus, leveraging technology to organize a base of support to advocate democratic change or to effectively mobilize supporters to take advantage of organizing opportunities offered by elections, even rigged elections, can be a challenge.

Voter files are often non-existent or inaccessible to opposition political forces. Maintaining secured records of supporter contact information is exceedingly difficult. Telecommunication firms who are closely aligned with the authoritarian regime may disable access to critical communication technologies, such as Gmail, Facebook, or Youtube, and have been known to monitor or disable certain telephone numbers and filter SMS. Collecting, securing and using supporter data is further complicated by the security services of restrictive governments, such as the Belarusian KGB, who routinely confiscate equipment, infiltrate democratic networks and detain activists.

The National Democratic Institute (NDI), a Washington-based democracy support organization that works in more than 70 countries around the world, recently completed a program to help pro-democratic political forces working to engage citizens and organize public support for democratic change to more effectively manage supporter data during and after electoral campaigns.

These democratic political forces sought to utilize technologies that political parties and movements in more open countries regularly use to organize members and potential supporters and to ensure national and local data can be shared and utilized by all levels of an organization. Through the use of technology, we saw an opportunity to help these democratic political forces utilize their resources more efficiently as well as assist them in increasing their outreach to supporters without endangering these same supporters.

In short, NDI sought to address the needs of our democratic partners by developing a secure and usable online voter management system. The development of the system incorporated two distinct but related approaches:

1. Data security via Tails (The Amnesiac Incognito Live System), a Linux-based, live-boot operating system that can be used on any Windows-based computer to completely obscure the user's activity (Tails is a portable operating system with all the security bells and whistles a user in a closed environment might need already installed on it, without having to manage or install security applications);
2. and a data management system; in this case a Drupal-based open source member management database called CiviCRM;

## **Context**

Belarus has not had a free or fair election since 1994, when Alexander Lukashenko was first elected to the Presidency and shortly thereafter began to systematically eliminate his competition, dismantle democratic political forces and reinstated a Soviet style authoritarian state often referred to as the "last dictatorship in Europe."

Prior to the December 19, 2010 presidential election, Belarus experienced a brief period of

psuedo-liberalization stemming from the regime's need to build better relations with western democracies and improve negotiating leverage with Russia. Compared to the 2001 and 2006 presidential elections, the candidates were given more freedom to meet with voters and disseminate their campaign materials. Lukashenko even took the unprecedented step of allowing nearly all opposition candidates to register and even debate each other on state-controlled media. Election day and its aftermath, however, demonstrated the shallowness of Lukashenko's liberalization policy. The authorities violently dispersed tens of thousands of Belarusians who gathered on the main square in Minsk to protest fraud and vote rigging. Hundreds of political activists, journalists and civil society representatives were severely beaten and detained by the police, including seven of the opposition candidates who challenged Lukashenka in the election.

In the days and months following the election, Belarusian security services, led by the KGB, actively worked to disrupt and eliminate the capacity of democratic political forces, civic groups, independent media and individual democratic activists. To silence dissent and re-establish authority the KGB raiding the homes and offices of democratic organizations and activists. Over 600 persons were arrested, of whom 13 remain political prisoners until today, numerous computers and servers were seized costing political forces much of their organized database lists. Included in the seized items were much of the supporter lists of the democratic forces. Ultimately the goal of the crackdown on Dec 19th and the months following was to re-instill a sense of fear of politics and political action in society that was whittled down as an unintended consequence of the government's psuedo-liberalization policy.

The early summer of 2011 was marked by a number of protests by workers and drivers that were focused on the economy, and by a wave of "silent protests" that were organized primarily by youth activists through online social media. These were the first actions following the Dec 19th crackdown and the first efforts of the society to push back against the culture of fear imposed by the government. In response to the "silent protests," authorities arrested hundreds of protesters and threatened activists with expulsion from universities or loss of employment. The authorities also increased their online anti-activism efforts by disseminating propaganda via Twitter and Vkontakte (the Russian social network that is similar in functionality to Facebook), and by conducting targeted digital attacks against the websites and accounts of pro-democracy organization. With activists harassed, equipment confiscated, and leaders awaiting their fates in jail, parties and NGOs are struggling to regain the momentum built up prior to presidential elections.

Over half a dozen of the democratic political forces working with NDI recognized the need to regain their lost footing and to re-establish a meaningful dialogue with citizens. They turned to local grassroots action and participation in elections as a mechanisms to communicate with citizens and build long term support for democratic change. While elections in Belarus are not competitive nor legitimate they provide political forces with a legal opportunity to engage the public and build support. To make the most of the political opportunities presented through elections and grassroots action NDI's democratic partners sought to embrace technologies (already used by political parties and organizations in other countries) to maximize their potential and efficiently build and sustain support networks.

