Web cam governance: The struggle within Panopticon.

On March 4th Russia will face a new round of elections, this time presidential. Many experts are focused on various aspect of political contest and discuss the increasing activity of those who oppose to the current prime minister and presidential candidate Vladimir Putin. However, what stays beyond the range of most debates is that the Russian elections are accompanied by most rapid construction of one of the hugest centralized surveillance systems in human history. The idea to cover the majority of polling stations by a network of web cameras was suggested by Vladimir Putin as a way to increase transparency and guarantee legitimacy of presidential elections. It can also provide a case study of how idea of electronic democracy can be abused. This article provides historical perspective to the emergence of the Russian web-governance idea, discusses the political sides of project webvybory2012.ru/ *and analyses the current Russian election through lenses of struggle between government-based surveillance and citizen-based counter surveillance that is mediated through information technologies.*

1. **Constructing vertical and webcam governance.**

Once upon a time, a governor came to meeting with president Medvedev to report about recent developments in his region. Russian president asked him about progress on building of new hospital that was funded by federal money and considered as, so called, "national project" (a special projects that defined as high priority and supported by Russian government). The governor responded that the construction moves forward fast and will be completed soon. Than president Medvedev turned the screen of his computer to the governor and he saw a picture of the web camera based live broadcasting from the construction site. It was empty…

One of the major challenges of the Russian government is controlling a big country. That's why the core idea of Putin's policy was constructing "Power vertical" as a system that enables full control of the entire country by the person on the top of the pyramid. For instance, as a part of this policy, the Russian president cancelled independent elections of governors, and replaced it with his appointments that were approved by local parliaments.

Still, the capacity of the person who seats in Kremlin to monitor and control the entire country was more than limited, and budget money continued to disperse in the regions. In this light, some of Russian officials planned to increase role of social media, not as a threat but also as opportunity to improve collection of feedback about what's happening in the country, especially in the regions. Bloggers and any other person who share information online can be seen as a human based network of sensors. Since people tend to use social media for sharing complaints and information about injustice, it can help central government to monitor local governments.

The Panopticon Model

The classical Panopticon model says that government follows citizens. The new model suggested that the central government can use the citizens as sensors to follow local government. As a consequence, some of e-government projects focused on the idea of collecting complaints from citizen. Additionally, the government expressed interest in tools that will be able to collect and analyse information based on social media. A special social media monitoring system was developed by one of Russian companies. It included an i-pad

application, that has compared information from social and traditional media around a particular topic, and that could also check “Negative” and “Positive” coverage.

Besides, Russian president Medvedev, who is well known as a fan of “i-gadgets” by Apple and Twitter, significantly increased his presence online, and started to get many complaints from citizens based on his blog and Twitter. Reaction to specific complaints from blogger or Internet user is also a populist tool that enables the leader to demonstrate that he follows the situation in his country and is personally involved in solution of problems.

However the most straightforward use of information technologies for empowering the “governance vertical” was deployment of an Internet based networks of sensors – Webcams. It started from surveillance focused on national projects, however, the first project that attracted attention used webcams for monitoring the reconstruction of villages destroyed by wildfires on Summer 2010.

Social Media Wildfires

The wildfires of summer 2010 leaded to increasing distrust of citizens in government. Fires heavily damaged few dozens of villages and few dozens of people died. Moreover, for many days Moscow was covered by smog. Complaining citizens also personally attacked Prime minister Putin during his visit to one of the villages.

In the beginning of august 2010 Prime Minister Putin announced that the entire country would be able to follow the reconstruction of villages through web cameras. It was not only a strategy to monitor and control construction, but primarily to improve the trust of people in government that was earlier highly criticized for its emergency response. The web cameras were introduced as a new ways to increase transparency and accountability.

