Autocratic Adaptation*

The Strategic Use of Transparency and The Persistence of Election Fraud

Fredrik M Sjoberg†

First Version: March 22, 2012
Current Version: June 30, 2012

Abstract

Why would an autocrat want, or at least make it appear to want, to reduce election fraud? In recent years, non-democratic rulers have surprisingly begun to embrace fraud-reducing technologies, like web cameras or transparent ballot boxes. The reason for this is not found in international norms or domestic conditions for post-electoral protest, but rather in the null effect on the ruling party vote share. With the help of new fraud identification techniques, I argue that the installation of web cameras in polling stations changes how fraud is conducted. Web cameras do not reduce fraud, but rather make certain blatant forms of fraud, like ballot box stuffing, more costly. Autocrats then substitute for other types of fraud, such as fabricating vote count outside the view of the cameras, in order to secure electoral victory. Overall, this paper identifies this compensation mechanism where incumbents are able to prevent vote share losses, while contributing a veneer of legitimacy by self-initiating anti-fraud measures.

JEL Classification: P16 (Political Economy), D72 (Political Processes and Rent-Seeking), D73 (Corruption)

Keywords: Autocratic Adaptation, Institutions, Election Fraud, Ballot Stuffing, Vote-Count Fraud, Fraud Forensics, Digit-Based Tests, Election Monitoring, and Web Cameras.

Introduction

Why would an autocrat want to reduce election fraud? It seems counter-intuitive that autocrats would voluntarily deny themselves such a useful electoral tool. As of late, a large number of non-democratic states have embraced new anti-fraud technologies. For instance, in the most recent 2012 Russian presidential elections, web cameras were installed in polling stations across the country, in what authorities have labeled as a unique transparency initiative.[1] Countries like Pakistan and Albania are also reportedly considering polling station webcams. In order to understand this seemingly paradoxical emphasis on electoral integrity in a less than democratic regimes, we need to understand the menu of manipulation available to political actors (Schedler, 2002).

There is a range of institutional setups that have been adopted throughout history in an attempt to increase the integrity of elections. The secret ballot (Bertrand et al., 2007); independent electoral commissions (Eisenstadt, 2004, Lehoucq, 2002); centralized counting, transparent ballot boxes, and different forms of monitoring (Kelley, 2012, Hyde, 2011) are all examples of 'institutions' that structure electoral behavior. Altering the institutional setup in which elections are organized often occur in contexts where there is competitive pressure for reform (Acemoglu and Robinson, 2006, Przeworski, 2009). All such reforms are associated with both benefits and costs to the ruling party. The benefit to the ruler relates to trust in the electoral process and the prevention of possible post-electoral challenges. The costs arise from not being able to use a particular form of manipulation anymore. Regimes vary in how much they need voters to trust the electoral process and how dependent they are on a particular manipulation technique. For instance, independent electoral commissions increase the trust by ensuring impartiality in the administration of the elections. Electoral management bodies that

---

† Postdoctoral Scholar, New York University, fredrik.m.sjoberg@gmail.com.
* Acknowledgement: For helpful comments thank you Joshua Tucker, Henry Hale, Bernd Beber, Cyrus Samii, Andrew Little, Jonathan Mellon, and David Szakonyi. I also thank Erik Herron for graciously sharing his data.
[1] The Central Election Commission Chair, Vladimir Churov, even went as far as suggesting that this technology should be adopted in United States and other democracies in order to increase the trust in the process.

are independent from the ruling party also means that voter registration, distribution of voting materials, tabulation and aggregation of results cannot be manipulated. A capable autocrat might not fear an independent electoral commission since there are other components of an election that could still be manipulated.

The threat of revolution often compels ruling parties to make piecemeal reforms that increase the integrity of the electoral process. Each of these interventions can result in perverse side effects when the ruling party adapts by re-calibrating the use of manipulation techniques. After all, ruling parties are in the business of winning elections. The argument in this article is that institutional reforms can have unintended consequences and capable autocrats are well placed to reduce the potential downsides associated with certain democratic reforms. The overarching question about why autocrats want to reduce fraud by adopting fraud-reducing institutions is therefore inherently linked to the adaptive capacity of the regime. An intervention that is supposed to increase the integrity of the electoral process might be embraced simply because the negative effects can be dodged by using other forms of manipulation.

The puzzle in this article concerns why regimes that do not face a direct revolutionary threat nevertheless adopt fraud-reducing institutions. The particular focus is on election monitoring and especially on the use of new information technology to improve the transparency of elections. Perhaps the ruler realizes that adhering to international norms is associated with material benefits and therefore allows for monitoring (Hyde, 2011) Another theory is that monitoring is allowed for since voters have started to discount the inflated vote totals (Little, 2011). The latter theory assumes that monitoring improves the signal of strength that winning elections otherwise entails. Both of these theories assume that monitoring reduces fraud. These theories all contribute to our understanding of the paradoxes of democratic monitoring in autocracies. However, what if the answer is simply that monitoring is allowed for and even pro-actively embraced due to its negligible effect on the electoral outcome? Monitoring might reduce one type of fraud, but this could theoretically be compensated for by the use of another, less detectable, form of fraud. This is what I mean by autocratic adaptation. Here monitoring is an efficient way for an autocrat to realign the incentives at the micro-level, where votes are cast and counted.

Exposing election officials to monitoring incentivizes them to get votes through less detectable, perhaps equally fraudulent, means.

In order to fully understand why an autocrat would pro-actively embrace monitoring we first need to know the micro-level effects of such interventions. The question is therefore: what are the effects of webcams on the micro-dynamics of fraud? As a particular monitoring technology, web cameras capture only a small fraction of activities within a polling station, opening up the possibility that while blatant ballot box stuffing is reduced, other fraudulent practices go on unabated, or even increase. This way, the ruling party incumbents perpetuating fraud may not necessarily be punished in terms of votes and thus escape any potential negative consequences of monitoring. The capacity of autocracies to adapt can explain why monitoring is so widely accepted. If an autocrat that invites election observers or installs webcams can adapt by having local officials deliver the vote by other less detectable means, then monitoring can be considered essentially cost-less for the ruler. In theory it would therefore make sense for an autocrat to adopt such a technology since it can only benefit them by appearing to be sincere in their efforts to improve electoral integrity.

Explaining the puzzle about why autocrats would embrace monitoring requires two important steps. First, we need valid and reliable measures of election fraud. In existing literature, statistical proxies like turnout and vote share of the ruling party have been used, but require non-negligible assumptions (Hyde, 2007, Hyde, 2010, Herron, 2010). Recently developed fraud forensics techniques can provide a good complement by getting directly at vote anomalies (Beber and Scacco, 2012). Second, we need an identification strategy that allows us to draw causal inferences in a context where monitoring is not randomly assigned. Without accounting for the biases in terms of how a particular monitoring technique is being applied, we run the risk of biased estimates and arriving at simply incorrect conclusions.

When subjected to a web camera that streams live footage from the polling station, blatant fraud such as ballot box stuffing should be deterred since cameras can easily capture the violations. That is, we should observe a reduction in turnout in polling stations with a webcam installed. The easiest compensation for this reduction in votes is to simply manipulate the vote count, often times outside the purview of video camera, and hard to accurately identify on screen. Vote-count fraud as evidenced by last digit deviation from what can be expected under conditions of a clean count should therefore increase in the presence of a webcam. This possible compensation mechanism, in which one type of fraud is replaced by another may not lead to any negative effects on the ruling party vote share at the precinct level.

The article begins by presenting some theoretical considerations based on the literature on election fraud and election monitoring. I then devote considerable attention to methodological concerns, both in terms of identification and measurement of election fraud. To provide support of my hypotheses, I utilize polling station level data from the 2008 parliamentary elections in Azerbaijan, the first ever case of large-scale web camera deployment. In contrast to previous studies that failed to account for how web cameras were allocated, I show that web cameras were installed in polling stations less prone to election fraud. Understandably an autocrat might hesitate to expose blatant fraud and therefore opt for selectively allocating webcams to less fraudulent precincts.

In the 2008 elections in Azerbaijan, I show the magnitude of the webcam effect is a 7-percentage point reduction in officially reported turnout. This reduction, it is argued, comes from less ballot stuffing in the presence of web cameras. Interestingly I find more miscounting of ballots and therefore more outright fabrication of the results in the webcam-monitored precincts. As a consequence of this compensation mechanism, there is no effect on the vote share of the ruling party in polling stations with a camera. The theory developed shows that authorities adjust their fraud strategies in the presence of a particular monitoring technique; one type of fraud is simply replaced with another form of fraud. The article finishes with some practical implications for the study of elections in non-democracies, including warnings about relying on technology-driven quick fixes to problems of electoral integrity.

