

National Democratic Institute

This case study examines how the National Democratic Institute (NDI) worked with and trained partner organizations to use FrontlineSMS for election monitoring and the associated data protection and security vulnerabilities, threats, risks and actions taken to reduce risks.

Project Description	NDI used FrontlineSMS to work with a coalition of opposition parties in Belarus to monitor the election in December 2010.
Vulnerabilities	<ul style="list-style-type: none">• Service interruption• Data monitoring• Data poisoning
Threats	<ul style="list-style-type: none">• Local government and mobile network operator
Risks	<ul style="list-style-type: none">• Location information accessible by the mobile network operator• Election monitoring program is not available during the election period• Monitors identified and arrested
Risk Reduction	<ul style="list-style-type: none">• Service interruption plan created

FrontlineSMS and NDI

NDI provides technical assistance to political parties, legislatures, civic groups and other organizations in over 70 countries to strengthen democratic institutions, safeguard elections, advance citizen engagement and promote open and accountable governments.

NDI worked with partners in Belarus to deploy FrontlineSMS to monitor the national election in December 2010. The goal of the platform was to provide qualitative election monitoring information to groups that could hold the government accountable for the numbers reported. By generating indicative information that could be compared with government-reported statistics, NDI hoped to be able to illustrate inconsistencies. For example, if only 200 people were registered at a polling station but 400 votes were counted from that location one may be able to conclude that unusual or illegal activities had taken place. NDI decided to use FrontlineSMS rather than an online or commercial alternative in order to try to avoid government attention.

Together with political opposition parties, NDI worked closely with the political parties to develop checklists and set up a reporting strategy, which the parties implemented. Observers from the parties were trained to report on voting activity and potential irregularities.

Data Integrity Concerns

Within three hours of the program's phone number being used, the number was shut down without explanation. NDI contacted the mobile network operator, who explained that the number had been intentionally blocked and warned that any additional numbers used for this program would also be shut down. It appeared that program information and plans had been leaked to adverse parties, resulting in the shutdown of the account. Because NDI was unable to maintain access the mobile network, this program was not able to collect the intended information using the FrontlineSMS platform.

Actions to Protect Data

NDI and their coalition of partners anticipated the possibility of their program being shut down prior to implementation. Therefore, the team took several actions to ensure the availability for the program for voters to send reports regarding the election.



NDI created a backup plan in recognition of the threats listed above - rather than sending reports via SMS, people reported via phone calls. This plan was not as efficient as the intended election monitoring plan, but allowed for a reporting system to be in place. The creation of a backup plan reduced the risks associated with the interruption of the program and enabled NDI to continue to operate, even when it became clear that SMS would no longer be an option.

In addition, NDI advised their partners before implementation to set up the FrontlineSMS hub with multiple devices so that it could receive reports on multiple phone numbers, although this step was never taken. This could have allowed different cells to report using different numbers, so that even if one number is leaked and shut down, others can continue to operate.

Conclusion

There were very few actions NDI and the coalition could have taken to prevent the blocking of the election monitoring number and the shutdown of the program. Government infiltration of all opposition groups meant that information about the system and the data collected in itself was vulnerable to being compromised. In such situations, it should be anticipated that the number may be blocked and a backup plan, such as alternative reporting methods and multiple incoming numbers, should always be documented. Even if the backup plan does not operate as effectively as the FrontlineSMS platform, the goal is to provide a service that is available during the election period.