During a meeting with victims of wildfires Putin said webcams were: “One of the most efficient methods of control – it’s 24 hours surveillance. Therefore I gave an order to place cameras on every significant construction site and three monitors: one in the White House (the Russian government compounds), one at my home, and one more – on the website of government.” Putin emphasized that it will allow to citizens to follow what happens on construction sites.[1]

Putin’s Order

Following Putin’s order, a special dedicated page was made on prime minister website, where anyone could follow one of 35 cameras in 28 villages. The cameras had night vision and could move around themselves.[2]

The system was used to show that prime minister keeps the situation under his personal control. The media called it “all-seeing” eye, referring Tolkien “The Lord of the Rings”, where the Dark Lord Sauron used “the all-seeing” eye for surveillance of the Middle-earth.

A Russian cartoon that was distributed online showed webcamera that is standing opposite to a picture of beautiful house in the middle of huge wildfires[3]. Some political expert claimed that a

technology for distant viewing under control of government creates a feeling that work is done and everything under state's control, while actually, the scope of reality that is represented by few dozens of cameras is very limited. Some of citizens argued that the cameras are distraction that is used to cover up for corruption and inappropriate usage of budget that was given for reconstruction. "The cameras should be place in the office of officials where they share money" – said on of online comments to article about the webcam project.

2. The networked Panopticon.

The real power of citizens, however, as a system of sensors that is able to perform large scale surveillance, was demonstrated not as a tool for monitoring local authorities or following reconstruction, but on very different occasion – election monitoring.

On December 4^{h} 2011 Russia voted for a new parliament. Following the election day an unprecedented amount information about falsifications, including many documents and videos footage was uploaded to Internet, distributed and shared online, as well as discussed by Russian liberal media. One of the users even created a YouTube watch list of 60 most popular falsification movies. The amount of evidences about falsifications reached some kind of tipping point, when a significant number of people shared the understanding that the elections were not legitimate. This understanding that was based on degree of online coverage of falsifications, were among major triggers to a wave of protests that started following the Duma election.

Actually, the fact that the government is using, so called, "administrative resource" and various techniques to "improve" the results was not a secret even in previous elections in 2008. What was really different this time is the extent to what information technologies enabled to document, visualize, mediate and distribute the real dimension of falsification to a wide audience.

Balance Of Power

The Panopticon model by Foucault provides framework to analyse the balance of power between those who conduct the surveillance in the centre and those who are surveyed. The power is built on the fact that the one in the center of Panopticon is able to see everyone, but those who are observed has very limited capacity to survey the center and no communication with other surveyed.

But what happens if the other side of Panopticon not only has the tools to follow the center, but is networked? It has a mechanism to exchange information and collaborate. In this case, the balance of power is shifted. The center faces not lonely citizens, but a powerful networked surveillance system with many sensors that are focused on the center of Panopticon.

In case of monitoring Russian elections the citizen based surveillance system was strengthened by a number of factors. First, technological progress provided better and less expensive sensors that are available for more citizens (primarily mobile phones). Second, the development of wireless and 3G networks enabled faster, almost real time sharing of information. Third, the Internet provided many platforms for sharing, distribution and analysis of this information

including crowdsourcing systems, blogosphere and social networks. Last, but not the least, the nature of general election process provides access to the observed event to almost anyone, since everyone has the right to participate in the process and therefore collection and distribution of information is much easier. All these factors together, as well as general frustration of people about the political situation, created motivation for participation in networked citizen-based surveillance system and leaded to significant power shift when the surveyed became more powerful that the state's institutions. As consequence, the government failed to protect the legitimacy of elections and avoid emergence of protests (More detailed analysis in an article "The other side of Panopticon").

3. The revenge of the sensors

The elections to Russian Duma, however, were not the last elections in the current political cycle. On March 4th 2012 Russian citizens will elect a new president. Based on the experience of parliamentarian elections, one of the major concerns of Kremlin is how to safeguard the legitimacy of the upcoming elections. For this purpose, the state has to restore the balance of power, that was challenged by emergence of citizen based networked surveillance system and reconstruct the Panopticon according to it traditional hegemonic structure.

This type of strategy can have two layers. On the one hand, it is focused on challenging the credibility and delegitimatization of the citizen based surveillance system. On the other hand, it should increase the capacity of state affiliated sensor system as the major source of credible information, and keep this system under full state control.