Theoretical Framework

Manipulation of the electoral process is widespread in authoritarian states (Levitsky and Way, 2002, Levitsky and Way, 2010, Diamond, 2002, Schedler, 2002, Schedler, 2006, Simpser, 2012). This manipulation comes in many forms, of which outright fraud is only one. Conceptually, election fraud can be understood as illegal efforts to shape election results (Lehoucq, 2003). This is distinguished from other forms of unfair interventions like intimidation or the use of administrative resources that might or might not be illegal. Even more narrowly, by 'election fraud' we here only refer to such illegal efforts on the day of the election itself. Efforts to skew the electoral process can naturally take place during any time of the electoral cycle, ranging from the pre-election campaign, election day, to post-election counting (Schedler, 2002). The concept of electoral manipulation is used for this broader category of techniques that autocrats use to control the electoral process, such as restricting who can run for office, controlling the media, and vote buying. All forms of manipulation are associated with a cost as well as a benefit to the incumbent ruler.

In terms of the benefits of fraud it has been argued that fraud is mostly used in competitive elections by incumbents in order to secure victory (Nyblade and Reed, 2008, Greene, 2007, Lehoucq and Molina, 2002). Here fraud is used in order to win in elections that otherwise might have been lost. Others have argued that this is not empirically true, and that all sorts of manipulation occurs even in noncompetitive settings (Simpser, 2012). In noncompetitive cases fraud and other forms of manipulation are perhaps better understood as a way to deter future challenges. By delivering a fraudulent supermajority authorities signal their capacity to dictate the outcome (Wedeen, 2008, Simpser, 2012). If authorities are able to pull of a fraudulent supermajority then oppositional candidates essentially are discouraged from participating in the process in future elections. Participating in such a blatantly fraudulent process would clearly be futile.

Fraud is also associate with a cost for the ruler since it might provoke protests (Dahl, 1971, Hyde and Marinov, 2011).[2] As has been argued the threat of revolt is what makes democracy self-enforcing (Fearon, 2011). Knowledge about blatant fraud can galvanize anti-incumbent sentiments and essentially act as a focal point for overcoming collective action problems associated with protesting (Tucker, 2007). Reducing detectable forms of fraud could therefore be

[2] 'In terms of domestic costs, the main variable of interest is post-election protest' HYDE, S. & MARINOV, N. (2011) Information and Self-Enforcing Democracy: The Role of International Election Observation.

a sensible thing for an autocrat to do. This is the context in which fraud-reducing institutional experimentation has taken place. Fraud can help the incumbent win elections, but it can also provoke a backlash, especially in more competitive cases. In noncompetitive cases, however, it is still puzzling why the ruler would want to reduce fraud since the supermajorities that it can produce can be an effective deterrent of oppositional challenges.

The development of the institutional framework for the conduct of free and fair elections has historically been the outcome of a protracted battle between different interests (Acemoglu and Robinson, 2006, Mozaffar and Schedler, 2002)).3 Democratic reforms get enacted in competitive settings where there is a threat of revolt. This applies to the expansion of suffrage (Przeworski, 2009); the establishment of independent electoral commissions (Lehoucq, 2002); etc. The demand for such institutions is simply not there in less competitive regimes. This is not to say that non-democratic rulers prefer to win by force or by rigging elections (Lust-Okar and Jamal, 2002). As noted by Huntington in 1991, in reference to Pinochet's Chile 'If the government's candidate wins everyone will say it was fraud. If he loses everyone will say it was a fair election. So it is more in our interests than anyone else's to be able to show it was an absolutely fair election'.[4]

Establishing an institutional framework where the transparency of the electoral process is increased can be a good way to increase trust in the process. However, rooting out old electoral malpractices can be difficult for even the most capable autocrat. Even if the ruler genuinely wanted to reduce blatant fraud there is no guarantee of the bureaucratic capacity to do so, especially in a context with a long history fraud. Establishing autonomous third-party actors, like independent electoral commission or election monitors, can help re-align the incentives at the local level. What the ruler does not want to do is to allow for genuine competition. Fraud reduction should therefore ideally take the form of only marginally affecting fraud, and above all the more detectable forms of fraud. A manipulation technique that is detectable is inherently more expensive to the ruler than one that is not detectable (Birch, 2012). For instance

[3] 'New electoral institutions are chosen under the pressure of political uncertainty surrounding regime transitions.' MOZAFFAR, S. & SCHEDLER, A. (2002) The comparative study of electoral governance - Introduction. *International Political Science Review,* 23**,** 5-27.

[4] Quoted in HYDE, S. & MARINOV, N. (2011) Information and Self-Enforcing Democracy: The Role of International Election Observation..

manipulation of voter registration is not necessarily as detectable as ballot box stuffing on election day. This is not to say that capable autocratic regimes could not handle the cost associated with being caught conducting fraud.

The ideal setup in terms of electoral institutions in a noncompetitive autocracy should fulfill the following criteria. First, signal democratic credentials to both domestic and international audiences by making it appear that fraud is being reduced. Second, allow for less detectable forms of fraud to continue (or even increase) in order to continue delivering supermajorities that would deter future challengers.

Having considered the benefits and cost of fraud it is now time to consider the role of monitoring in the larger game of electoral manipulation. In the literature it has been suggested that the ubiquity of monitoring is indeed puzzling (Hyde, 2011, Kelley, 2012, Little, 2012). What makes widespread monitoring puzzling, especially in noncompetitive regimes, is the fact that the ruler would voluntarily take such a useful technique, fraud, off the table, After all, it is in the interest of the incumbents of any regime to inflate their own popularity. In order to understand this puzzle we need to understand the electoral cycle as a whole and the role that different forms of manipulation can play in different stages of the process. As noted above, perhaps relying on rigged elections is not the best way to win, even for a strong autocrat.

Much of the literature on the spread of monitoring has focused on the international dimension (Hyde, 2011, Kelley, 2012). In this literature the international audience takes note of fraud and punishes the regime by denying aid and other international benefits (Hyde, 2011). The argument is that international norms of free and fair elections have spread throughout the world, thus making blatant fraud more costly. The spread of these norms have also made it costly to deny monitoring. Others argue that there might be a domestic logic to the deployment of fraud-reducing technologies. Monitoring might make sense for the autocrat since it improves the signal of strength that an electoral victory otherwise is associated with. If the citizenry knows that fraud is widespread, then by allowing for monitoring the expectation about how much fraud occurs can be reduced (Little, 2011). That is, voters who know that an election is observed think that there is less fraud, compared to a situation with no monitoring. What all these theories have in common is that monitoring reduces fraud and that this punishes the incumbent (Hyde, 2011, Kelley, 2012).

This article presents a novel argument, namely that some forms of monitoring are essentially cost-less for the ruler and therefore the deployment of such is a no-brainer. Contrary to earlier theories about monitoring I here suggest that passive monitoring in the form of web cameras do not reduce fraud. The argument is that autocracies adapt and that there is elasticity to fraud. A particular type of fraud might well be reduced in the presence of monitoring, but another type of fraud might increase as a consequence. In such a context monitoring could conceivably be cost-less to the ruling party. This being the case the autocrat can only benefit by publicly embracing monitoring, since the public perception about the integrity of the elections, both domestic and international, is affected by the willingness to monitor elections. As has been argued elsewhere, certain monitoring techniques, like domestic observers, may displace rather than remove irregularities. In Ghana, for example, the rate of increase in voter registration is lower in registration centers where domestic observers were stationed (Ichino and Schundeln, 2011). Some of these deterred registrations spilled over to nearby electoral areas, i.e. manipulation efforts were simply displaced in the presence of monitoring. Cross-national studies have also shown that election monitoring has a measurably negative effect on the rule of law, administrative performance, and media freedom (Simpser and Donno, 2012). The explanation for this observed pattern is that monitoring induces incumbent rulers to resort to other less detectable forms of manipulation as compensation. These so-called compensation mechanisms are triggered whenever a particular form of monitoring is deployed. The elasticity of fraud can therefore explain why certain interventions, like webcams, are rather harmless for an autocrat.