**TAILS: A Secure, Bootable Operating System**

One of the major challenges facing the partners in their ability to securely access any collected data. Housing the extensive set of data on supporters that partners had collected inside of Belarus was not feasible - a high risk of office raids and confiscation would have put the democratic partners and their supporters at risk. However, accessing this information on a web-based system was that their own computers and internet access could not be trusted.

According to the Opennet Initiative, while Belarus does not have the same capabilities as Russian authorities to conduct wide-scale monitoring of internet use, it is widely believed that

*“Belarusian and Russian special services cooperate in this sphere. More than 70 percent of Belarusian Internet traffic goes through Russia, and part of it is processed through the Russian system SORM-2. Nonetheless, some providers confirm that the authorities have unofficially requested that all user IDs be kept for a few months and be turned over to the security services on demand.”<sup>1</sup>*

In addition, the majority of participants in this project reported that the operating systems on their personal computers were infected with malware, and that they suspected that email and chat conversations taking place on these machines were being tracked and provided to the authorities without their knowledge. Thus, these individuals needed to utilize a secured operating system that would not leave traces of their data on the machine, and that would increase the likelihood that information sent over an internet connection would evade any filtering or monitoring techniques.

To accomplish this task, NDI trained partners on the use of TAILS, a Linux-based operating system that routes all internet traffic through the Tor network and expunges all user-added data upon system shutdown. One of the limitations to TAILS is that it relies on a legacy BIOS framework to boot on computers, so a few participants were unable to successfully boot the system on their newer machines. Despite this challenge, TAILS ensured that the using participants were practicing good digital security habits (securely delete sensitive files, visiting websites through an SSL connection, and connect to the internet through an anonymizing proxy over an untrusted network, etc.) because these habits were inherent in the design of TAILS, instead of relying on participants remembering to do so in the stressful and hectic political environment like Belarus.

## **CiviCRM**

The partners in Belarus used varied methods at the national and local level to store and categorize the collected data they received from their supporters such as paper note pads, cell phone lists, Excel spreadsheets and Access databases, stored on servers both inside and outside of the country. A major problem was that data was often either too centralized at the national level and inaccessible to regional activists who needed it or so fragmented at the local level that it could not be linked into part of a nation wide supporter and voter outreach effort. A major goal of the NDI developed data management system

---

<sup>1</sup> Opennet Initiative Country Profile: Belarus <http://opennet.net/research/profiles/belarus>

was to create an effective national level data management system that was accessible and user friendly for regional democratic activists. NDI developed a customized constituent relations system (CRM) database based from the open-source system CiviCRM. Each organization had their own CiviCRM instance, developed to meet the unique needs and feedback received from each partner, which was then sub-divided by divisions within the party, with each lower-level organizer only able to view and modify information for their region. In addition, there are a number of different roles within the system, with some groups able to do only data entry, others with access to data for viewing, and a few with access to view and update all records in their particular geographic zone. The purpose of the use of fine-grained roles is to ensure that if any specific accounts became compromised, an attacker would only be able to see a portion of information within the database rather than all stored content.

With use of CiviCRM, the participating organizations were able to: define the criteria of data which they wanted to keep, and have these definitions inform their data hygiene as well as their data collection procedures going forward. This systematized way of collecting data improved coordination among the central office and organization branches, resulting in more impactful outreach to supporters. One obstacle that emerged through implementation of this system was complete localization. While all organization members were fluent in Russian, it was acknowledged that some of the nationally oriented Belarusian opposition groups, particularly some of the younger activists, would have preferred for political and cultural reasons to utilize a system in Belarusian. Ultimately due to financial and time constraints it was not possible to fully translate the system into Belarusian though the system did incorporate spelling for cities, streets and surnames in both Belarusian and Russian.

### **Outcomes and Conclusion**

The participating organizations in this project have largely seen the value of more effective data management. Creating a detailed record of supporters (due to the absence of voter files) will greatly improve upon their ability to conduct outreach. In the months since the launch of the data system, eight political forces have uploaded over 113,220 contacts into the system. During the parliamentary elections of 2012 at least one candidate team began utilizing the system recording the voters they contacted and uploading 3,000 new supporters to the system. Belarusian political forces have utilized database also to re-engage their supporters after the elections: 7,700 letters were sent in Minsk, Bobruisk and Brest cities of Belarus.

Political forces have trained regional teams to utilize the data and they are now incorporating the system into voter outreach plans for both issue advocacy efforts and preparations for the 2014 local elections and 2015 presidential elections. Using a secure access tool like TAILS will help to keep the organization's data safe and help thwart any efforts to monitor and track the political activities of these groups. Despite efforts by a repressive regime like that in Belarus to diminish the campaigning and outreach efforts of political and social movements, with a combination of secure access and data management technologies, these movements can continue to thrive.