Challenging the citizen-based surveillance started even before the elections, when the credibility of crowdsourcing platform for monitoring elections "Karta Narusheniy" was under attack by pro-Kremlin movements and kartanarusheniy.ru the prosecutor's office started investigation against it (more details about attacks against Russian citizen-based monitoring can be found in article by Patrick Meier). Than, on the day of the elections, many spaces for sharing information, including blogosphere and liberal media websites were blocked by DDoS attack (there is no proof that attacked were initiated by government since it is always difficult to attribute DDoS attack with particular source, however, that's what a number of analysts believe, for more detailed analysis please check an article by Alexey Sidorenko). That can be seen as an effort to limit the power of the other side of Panopticon through damage to its capacity to share information that was collected through sensors.

About Falsifications

But, perhaps, the most significant delegitimization effort was done after the elections, once the government realized how significant was the influence of the citizen-based information about falsifications or electoral fraud. On February 4th the official representative of Russian Investigation Committee Vladimir Markin made a statement about ongoing investigation of the online election fraud movies. He stated that the majority of falsification movies were falsified. Moreover, according to Markin, "all the movies were distributed from the same server in California". The Russian investigator didn't mention the name of server, but most of the Russian journalists concluded that he referred to YouTube (which is obviously a nonsense, since the fact that YouTube servers are in California, doesn't mean that the videos origin is in California or that it was uploaded by someone in California).

Weakening the other side of the Panopticon, however, is not enough, especially if the political system is facing presidential elections. The legitimacy of presidential elections in this case is not less important than the result of these elections.

Putin Talk

A few days after the elections, in a TV show "A talk with Vladimir Putin" the Russian prime minister offered to put web-cams on all polling stations all over Russia. He explained that the country should see what happens at every polling box, as a way to eliminate fraud as well as to minimize the capacity to argue after the elections that the voting process wasn't fair.

Putin's response to the increasing power of the other side of Panopticon was the construction of a new Panopticon, which is probably the biggest centralized surveillance system in human history, especially if you take into account that it had to be constructed in the biggest country in the world in just few weeks.

However, the idea is not the creation of a simple surveillance system just to monitor the election, but the construction of a system that will significantly increase citizen's trust and elections' accountability. Therefore, unlike the classical Panopticon, in this Panopticon the citizens have access to the governmental network of sensors. Actually, the citizens' view is embedded within a network of sensors that is created by government. The power of citizen's gaze is co-opted by government, based on the state's protocol of surveillance.

Indeed, the scale of this project was unprecedented for ICT development. At the beginning, Putin set up a special website where experts and citizen could brainstorm how to create the surveillance system. But than, the website "Technology of election web-monitoring" was closed due to the urgency of task and the project was given without tender to the state's telecommunication company "Rostelecom".

A Challenging Mission

"Rostelecom" got a very challenging mission. Russia has around 95 thousands polling station. According to the project the majority of stations (except around 1500 sensitive places like jails, hospitals or military bases) should have two web cameras. On camera should be focused on polling box and another camera to give general picture of the polling place. After the end of voting, one of the cameras should also broadcast the counting of voting.

The budget is at least 13 billion rubles (around half billion dollars). An average price of every computer+camera set is around 26.000 rubles (almost 1.000 dollars). However, the most expensive part of the project is development of infrastructure that allows to connect all the stations, including cables deployment and satellite-based Internet. The web cameras should be placed in most remote places in Russia, e.g. Kuril Islands.

In addition to the digital divide and lack of infrastructure, one of the most significant challenges it the capacity of the Internet network to survive simultaneous broadcasting of 90.000 live web-cameras, when the potential audience includes dozens of millions of Russian citizens. The required capacity of the system was defined as 25 million users and a maximum of 60 thousand viewers for one camera. Russian ministry of communication found a solution that might help to limit the Internet traffic. Those who interested in following the elections through webcams

should not only register in advance, but also create a list of the polling stations that they would like to follow. There is no limit on how many stations one can add to his watching list, but he can't select all 90.000+ stations by one click. According to Russian officials, this arrangement will help to know where the peak of traffic is going to be expected and prevent collapse of the system.