In terms of improving electoral integrity, it should be noted that only a handful of countries do not allow for active monitoring of voting and counting. Monitoring, however, comes in many different forms and the intensity of the monitoring 'treatment' varies. Political parties are usually the most active actors, in this regard, as party representatives set up shop at polling stations. Foreign-funded domestic NGOs are also used in many countries, in some instances randomly assigning observers to polling stations. Most of the literature has focused on international observers and their effects (Hyde, 2007, Hyde, 2010, Hyde, 2011, Simpser and Donno, 2012, Kelley, 2009, Kelley, 2012). More recently experimental work has been conducted with domestic observers as the treatment (Sjoberg, 2012). The literature does indicate that active monitoring in the form of observers has an effect on electoral returns, suggesting that fraud might be reduced in the presence of observers (Hyde, 2010, Sjoberg, 2012). Of particular interest in this article is the phenomenon of pro-regime monitoring initiatives. The first ever ruler to embrace web cameras as a monitoring technique was Azerbaijan in 2008. An earlier study found a consistent negative effect on turnout in polling stations that had a webcam installed, but interestingly no effect was found on the ruling party vote share (Herron, 2010). As we will see, the theory and empirical evidence presented in this article reconciles these seemingly paradoxical findings.

Hypotheses

Based on the theoretical overview we have arrived at the following specific research hypotheses in terms of the effects of web cameras.

> *H1*: Web cameras reduce ballot box stuffing and other forms of fraud detectable by webcams.

Ballot box stuffing is one of the most important historical forms of electoral fraud (Lehoucq and Molina, 2002). Numerous reports from the post-communist region suggest that it has been a widespread phenomenon throughout the region.[5] Ballot stuffing is clearly a form of fraud that is webcam-detectable since the webcam is focused on the ballot box during voting. Any attempt to place multiple ballots through the narrow hole in the box would require some extra effort and could thus be detected by the camera. Ballot stuffing is best measured by focusing on the absolute number of ballots in the box at the end of election day. The best available measure for this is turnout.

---

[5] See OSCE/Odihr election reports since 1990s.

As a practical matter the vote count starts with opening the ballot box and counting the total number of ballots in the box. Only after this are the votes separated into piles for each candidate and counted. Earlier in the day, parallel to voting, an individual from the election commission is assigned with the task of keeping track of how many vote and these numbers are compared at the first phase of the counting stage. If ballot box stuffing occurs it is conceivable that the person keeping track of the total number of voters would add these fictional voters to the tally during the day. The most likely scenario is therefore that the total number of ballots in the box, the turnout metric, is not falsified, but rather the votes for individual parties.[6] Turnout is therefore a good approximation of ballot box stuffing in the post-Soviet context, where there is a long history of turnout-enhancing fraud (Myagkov et al., 2009).

Theoretically there are also other forms of webcam-detectable fraud, like forced voting and multiple voting. For multiple voting to be deterred by webcams they would have to provide enough focus for racial recognition and therefore discourage people from showing up more than once. On the other hand, if multiple voting is organized in a way that 'busses' voters from one polling station to another, then webcams would not deter from it. Finally, forced voting should also be deterred by the presence of a webcam, but it would be difficult to measure without examining all the webcam footage in detail.

There are also other forms of fraud that are not necessarily webcam-detectable, like the completion in of the final protocols, and especially the specific vote count for each party. Consequently,

> *H2*: Web cameras increase the occurrence of vote-count fraud and other forms of fraud <u>not</u> detectable by webcams.

Installing a webcam in a polling station could potentially increase fabrication of vote totals. The logic here is that the ruling party and its local level loyalists want to compensate for the

[6] There is only limited evidence of this, but the author has witnessed firsthand (Armenia, Kazakhstan, Kyrgyzstan) how the total number of ballots in the box was first verified and recorded in the presence of all commission members, party representatives and observers. Only after having recorded this number the chaotic process of counting of party votes began.

reduction in ballot stuffing (*H1*). The underlying assumption here is that there exists an informal quota for delivering a particular vote share to the ruling party. Miscounting the ballots or tampering with the protocols out of the view of the web camera is an efficient way to compensate for not being able to stuff the box earlier in the day. Other ways of compensating for the loss due to less webcam detectable fraud (*H1*) would be to engage in manipulation outside the polling station, like vote buying, carousel voting, or intimidation.

Given that monitoring reduces one type of fraud (*H1*) and increases another (*H2*) we arrive at the final hypothesis about the relative effect on the ruling party vote share,

> *H3*: Web cameras do not necessarily have any effect on ruling party vote share, at the precinct level.

At first one might expect an anti-fraud technique, like webcam monitoring, to also reduce the vote share of the ruling party. This is based on the wrongful assumption that fraud perpetrators only have a limited set of manipulation tools at their disposal. Here we argue that blatant fraud in the form of ballot stuffing only constitute one part of the fraud toolbox (*H1*). A non-democratic ruler can utilize a whole range of techniques to ensure that they get the desired vote share. As already argued, local officials that are exposed to web cameras might compensate for scrutiny of stuffing fraud with either vote-count fraud (*H2*) or with measures taken outside the polling station, like vote buying or intimidation. An anti-fraud intervention, like a webcam, thus pushes up the relative cost of one type of fraud, and thereby incentivizes incumbent loyalists to attract votes by other means. There might be both over- and under-compensation in the presence of webcams, but these effects would equal out and produce a null effect when analyzing all of the monitored precincts.

Research Design, Case Selection, and Data

In general, studies of election fraud are based on either single-country case studies using ethnographic work, memoirs, formal complaints and legal cases, or cross-country comparisons using expert assessments on the electoral process. Only a few studies have used micro-data from polling stations, and here mostly focus on turnout anomalies as a proxy for fraud or ruling party vote shares. I complement these approaches with a direct measure of vote-count fraud: digit distribution tests. To my knowledge, the new digit-based approach has not been used before in an explanatory study.

The effect that we want to estimate derives from the webcam treatment. In the context of Azerbaijan web cameras were installed in around ten percent of the precincts. Cameras were set up in such a way that they would capture what happened inside the polling station. There was no audio capability and therefore whenever there was commotion inside the precinct there is no way to determine what the argument was about. Anyone could watch the supposedly live-streaming video footage by going to the Central Election Commission website.[7] From the description above it is clear that this form of monitoring was completely controlled by the authorities. Authorities decide where to allocate web cameras and they also provided the web platform for showing the footage. In this sense web cameras, as a monitoring technique, are very different from high-quality election observers, where authorities have no control over the 'treatment'.

Using micro-level official electoral returns and knowledge about the exact placement of web cameras allows us to statistically estimate the effect. Azerbaijan is an ideal case for considering rampant election fraud in recent elections. As noted by other scholars in the field, the ideal case study for monitoring would be 'an election with clear-cut cases of blatant election-day fraud' (Hyde, 2010). The reason here is that in the absence of polling station level fraud the fraud-reducing effect is impossible to estimate. Azerbaijan is a non-competitive dominant party regime where the opposition is marginalized and unable to use fraudulent techniques. The findings of this paper do not necessarily apply to more competitive contexts where there is less fraud or where both the opposition also can use fraud.

In any case, Azerbaijan being the first country in the world to install web cameras make it an important case. Azerbaijan is furthermore a good case because there is both a control group with no web cameras and a treatment group to analyze the differential effects. In the 2012

[7] No information was provided as to the number of viewers that actually used this opportunity.

presidential elections in Russia, there is no such variation, since web cameras were installed in all polling stations.

Azerbaijan is one of three former Soviet republics situated in the South Caucasus. The Aliyev family has dominated politics for most of the last 20 years, capitalizing on an abundance of oil and gas resources that have been extracted since the days of Alfred Nobel in the late 19th century. The country has a history of fraudulent elections: in 2005 the parliamentary elections were considered substantially flawed (OSCE, 2005), while the 2008 presidential election saw Ilham Aliyev, whose father also served as president, re-elected for a second term by a landslide victory with nearly 90 percent of the vote. Taken together Azerbaijan is thus a non-competitive authoritarian state with a history of flawed elections. However, it should also be noted that since the 2000 parliamentary elections authorities have selectively clamped down on the fraud by invalidating results from certain polling station, rescheduling new elections in some constituencies, and by prosecuting election officials (OSCE, 2006, OSCE, 2001). Installing web cameras is therefore not necessarily as counter-intuitive as it first might seem in a case like Azerbaijan. Officially the introduction of cameras was to improve the transparency of the elections and the increase public confidence in the process.[8]

The main challenge in terms of research design is to account for the fact that the investigator did not control the assignment of precincts into a treated group (camera monitored precincts) versus a control group. In the empirical analysis, I account for the fact that web cameras were not randomly allocated by utilizing matching based on a set of strong observables. This means that we voluntarily restrict our data to include only polling stations that can be considered roughly equal on all relevant dimensions, apart from the fact that some were assigned a web cam and others were not.

Matching as such does not solve all the problems associated with non-random assignment of the treatment. Herron, in his analysis of the 2008 elections used optimal matching based on covariates from the 2008 same election, instead of looking at pre-treatment factors. By using

[8] 'Rules on installation and use of web cameras in election precincts', CEC decision 27/132, October 8, 2008.

historical covariates on turnout and competitiveness, I can instead reduce potential biases. What if web cameras were installed in precincts with lower historical turnout? In such a scenario the negative turnout effect that Herron reports might not be an effect at all, but simply due to a bias in terms of allocation of webcams. In terms of identification strategy, it is thus crucial to account for any possible biases in terms assignment of web cameras. As noted by Holland, 'for causal inference, it is critical that each unit be potentially exposable to any one of the causes' (Holland, 1986, OSCE, 2006, OSCE, 2001). If high-turnout fraudulent precincts were less likely to be exposed to the webcam 'treatment,' then any causal inference that does not account for this bias is questionable. The first part of the empirical section will be solely devoted to explaining the allocation of web cameras.

Measuring the Dependent Variable: Election fraud

In this article we will utilize three different measures of election fraud. One of them is a direct observable metric that captures vote-count fraud and nothing else. The other two measures can at best be considered useful proxy measures for fraud. I begin with a thorough discussion of the recently developed digit-based test.

Digit-based tests examine the distribution of digits for individual candidates/parties and compare this with what would be expected if the vote-count were clean.[9] Intuitively it makes sense that the last digit would follow a uniform distribution if the vote count is large enough. Say that a candidate receives over 100 votes in one thousand polling stations. If the votes were counted properly it is expected that the last digit would be a 'zero' 10 percent of the time, a 'one' in another ten percent, and so on. A uniform distribution on the last digit simply means that each digit occurs with a 10 percent frequency. If the vote count has been fabricated, then humans may just be writing down a number that comes to mind, making the distribution deviate from uniform. In fact, humans, when prompted to produce a random list of numbers, actually favor small numbers on the 1-9 scale (Boland and Hutchinson, 2000). If there is a natural distribution of digits in vote counts and the actual election returns differ from this, it can be taken as evidence of fabrication.

[9] More information about the digit-based fraud tests is located in the appendix.

Some scholars focus on the last digit (Beber and Scacco, 2012, Mebane and Kalinin, 2009), while others focus the second digit and stipulate that the distribution should follow a Benford distribution (Mebane Jr, 2006, Mebane Jr and Kalinin, 2010). The distributional assumption about leading digits following a Benford distribution have been questioned (Deckert et al., 2011). Beber and Scacco show that a last-digit test requires extremely weak distributional assumptions and therefore suggest that it might be more suitable to detect fraud (Beber and Scacco, 2012).[10]

A digit-based measure of election fraud would naturally only capture what we here call vote-count fraud, which is only one of many forms of election day fraud. Other types include allowing multiple voting, ballot box stuffing, or coerced voting, which unfortunately, digit-based test cannot detect. For instance, as long as the stuffed ballots are counted properly, a digit-based test would not indicate fraud. An analysis of turnout, allows me to detect ballot box stuffing. Aggregated turnout figures should follow a normal distribution and if there is a spike at the higher end of the scale, it indicates an artificial boosting of the number of ballots cast (Myagkov et al., 2009). The same authors have further developed regression techniques to determine which parties benefit from an increase in turnout (Myagkov et al., 2009). However, this approach suffers from some simplifying assumptions, for instance that the data are homogeneous and that turnout therefore varies across polling stations randomly. Including relevant control factors in a multiple regression model can help solve this problem.

Finally, I use the vote share for the ruling party, which according to some authors can be understood as a proxy for fraud (Hyde, 2007, Hyde, 2010, Herron, 2010). The main problem here is that vote shares depend on many other things, and not only on fraud. There is therefore an omitted variable bias if we do not account for other relevant factors that affect vote share for governing parties.

Model

The relationship between web cameras and election fraud will be estimated in two different ways, both using matching techniques. First, turnout analysis will be conducted using multiple

[10] '...the theoretical result of uniformly distributed last digits holds across a wide range of data-generating processes' BEBER, B. & SCACCO, A. (2012) What the Numbers Say: A Digit-Based Test for Election Fraud. *Political Analysis*..

OLS regression techniques, controlling for previous turnout, the size of the polling station, and whether or not the precinct is in the capital city of Baku. The model estimated is:

$$Y_i = \alpha + X_i\beta + X_{ki}\beta_k + \varepsilon_i \quad [3]$$

where Y is turnout or government vote share in polling station i, X is a dummy for web camera in polling station i, X_k is a vector of k control variables, and ε_i are unobserved random error terms. Second, I conduct an analysis of fraud separately for monitored and non-monitored polling stations using digit-based tests for the two groups separately. This will tell us whether or not there is vote-count fraud in the treatment group. Finally, the ruling party vote share analysis will be conducted using the same formula as for turnout [3].

Results

In order to answer the question about the allocation of webcams and their possible effects on preventing fraud, I here present two central pieces of evidence. First, historical polling station level evidence is presented to estimate covariates of web camera allocation and thus adjust for the possible non-randomness of assignment. Second, micro-level electoral returns are used to analyze differences between monitored and non-monitored precincts.

Assignment of web camera treatment

Earlier studies do not test for different hypotheses about the allocation of webcams, instead attempting a statistical solution to the problem by matching using covariates from the same election (Herron, 2010). The Azerbaijani authorities have not revealed the specific allocation logic, but installation was done by the Ministry of Communication and IT, by request of the Central Election Commission..[11] An analysis of the location of webcams reveal that it clearly was

[11] 'A static camera that will allow viewing only the area where it is focused shall be installed in polling station. The cameras must be installed in election precincts in such a way to be able to cover the desk where precinct election commission members sit and issue ballot papers to voters and implement other processes with election documents, and to cover the ballot box.' (rule #6, CEC decision 27/132, October 8, 2008 'Rules on installation and use of web cameras in election precincts').

not random. For instance larger more urban areas are over-represented.[12] As already noted, biases in terms of allocation of this monitoring technique could possibly skew the results. In an autocratic context, we would have to assume that this allocation follows some rationale that would benefit the ruler. After all, there are plenty of indications of authorities being adamant about controlling the electoral process in authoritarian states (Levitsky and Way, 2010).

The central question in terms of the matching exercise is what the authorities could have known about precinct level of fraud. First, I need to establish what a plausible population for the assignment was. I will here argue that precincts with a history of less fraud were selected as the target group for web camera assignment. Second, out of this population, the authorities picked out only a proportion to be assigned a web camera, mainly due to resource constraints. For the matching analysis to be convincing, I need to account for why two precincts with otherwise similar characteristics were treated differently. I argue that in selecting between two otherwise similar precincts authorities essentially tossed a coin, controlling on the observables available. This allows for robust and accurate estimation of the causal effect of web camera.

Let us assume that the authorities know the level of fraud at the precinct level. The fact that after the 2005 elections as many as 650 precinct level protocols were cancelled and several fraud convictions were made partly validates this assumption. In addition, the authorities have access to parallel vote tabulation as well as exit polls that allow them to assess discrepancies between officially reported numbers and actual votes. Also, since the opposition and both domestic and international observers publish detailed results, the Azerbaijani authorities know where fraud was most common in previous elections.

There are broadly speaking four different conceivable rationales for allocation of webcams to particular precincts. First, authorities might genuinely be interested in reducing certain detectable types of fraud. In this scenario precincts with a bad track record of fraud would be selected for a webcam. The reason would simply be that blatant fraud is very costly in terms of providing the opposition with a target for their anticipated post-electoral mobilization and signaling backwardness to the international community. Also, granted that the authorities knew

[12] See balance table in appendix.

their candidates would prevail in any case, less blatant fraud allows for a better signal of strength (Little, 2011). Since only around 10 percent of precincts were assigned a webcam, fraud could continue unabated in the non-monitored locations and thus any potential loss in terms of votes for the government would be marginal. Such an allocation of webcams in effect incentivizes local officials to be smarter in conducting fraud

Second, authorities might be interested in putting on display well-to-do precincts where detectable fraud is non-existent. Here the government wants to show the world how clean the elections are. Third, theoretically speaking authorities might want to deny the opposition the use of detectable fraud techniques. Here oppositional strongholds would be denied the use of fraud. In the case of Azerbaijan this scenario is not necessarily plausible, but in other cases, like Kyrgyzstan, where there is a history of oppositional strongholds this logic might apply (Sjoberg, 2011). Finally, the allocation of webcams might due to practical considerations, as suggested by Herron. In a developing country with poor infrastructure, webcams can only be installed larger polling stations in more urban locations. Herron argues that practical considerations as well as proximity to the district level center were decisive for the 2008 assignments in Azerbaijan (Herron, 2010).