"It is possible to accomplish this mission, but it's very difficult", - concludes Ilya Massuh, the deputy minister of communication given the task by Putin. Indeed, there is no doubt that the this is an amazing project from the technological point of view. It could make a significant contribution to reduction of digital divide in Russia. However, the value of this project for election monitoring and making the process fair and open should be questioned.

4. The distortions of webcam reality

When citizens documented fraud through their mobile phones, they could not only share it online, but also immediately complain about the incident. In the case of webcam-mediated surveillance one of the major features of the process is remoteness. But what happens if someone watches the webcam and sees something that raises his suspicion? Now he cannot complain, and he also can't take this video and share it with others.

And what if the person wants to get the footage of particular incident that he saw online? According to regulations, all the video recordings will be kept for one year in special databases also developed by Rostelecom. However, who will be able to request this video and how is not clear. According to some official sources, the access to the database will be allowed only after specific bureaucratic procedure that will include verification of identity of a person who requested the video. Other sources argue that only Parliament can decide how access to the database will be regulated. And even if a person will get access to data, it's not clear how he will be able to share it, and if the Russian court will recognize the webcam based video as evidence.

Another gap of webcam based election monitoring is its limited capacity to identify fraud in the first place. Many experts question if this system can identify the most common and most significant violations. According to Russian sources the majority of violations were made by manipulation with protocols of voting, or by multiple voting by the same people. Both types of violations can't be identified through webcams. A well-known oppositional blogger Malgin writes: "The falsification took place out of the territory of polling stations. It is clear, why it was so easy for Putin to announce the webcam plan. You can't catch anything with webcams. You can fill all the station with cameras, but you wouldn't see how they draw the numbers on the top level."

Malgin suggests another explanation why web cameras are good for fraud. It can be used as justification to remove the real observers from the polling station. Another oppositional blogger, Oleg Kozlovsky suggested, that requirement to create in advance watch list can help to map the polling station that won't be followed by anyone. As a response Kozlovskiy offered to divide surveillance between various online teams and coordinate it in a way that will guarantee that no station will be left without attention.

That's Entertainment

The webcam system can also play a role of distraction, when people chose to stay home and follow the webcams, but not going outside and being offline observers. At the same time, the huge number of available cameras makes difficult focusing on particular place. Information overload reduces the efficiency of surveillance. Finally, the webcam based monitoring with more than 90.000 cameras turns to be one huge reality show, while the surveillance is approached by many more like entertainment, than fulfilling a function of observer.

The system also raises some significant questions about privacy. The fact that the state is going to hold database with video footage of the voting process in the majority of polling stations might suggest some very unpleasant scenarios.

Finally, many claim that the project's true motivation is not political, but financial and it's just another corruption story around the state's budget (or waste of money in best case). The fact that half billion dollars spent in just few weeks without any tender indeed raise some question about transparency and accountability of Russian government.

But probably the most significant point of critiques related no to the capacity of web-cameras to monitor elections, but how this project is going to be used as a part of official narrative following the elections. One the one hand, cameras can be used as one of the major argument in favor of fairness of elections, since allegedly web-cameras guaranteed transparency of voting process.

But, even more concerning is that it can be used to delegitimise protests against the election results and any oppositional activity. This point was well presented by an expert from National Politics Center at Moscow State University Grigoriy Trofimchuk. At the public debates about the role of the webcams, that was sponsored by government, he explained, that webcam monitoring system makes to non-legitimate any type of public protests against election results and police shouldn't allow any demonstrations following the elections. Otherwise, he says "spending 13 billions of rubles for deployment of webcams was a waste of money".

5. **Hybrid surveillance system.**

A founder of Russian most popular search engine "Yandex" Ilya Segalovich suggested a solution that could significantly increase the capacity of web cam system to contribute to real election monitoring. Segalovich suggests monitoring system that will be based on network of webcams and network of citizens' mobile phones. According to him, the two networks of sensors have different capacities to follow different type of incident and violations. Therefore the monitoring system should include mechanism that allow information exchange and collaboration between those who monitor elections on ground based on mobile phones, and those who follow elections from home based on web cams. Segalovich also suggested creation of special mobile application "Observer's notebook", that will simplify monitoring for any voter. Indeed combination of two types of sensors looks like ultimate solution. The only problem that it doesn't look that a system that can really increase transparency around elections and catch more falsifications, is something that the Russian government is interested in. At the same time, the idea of Segalovich inspired development of mobile application for monitoring elections by a group of volunteers.