To answer the question about where webcams were allocated, we need to look at the characteristics of polling stations that consequently were monitored by webcams. The approach here is to use the last non-webcam monitored 2005 elections as the baseline in order to determine which of the scenarios outlined above are more likely. First of all, 90 percent of the cameras installed in 2008 stay in the same polling station in the following elections. This seems to suggest that once installed the cameras stay in the same place due to fixed costs associated with installation. The fundamental question is why where the cameras allocated to those specific 500 precincts in 2008 in the first place.

Comparing with the detailed 2005 electoral results, it turns out that the size of the polling station and turnout in 2005 rather well predicts where webcams will be allocated in 2008 (see model 4 in the logistic regression table). Both previous turnout and size of polling station are significant at the 1-precent level.

Table 1. Predicting the Allocation of Web Cameras, Azerbaijan 2008

	(1)	**(2)**	**(3)**	**(4)**
	b/se	b/se	b/se	b/se
Size of Precinct (ln)	3.980***	3.675***	3.690***	3.573***
	(0.31)	(0.29)	(0.27)	(0.34)
Margin of Victory, 2005	-0.014			0.024
	(0.08)			(0.09)
Turnout, 2005		-1.288**		-1.703***
		(0.41)		(0.50)
Baku (Capital city dummy)			0.273*	0.197
			(0.11)	(0.13)
Constant	-30.166***	-27.308***	-28.140***	-26.458***
	(2.21)	(2.09)	(1.90)	(2.46)
N	4166	4438	5357	3498
R^2 *(adj.)*	0.178	0.184	0.173	0.201

**Note:* The dependent variable is a dummy for whether or not the precincts had a webcam installed on election day. Logistic regression, significance levels: + p<0.10, * p<0.05, ** p<0.01, *** p<0.001.

The lower the turnout in 2005 the more likely it is that the precinct will be allocated a webcam in 2008. This is an especially important finding since the claimed association between webcams and turnout in 2008 (Herron, 2010), could be caused by webcams simply being allocated to precincts with lower turnout.

An even better metric for fraud is the digit-based test. In terms of vote-count fraud there seems to be less vote-count fraud in precincts that were eventually selected for the 2008 elections to be monitored by webcams; $\chi^2(9,\ N{=}4{,}515) = 22.38$, $p < 0.008$ in non-monitored precincts and $\chi^2(9,\ N{=}624) = 3.56$, $p = 0.938$ in monitored precincts.[13] Thus far, it seems as if web cameras were indeed allocated to less fraudulent polling stations in the sense of there being less vote-count fraud and possibly also less turnout-related fraud. Again, this makes perfect sense, since an autocrat would hardly benefit from pro-actively exposing fraud by allocating webcams to 'dirty' precincts.

It should be noted that there is no relationship between the allocation of webcams and anecdotal evidence of vote-count problems taken from the OSCE report.[14] The international election observation reports often single out individual polling stations where count-related fraud was detected. However, since the allocation of international observers was not random, such an

[13] For a graphical illustration of the difference, see the appendix.

[14] We have not been able to obtain the list of cancelled PS after the 2005 elections, but international observers notes that 'In total, 625 PEC results (12%) were cancelled by election commissions and courts, overall affecting 88 constituencies' (OSCE, 2006).

analysis can only be speculative. In addition to these factors, there are a couple of structural factors that complement the analysis. A higher percentage of the polling stations in and around the capital city of Baku were observed, 19 percent compared to 7 percent coverage for the rest of the country. But as the regression analysis illustrated, the capital city bias disappears when we control for other features. Larger polling stations also seemed to have been preferred, as noted by Herron, with 1,300 being the average size of a monitored precinct and 900 being the average for a non-monitored.

Based on comprehensive evidence I thus argue that webcams were allocated with an interest of showing relatively well performing polling stations. Since larger polling stations with a lower reported turnout in 2005 were selected for webcam monitoring, it is unclear if the turnout 'effect' in 2008 remains after controlling for these factors. Perhaps the cameras were simply allocated to polling stations where turnout was lower, but where the government nevertheless were confident that it would perform well. To account for the biases in terms of webcam allocation I pre-process the data by matching on: size, district, and turnout and competitiveness in 2005. Again, note that earlier work on webcams in Azerbaijan also used matching in estimating the effects (Herron, 2010). However, since none of the historical covariates were used, the biases in terms of web camera allocation remained given the use of post-treatment covariates.

Matching was done using a genetic matching search algorithm, as developed by (Sekhon, 2008). Genetic matching uses a weighted Mahalanobis distance to determine the optimal weight that each variable should take. The purpose of the procedure, from a statistical point of view, is to estimate some version of a causal effect. As a result we get a reduced dataset with a total of 749 observations that are similar on all other observable accounts, but differ in terms of whether or not a webcam was assigned. For item-wise improvement in balance, see appendix. After having pre-processed the data, taking into account the biases in terms of allocation of web cameras, we now move to the substantive analysis of webcam effects on election fraud.

Turnout tests

A regression analysis reveals that web cameras do seem to have a negative effect on turnout. In 2008, in the first ever webcam monitored elections anywhere in the world, turnout is reduced by as much as six percentage points. Here we use the coarsened exact match data described above. This finding confirms what earlier studies of the effects of webcams have shown (Herron, 2010). The presence of a web camera in the polling station somehow seems to suppress officially reported turnout numbers. These findings are robust for other specifications of coarsening as well as for more elaborate ways of matching.[15] For instance, the results from a genetic match using exact matching for district and matching on size and 2005 turnout levels, produce identical results.

Table 2. Turnout Effects of Web Cameras

	Full	**Match**
	b/se	b/se
Webcam	-0.069***	-0.070***
	(0.01)	(0.01)
Size (ln)	-0.029***	-0.127***
	(0.00)	(0.02)
Capital	-0.076***	-0.068***
	(0.00)	(0.01)
Turnout (2005)	0.140***	0.286***
	(0.01)	(0.04)
Margin of Victory (2005)	0.068***	0.094***
	(0.01)	(0.02)
Constant	0.877***	1.516***
	(0.02)	(0.15)
N	4434	749
R^2 (adj.)	0.356	0.388
F	491.90	95.68
p	0.000	0.000

* *Note:* Matched data using genmatch function in R, see appendix. Full stands for full dataset. The dependent variable is official turnout. OLS estimation. Significance levels: + p<0.10, * p<0.05, ** p<0.01, *** p<0.001.

At this point we do not know whether the inflated turnout numbers in non-monitored precincts in 2008 come from ballot box stuffing, multiple voting, miscounting, or from measures taken outside the polling station. Technically it is possible that web cameras induce more rigorous vote identification checks by election officials and therefore in essence disenfranchise voters that in the absence of a webcam would have been allowed to vote. Furthermore it has been argued that there could be a Soviet-era dynamic at play in which monitoring puts pressure on people to show

[15] For instance using optimal matching, as called through the MatchIt function in R, see KING, G., HO, D. E., IMAI, K. & STUART, E. A. (2011) MatchIt: Nonparametric Preprocessing for Parametric Causal Inference. *Journal of Statistical Software,* 42.

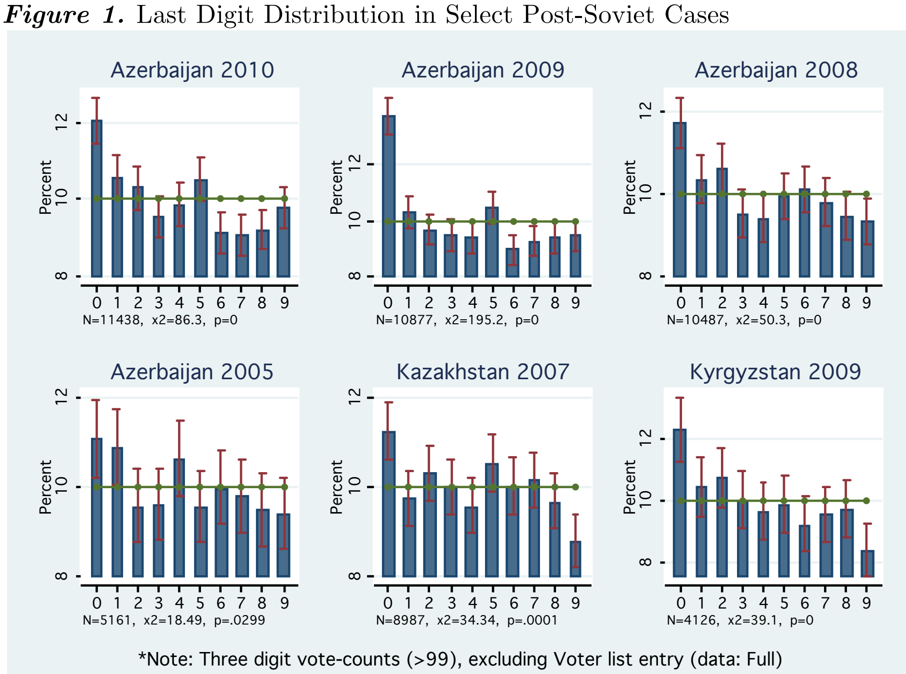
up (Herron, 2010). Evidence so far clearly shows that that is not the case. If anything there is a negative effect on turnout from having a web camera installed in a polling station.