Conclusion: three dimensions of sensors.

The Russian webcam election-monitoring project will probably find its way to the books of Internet history as one the most large-scale ICT construction projects that created the biggest online Panopticon in the biggest country on the Earth in the shortest period of time. In addition to this fact, however, this case study suggests 3 angles for analysis for construction of ICT based surveillance system by state actors: manipulation, power struggle and governance.

First, the **webvybory2012.ru** project demonstrates how information technologies can be used for the construction of fake transparency, fake accountability and fake legitimacy.
The state gives controlled access to citizens to its system of sensors in order to increase trust. But are citizens ready to trust the states' system of surveillance? The result of this strategy might be quiet opposite if next day after elections, the officials will try to use the Webcam project as proof of legitimacy and justification for limitation of protests against elections' result. It might only contribute to tension.

Manipulation with information technologies as a way to send a message that everything is under control can substitute for real action and real reform. However, in the new information environment, attempts to conduct manipulation based on ICT can be exposed and opposed by using the same technologies. In this case the new Panopticon can follow Carthage – it has to fall.

Second, the situation around Russian Webcam project enables us to follow a new type of struggle for mobilization of networked power in ICT enriched environment. Information technologies enable the emergence of a new kind of networked surveillance power that is based on interconnected system of sensors and people. This surveillance power can be used against the state. As a response, the state makes an effort not only to limit the new counter-power, but also harness it within its own system of sensors. There is also third path, when the citizens and state create a new mode of collaboration, around a particular goal as it was described by Segalovich, but in this case both sides should truly share the same goal.

The struggle around mobilization of networked power is a process that takes place on many grounds and the surveillance is just one of them. Which side of Panopticon will win? Will the state be successful in distracting the networked power from independent bottom up network of sensors and harnessing it within its own constructed surveillance system? There is no clear winner. It is an ongoing struggle, but one might claim that the capacity of a vertical system to conduct top-down mobilization of horizontal structures is more than limited.

The third angle for addressing the Russian webcam election-monitoring project is role ICT for governance. Cybernetics argues that the survivability of a system depends on its capacity to get feedback, including negative feedback that requires reconsideration of policy and action. Russia has a significant functional problem in controlling the state. The attempts to construct vertical doesn't really improve the governance capacity.

ICT can definitely help to improve control, including collection of feedback and incorporating it in decision making. What we can however see in Russian case is how the control is replaced by imitation of control. In this case ICT is used to construct the imitation and images, but not really improve the governance capacity and degree of statehood.

The system that should be able to collect feedback and translate it to decision making is replaced by a construction of an image of system that is able get feedback and respond to it. The webcam project isn't really a project that is created by government to get more information about election process. It's a huge sensor system that constructed in a way that feedback can't be really collected and certainly can't make impact on the system. It is a sensor system that was created for one purpose – maintenance and protection of status quo.

What should improve capacity to get negative feedback, eventually contributes to positive feedback, since it's constructed in way that should support the decision that were made. It is interesting that surveillance system that is based on ICT can be constructed in a way that will produce positive feedback, and block negative feedback. The Russian webcam system doesn't really created for monitoring reality, but construction of reality.

At the same time, citizen-based bottom up horizontal sensors system are able to provide a constant flow of negative feedback. However, traditional institutions ignore this feedback since it challenges their political interests. Eventually, according to cybernetics, a type of governance that ignores negative feedback, might lead to a collapse of system, or at least to increasing gap between citizens and the state.

The effect of this gap is not only to decrease legitimacy and trust. The collective surveillance and information sharing mechanisms not only contribute to capacity of citizens to follow the situation, but also to self organize and respond to it. It might mean, that the more the traditional institutions' capacity to govern is limited, the more networked society is powerful both in protesting against these institutions as well as providing alternatives to the lack of real action by the government.