Not only is turnout at best only a proxy for fraud, but it also does not reveal anything about the specific mechanism causing the observed reduction in 2008 when web cameras were first introduced. Interestingly, the effect on turnout disappears in the two following elections. That is, after having accounted for biases in the allocation of web cameras, I show that there is no negative effect of web cameras in the referendum in 2009, contrary to what earlier studies have claimed. In any case, the main interest here is the 2008 elections when web cameras were first introduced.

Digit-based tests

A more direct measure of fraud is the distribution of the last digit in the officially reported vote count per candidate in each polling station. But first let us look at vote-count fraud at the aggregate level and in some of the reference cases. These are all cases of allegedly fraudulent elections, as documented by both domestic observation organizations and international observation missions.

Figure 1. Last Digit Distribution in Select Post-Soviet Cases

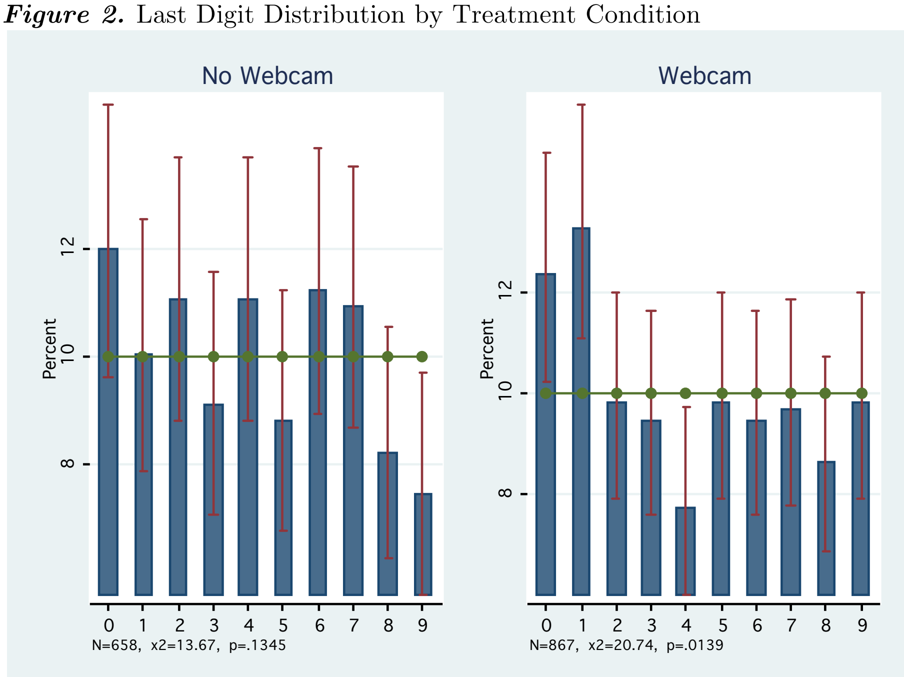


**Note:* Official Election Returns from the respective Central Election Commission. Only three-digit vote counts are included in order to avoid last digit biases. The green line indicates the expected uniform distribution under conditions of a clean vote count and the capped spikes in red indicate the 95-percent confidence interval for each individual digit (point-wise).

These graphs clearly illustrate that there are systematic deviations in terms of the last digit when compared to the expected uniform distribution under correct vote count. In all of these cases, the deviation is statistically significant at the .1 percent level, except for Azerbaijan in 2005 where the p-value is slightly higher. In any case, the four most recent national level elections in Azerbaijan have had a considerable amount of deviation form the expected uniform distribution on the last digit.

When examining the distribution of the last digit in polling stations with and without a web camera separately, we find some interesting patterns.

Figure 2. Last Digit Distribution by Treatment Condition



** Note:* Matched data using genmatch function in R, see appendix. The green line indicates the expected uniform distribution under conditions of a clean vote count and the capped spikes in red indicate the 95-percent confidence interval for each individual digit (point-wise).

When matched it turns out that there is actually vote-count fraud in monitored precincts in 2008, but no vote-count fraud in the control group. In the matched data where the sample size is roughly the same, the last digits deviate from uniform in the presence of webcams with a chi-square statistic of 20.74 and a p-value of .0139. In the polling stations with no webcam, where turnout was reported seven percent lower, none of the digits deviate from expectation under conditions of a clean count. The chi-square statistic here is a meager 13.67 and a p-value of .135. Furthermore, since humans when prompted to select digits at random prefer lower digits (Boland and Hutchinson, 2000), the pattern that we see in webcam precincts reveal this bias in human number generation. That is, the votes were here not reported correctly, but rather generated in a way that the officials might have considered random, but when analyzed across precincts reveal human preferences for lower digits. What makes this finding even more extraordinary is the fact that the precincts that were allocated a camera in 2008 had a relatively clean vote count in the preceding 2005 election. As was argued earlier, authorities seems to have picked out less fraudulent polling stations as the subjects for monitoring. The effect of web cameras therefore seems to be an introduction of vote-count fraud to places where it might not have existed before, at least not in 2005.

Since we already know that web cameras are associated with lower levels of turnout, the findings from the digit analysis seem to suggest that one type of fraud is substituted for another in the presence of web cameras. A camera perhaps deters blatant ballot box stuffing, but encourages fabrication of vote totals. As for the robustness of these findings, it should be noted that in the full monitored sample of 500 precincts, there were 1,017 vote counts that had more than three-digits. The distribution of these digits deviates from uniform at the 1 percent level.

Ruling party vote share

Having established that there are some effects of webcams on fraud, the natural follow-up question is: *Cui Bono*? That is, who benefits. A regression analysis, with precinct level vote shares for the ruling party as the dependent variable, reveals that there is no significant effect of webcams.

Table 3. Government Vote Share Effects from Web Cameras

	Full	**Match**
	b/se	b/se
Webcam	0.002	-0.001
	(0.00)	(0.00)
Size (ln)	-0.004*	-0.023+
	(0.00)	(0.01)
Capital	0.029***	0.031***
	(0.00)	(0.01)
Turnout (2005)	0.037***	0.010
	(0.01)	(0.03)
Margin of Victory (2005)	0.032***	0.054***
	(0.01)	(0.01)
Constant	0.864***	1.009***
	(0.01)	(0.10)
N	4434	749
R2 (adj.)	0.032	0.057
F	30.24	9.98
p	0.000	0.000

* *Note:* The dependent variable is incumbent President vote share. Matched data using genmatch function in R, see appendix. Full stands for full dataset. The dependent variable is turnout. OLS estimation. Significance levels: + p<0.10, * p<0.05, ** p<0.01, *** p<0.001

This follows the hypothesis laid out in the theoretical section. A supposedly anti-fraud monitoring technique does not necessarily punish the ruling coalition if there are compensation mechanisms available. As has been shown the introduction of web cameras decreased turnout-related fraud, but increased miscounting. It is therefore quite possible that authorities were able to compensate for the reduction in ballot box stuffing with adding votes to the governing party in the vote-count phase.

The compensation is simply that there are less ballots to play with (less ballot stuffing), as indicated by a lower turnout, but miscounting is done is a way that is vote share neutral for the ruling party. This way, it is not surprising to see reduced turnout, increased vote-count manipulation, and no precinct level effects on the ruling party.

Given that turnout appears reduced in the presence of webcams and pro-government candidates are not hurt electorally, the aggregate level the total vote share for the pro-governmental bloc should decrease. The authorities maintain the same level of support at the precinct level, but the decrease in turnout in monitored precincts in 2008 would have to be compensated by getting a higher vote share for their own candidates in monitored polling stations. That is, if full compensation is sought. Even if there is no negative effect on precinct level vote share form the introduction of webcams, on the aggregate level there is a negative effect due to the lower number of total votes case for the ruling party.

Summary and Discussion

In short, there are four substantive findings presented in this article: 1) Web cameras are selectively placed in precincts that were performing better in terms of fraud in earlier elections; 2) Web cameras reduce turnout-related fraud suggesting that there was less ballot stuffing; 3) Web cameras increase vote-count fraud indicating a compensation mechanism; and finally 4) The ruling party vote share, at the precinct level, is not affected.

When first introduced, webcams had a strong negative effect on turnout. An analysis of last digits suggests that web cameras actually are associated with more vote-count fraud, both when compared with the control group and compared with the historical data from the treated polling stations. The introduction of web cameras therefore seems to have had the perverse consequence of causing fabrication of vote totals, a fraud technique that election officials perhaps did not think would be captured by a camera. For the ruling party, there are no effects on the precinct level vote share, which suggests that the reduction in turnout-fraud was compensated by either miscounting or by measures taken outside the polling station. This being the case, the puzzle about autocrats embracing fraud-reduction technologies disappears. If web cameras can be introduced without any effects on the vote share, that is, without a cost to the ruling party, then it is hardly surprising that they are being deployed.

These substantive findings are consistent with a theory about fraud portfolio allocation and autocratic adaptation. An anti-fraud intervention alters the relative cost-benefit of different fraud techniques. In the presence of a supposed anti-fraud intervention, like web cameras, an adjustment of fraud strategies can therefore be expected. Web cameras reduce one type of fraud, but the fraud perpetrating ruling party does not suffer electorally, at least not at the precinct level. Since authorities control the timing and the communication of web camera allocation, it is likely that local and regional level pro-government forces had time to prepare for compensating for the removal of blatant fraud techniques. The findings presented here specifies the fraud reduction mechanism, something that earlier studies were unable to do due to only focusing on turnout and government vote share as proxies for fraud. Digit-based tests thus provide a valuable addition to the fraud forensics toolbox.

In this paper I also present a more plausible explanation for the placement of webcams. I argue that it might well be in interest of an autocrat to reduce blatant fraud, like ballot stuffing, but at the same time to avoid exposing really fraudulent precincts to web cameras. It makes perfect sense for an autocrat to introduce anti-fraud techniques as long as full control is retained elsewhere in the electoral cycle. In making use of new monitoring technologies, it is sensible to avoid exposing known fraudulent precincts. The case of Azerbaijan is a good illustration of this logic. Cameras were installed in only a fraction of polling stations and only less fraudulent precincts were selected for webcam installation.

There are several implications for further study. First, the focus in this paper has been on autocratic regimes. More democratic countries like Albania and Pakistan are currently contemplating installing web cameras at the precinct level. In a context with limited fraud on election day the effects of webcams might be different from that of Azerbaijan which has a history of blatant fraud. Second, there is only limited evidence of the suggested fraud compensation mechanisms. More work need to be done on vote buying, intimidation, and other techniques used out of the view of web cameras. Some interesting work on vote buying using list experiments is a promising avenue for further research (Gonzalez-Ocantos et al., 2010). Second, for both policy and research purposes, it would make sense to advocate for the random allocation of web cameras. This way we could estimate the causal effects with more confidence in the direction of causality. Random allocation would also make it more difficult for authorities to plan for fraud substitution to compensate for not being able to use ballot-rigging techniques. Also, in terms of policy recommendations I would suggest that we stop looking for quick technical fixes to the persistence of election fraud around the world. A cunning autocrat is able to cope with almost any quick fix you throw at them.

Appendix

Digit-Based Fraud Tests

The statistical test we use for vote-count fraud is chi-square goodness-of-fit. The null hypothesis of a clean vote-count is that the data follow a uniform distribution. Correspondingly a fraudulent vote-count is one in which the last digit deviates from the uniform distribution.

The chi-square test statistic is defined as

$$\chi^2 = \sum_{i=1}^{k} (O_i - E_i)^2 / E_i \qquad [1]$$

where O_i is the observed frequency for each digit i and E_i is the expected frequency for i. The hypothesis that the data are from a population with the specified distribution is rejected if

$$\chi^{2'} > \chi^2(\alpha, k - c) \qquad [2]$$

where $\chi^2(\alpha, k - c)$ is the chi-square percent point function with $k - c$ degrees of freedom and a significance level of α. In our example there are ten bins, digit categories, with nine degrees of freedom. The uniform distribution on the last digit means that in each cell there should be ten percent of the observations.

Let me illustrate this with a real example.

Table 4. Last Digit Distribution, Illustrative Example (Azerbaijan, 2010)

Digit Value	**Count Observed**	**Count Expected**	**Percent Observed**	**Percent Expected**	χ^2	**P-value**
0	2464	2016	12.2%	10.0%	99.753	0.0000
1	2144	2016	10.6%	10.0%	8.179	0.0028
2	2084	2016	10.3%	10.0%	2.321	0.1103
3	1880	2016	9.3%	10.0%	9.123	0.0014
4	1880	2016	9.3%	10.0%	9.123	0.0014
5	2256	2016	11.2%	10.0%	28.672	0.0000
6	1772	2016	8.8%	10.0%	29.441	0.0000
7	1848	2016	9.2%	10.0%	13.936	0.0001
8	1952	2016	9.7%	10.0%	2.007	0.1391
9	1876	2016	9.3%	10.0%	9.669	0.0010
Total	20156	20156	100.0%	100.0%	212.224	0.0000

* *Note:* Only three-digit (vote counts < 99) are used.

First we count the number of times each 0-9 digit occurs as the last digit. By using formula [1] we arrive at the chi-square test statistic. For instance, in the table above there are 2464 zeroes while we only expected 2016, 10 percent had the vote-count been clean. Following formula [1] we get (2464-2016)^2 / 2016 as the test statistic (χ^2) for the digit 0. After having done this for all digits we add them all up.

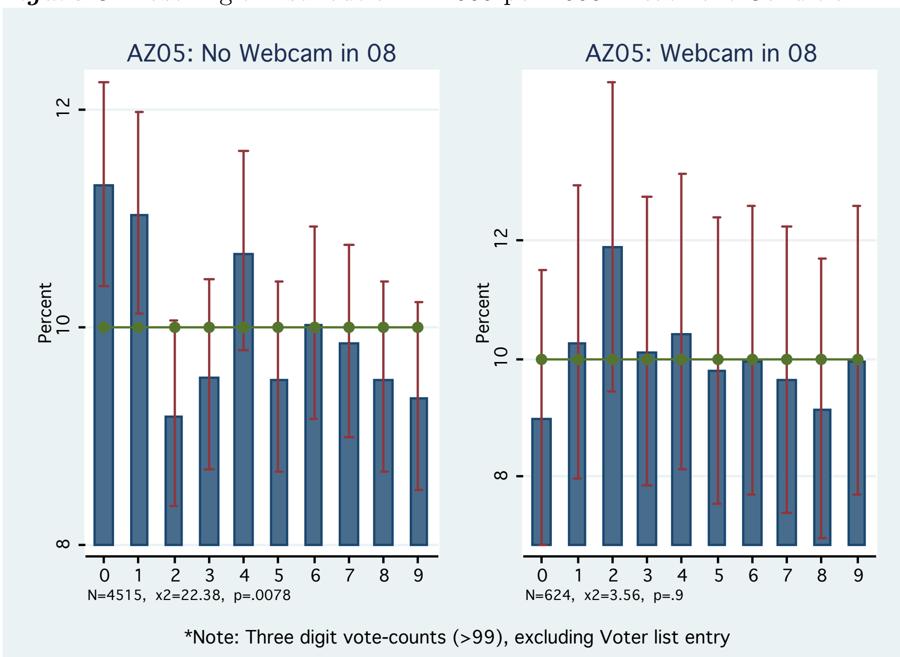
The next step is to use the chi-square distribution table and determine whether or not the chi-square test is large enough for us to reject the null at a conventional significance level. Given 9 degrees of freedom and a desired 5 percent significance level, any chi-square statistic equal or larger than 16.919 indicates a deviation from the expected uniform distribution under the null hypothesis. In this example the chi-square test statistic is 212.224, well above the 16.9 level, allowing us to reject the null at the 5-percent level. Substantively this finding suggests that the numbers are generated by humans jotting down whatever numbers comes to mind, and not by meticulously counting the ballots.

There are a few things to note about this statistical test. The chi-square statistic is sensitive to the size of the sample. With very large sets of data, the sum of all deviations from an expected distribution adds up to a large statistic. This is especially problematic if there are uneven number of observations in two groups that are compared. As in the case at hand when we compared monitored polling stations with non-monitored, the non-monitored groups contains far fewer observations and we therefore need to make sure that the differences in terms of *p*-values are not due to uneven sample sizes. To solve this problem we created smaller samples of equal sizes from the non-monitored group to match the sample size of the polling stations with webcams.

Camera allocation logic

The graph illustrates that there was no vote-count fraud in the precincts that were eventually selected for web camera installation in 2008.

Figure 3. Last Digit Distribution in 2005 per 2008 Treatment Condition



* *Note*: Full data used.

Balance Table

Here both the balance in terms of relevant structural and historical covariates is presented. A detailed table with the resulting genetically matched sample is also presented.

Table 5. Balance Table for All Data

Variable	**Means Control**	***N***	**Means Treatment**	***N***	**Diff.**	***t*-stat**	**p-value**
Voters (size)	878	4851	1333	500	-455	-22.590	0.000
Capital	0.166	4859	0.378	500	-0.212	-11.762	0.000
Turnout (05)	0.527	4013	0.424	427	0.103	12.436	0.000
Margin of vict. (05)	0.351	4030	0.257	427	0.094	7.394	0.000

* *Note:* The total number of polling stations in the dataset is 5,359.

Matching was done using a genetic matching search algorithm, as developed by (Sekhon, 2008). Below we present the balance table that the matching resulted in.

Table 6. Balance Table for Matched Data

1.	**Means Control**	***N***	**Means Treated**	***N***	**Mean Diff**	**Balance Improvement Mean Diff**
Voters (size)	1321	322	1332	427	11	97.6%
District (SMD)	52.304	322	52.304	427	0.000	100.0%
Turnout (05)	0.417	322	0.424	427	0.007	93.5%
Margin of vict. (05)	0.252	322	0.257	427	0.005	94.6%

* *Note*: Genetic matching was done separately for each Single-Member District (SMD). All the variables used in matching are here presented.

When matching we specified exact matching for election district (SMD) to account for heterogeneity between districts. This means that district where there was no webcam installed were automatically dropped.

References

ACEMOGLU, D. & ROBINSON, J. (2006) *Economic Origins of Dictatorship and Democracy,* New York, Cambridge University Press.

BEBER, B. & SCACCO, A. (2012) What the Numbers Say: A Digit-Based Test for Election Fraud. *Political Analysis*.

BERTRAND, R., BRIQUET, J. L. & PELS, P. (2007) *The hidden history of the secret ballot*, Indiana Univ Pr.

BIRCH, S. (2012) *Electoral Malpractice*, Oxford University Press, USA.

BOLAND, P. J. & HUTCHINSON, K. (2000) Student selection of random digits. *Journal of the Royal Statistical Society: Series D (The Statistician),* 49**,** 519-529.

DAHL, R. A. (1971) *Polyarchy: participation and opposition,* New Haven, Yale University Press.

DECKERT, J., MYAGKOV, M. & ORDESHOOK, P. C. (2011) Benford's Law and the detection of election fraud. *Political Analysis,* 19**,** 245-268.

DIAMOND, L. (2002) Thinking about hybrid regimes. *Journal of Democracy,* 13**,** 21-35.

EISENSTADT, T. A. (2004) *Courting Democracy in Mexico: Party Strategies and Electoral Institutions*, Cambridge Univ Pr.

FEARON, J. D. (2011) Self-enforcing democracy. *The Quarterly Journal of Economics,* 126**,** 1661-1708.

GONZALEZ-OCANTOS, E., DE JONGE, C. K., MELENDEZ, C., OSORIO, J. & NICKERSON, D. W. (2010) Vote buying and social desirability bias: Experimental evidence from Nicaragua. *American Journal of Political Science*.

GREENE, K. F. (2007) *Why dominant parties lose: Mexico's democratization in comparative perspective*, Cambridge Univ Press.

HERRON, E. (2010) The effect of passive observation methods on Azerbaijan's 2008 presidential election and 2009 referendum. *Electoral Studies*.

HOLLAND, P. W. (1986) Statistics and causal inference. *Journal of the American Statistical Association***,** 945-960.

HYDE, S. (2007) The observer effect in international politics: Evidence from a natural experiment. *World Politics,* 60**,** 37.

HYDE, S. & MARINOV, N. (2011) Information and Self-Enforcing Democracy: The Role of International Election Observation.

HYDE, S. D. (2010) Experimenting in democracy promotion: international observers and the 2004 presidential elections in Indonesia. *Perspectives on Politics,* 8**,** 511-527.

HYDE, S. D. (2011) *The Pseudo-Democrat's Dilemma: Why Election Monitoring Became an International Norm*, Cornell Univ Pr.

ICHINO, N. & SCHUNDELN, M. (2011) Deterring or Displacing Electoral Irregularities? Spillover Effects of Observers in a Randomized Field Experiment in Ghana. Working paper.

KELLEY, J. (2009) The More the Merrier? The Effects of Having Multiple International Election Monitoring Organizations. *Perspectives on Politics,* 7**,** 59-64.

KELLEY, J. G. (2012) *Monitoring Democracy: When International Election Observation Works, and Why it Often Fails*, Princeton University Press.

KING, G., HO, D. E., IMAI, K. & STUART, E. A. (2011) MatchIt: Nonparametric Preprocessing for Parametric Causal Inference. *Journal of Statistical Software,* 42.

LEHOUCQ, F. (2003) Electoral Fraud: Causes, Types, and Consequences. *Annual Review of Political Science,* 6**,** 233-256.

LEHOUCQ, F. & MOLINA, I. (2002) *Stuffing the ballot box: fraud, electoral reform, and democratization in Costa Rica*, Cambridge Univ Press.

LEHOUCQ, F. E. (2002) Can parties police themselves? Electoral governance and democratization. *International Political Science Review,* 23**,** 29-46.

LEVITSKY, S. & WAY, L. A. (2002) The Rise of Competitive Authoritarianism. *Journal of Democracy,* 13**,** 51-65.

LEVITSKY, S. & WAY, L. A. (2010) *Competitive Authoritarianism: Hybrid Regimes After the Cold War,* New York, Cambridge University Press.

LITTLE, A. (2011) Fraud and Monitoring in Noncompetitive Elections. *SSRN eLibrary.*

LITTLE, A. T. (2012) Elections, Fraud, and Election Monitoring in the Shadow of Revolution. *Quarterly Journal of Political Science.*

LUST-OKAR, E. & JAMAL, A. A. (2002) Rulers and rules. *Comparative Political Studies,* 35**,** 337.

MEBANE JR, W. R. (2006) Election forensics: the second-digit Benfordís law test and recent American presidential elections.

MEBANE JR, W. R. & KALININ, K. (2010) Electoral Fraud in Russia: Vote Counts Analysis using Second-digit Mean Tests. *MPSA.* Chicago.

MEBANE, W. R. & KALININ, K. (2009) Comparative Election Fraud Detection. *MPSA Annual Meeting.* Chicago.

MOZAFFAR, S. & SCHEDLER, A. (2002) The comparative study of electoral governance - Introduction. *International Political Science Review,* 23**,** 5-27.

MYAGKOV, M. G., ORDESHOOK, P. C. & SHAKIN, D. (2009) *The Forensics of Election Fraud: Russia and Ukraine*, Cambridge University Press.

NYBLADE, B. & REED, S. R. (2008) Who cheats? who loots? Political competition and corruption in Japan, 1947ñ1993. *American Journal of Political Science,* 52**,** 926-941.

OSCE (2001) Republic Of Azerbaijan Parliamentary Elections Final Report. *Osce/Odihr Election Observation Mission.* Warsaw, Office for Democratic Institutions and Human Rights.

OSCE (2005) Republic Of Azerbaijan Parliamentary Elections 6 November 2005 Final Report. *Osce/Odihr Election Observation Mission.* Warsaw, Office for Democratic Institutions and Human Rights.

OSCE (2006) Republic Of Azerbaijan Parliamentary Elections 6 November 2005 Final Report. *Osce/Odihr Election Observation Mission.* Warsaw, Office for Democratic Institutions and Human Rights.

PRZEWORSKI, A. (2009) Conquered or granted? A history of suffrage extensions. *British Journal of Political Science,* 39**,** 291-321.

SCHEDLER, A. (2002) The menu of manipulation. *Journal of Democracy,* 13**,** 36-50.

SCHEDLER, A. (2006) *The Logic of Electoral Authoritarianism,* London, Lynne Rienner Publishers.

SEKHON, J. (2008) Multivariate and propensity score matching software with automated balance optimization: The matching package for r.

SIMPSER, A. (2012) *More than Winning: Why Governments and Parties Manipulate Elections.*

SIMPSER, A. & DONNO, D. (2012) Can International Election Monitoring Harm Governance? *The Journal of Politics.*

SJOBERG, F. M. (2011) Competitive Elections in Authoritarian States : Weak States, Strong Elites, and Fractional Societies in Central Asia and Beyond. *Government Department.* Uppsala, Uppsala University.

SJOBERG, F. M. (2012) Making Voters Count: Evidence from Field Experiments about the Efficacy of Domestic Election Observation. *Association for the Study of Nationalities.* Columbia University, New York.

TUCKER, J. (2007) Enough! electoral fraud, collective action problems, and post-communist colored revolutions. *Perspectives on Politics,* 5**,** 535-551.

WEDEEN, L. (2008) *Peripheral visions: Publics, power, and performance in Yemen*, University of Chicago Press.