TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Andrii Grygoriev
156413ivgm

ANALYSIS OF OBSTACLES IN THE RAPID INTRODUCTION OF INTERNET VOTING IN THE USA

Master's thesis

Supervisor: Ingrid Pappel
Assoc. Prof.
PhD
Co-supervisor: Valentyna Tsap
MSe

Tallinn 2018

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Andrii Grygoriev
156413ivgm

INTERNETIHÄÄLETUSE KIIRE KASUTUSELEVÕTU TAKISTUSTE ANALÜÜS USA-s

Magistritöö

Juhendaja: Ingrid Pappel
Dotsent
PhD
Kaasjuhendaja: Valentyns Tsap
MSe

Tallinn 2018

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Andrii Grygoriev

22.05.2018

Abstract

This Thesis is attended to research key requirements and to find out the obstacles of why internet voting is introduced in a slow manner in such high tech country as the United States of America. The aim of this research is to show main obstacles to well working voting in such a technically advanced country like USA. Estonia is the good example where internet voting works well. This research is aimed to introduce a small part of e-Governance by Internet voting in USA and what can be done to go through the obstacles so more people will be engaged in voting, state will spend less money on voting process and citizens will be more motivated to be involved in development of e-Governance overall.

This thesis is written in English and is 48 pages long, including 7 chapters and 1 figure in it.

Annotatsioon

Internetihääletuse Kiire Kasutuselevõtu Takistuste Analüüs USA-s

Selle teadustöö põhirõhuks on uurida võtmeelemente ja leida põhilised takistused, miks internetihääletuse kasutuselevõtt ei ole olnud nii edukas kõrgtehnoloogilistes riikides nagu seda on Ameerika Ühendriigid. Uurimustöö eesmärk on välja tuua peamised takistused sellise hääletussüsteemi kasutuselevõtul tehniliselt arenenud riikides nagu seda on Ameerika Ühendriigid. Hea näitena võib välja tuua Eesti, kus e-hääletus töötab hästi. See uuring on suunatud tutvustama väikest osa e-valitsusest. Põhifookuseks on internetihääletuse peamised takistused USA-s ning võimalikud lahendused inimeste kaasamiseks. Lisaks kulutab riik vähem raha valmisprotsessile ning kodanikud on rohkem motiveeritud kaasa lööma e-valitsuse arendamise protsessi.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 48 leheküljel, 7 peatükki, 1 joonist.

List of abbreviations and terms

ICT	Information and Communications Technology
IT	Information Technology
IS	Information System
SSN	Social Security Number
DRE	Direct-Recording Electronic
UX	User Experience
E2Eviv	End-to-End Verifiable Internet Voting

Table of contents

Author's declaration of originality 3
Abstract 9
Annotatsioon 5
List of abbreviations and terms 6
List of figures 8
1 Introduction 9
1.1 Research Problem 11
1.2 Research Questions and Objectives 11
2 Theoretical backgroung 13
3 State of the Art 15
3.1 E-Governance in the USA 15
3.2 Internet Voting in the World 16
3.3 Internet Voting in the USA 18
3.4 Voting in the USA 20
3.5 Electronic Voting in the USA 22
3.6 E-identity as an Essential Infrastructure for e-Voting 24
3.6.1 Digital Identity in the USA 25
3.6.2 Digital Identity in Different Countries 26
4 Research Methodology and Observations 27
4.1 Research Design 27
4.2 Research Method 27
4.3 Interviews 28
5 Results from Conducting Interviews 29
6 Reccomendations for a Better Implementation Process of Internet Voting in the US 31
6.1 Benefits from Recommended System 36
7 Conclusion 38
References 42
Appendixes 46

List of figures

Figure 1. Internet voting with feedback system.....35

1 Introduction

In this thesis author will attempt to discover of what are the negative causes why internet voting is not well introduced in the USA. The idea and reason why author is motivated to research Internet voting in the USA is his future involvement in implementation of Internet voting in one of the states. Internet voting should decrease the amount of money which is spent on every election as the only sustainable expenditures will be on IT service, such as Cyber Security and IT support. Another positive key factor for Internet voting is citizen's engagement into voting overall. Concerning first year investment, author can assume that it will be more then providing one election. Almost every e-Governance and e-Government solutions need long-term investment but it is a one time investment. The USA is a country where people really afraid of their privacy. As there were a lot of incidents in Cyber Security during last decade people are not confident in security in internet voting. But if we research and analyze voting system which works nowadays in the USA, we can assume that even electronic machines are also vulnerable and can bring not an accurate data. In this thesis I will try to indicate about it.

The entry of mankind into the third millennium, connected by a number of specialists in the field of philosophy, informatics, economics, jurisprudence and other sciences, with the transition to an information society that has a new structure in which industries specializing in the acquisition, dissemination and processing of information play a special role in the natural transformation of political institutions of democracy.

The rapid dissemination and implementation of new information and telecommunication technologies provide new tools and methods that help accelerate the transition from a weak to a true democracy, create ample opportunities for all members of the community to manage their lives more effectively as independent participants.

The information available in electronic form, coming from the state, can contribute to the development of a dialogue with publicity. The state, as an instrument designed to serve the interests of the people, with the introduction of information and telecommunication technologies into the government bodies, has new opportunities to

inform its citizens, take into account their opinions on key issues, and increase the effectiveness of its activities. In the information society, state bodies use the Internet to restructure, enhance their work, open information interaction with publicity.

As an example of changing the characteristics of a democratic democracy, Finland can be cited, where the tele-democracy is successfully developing at the municipal level. So, the municipality, which has 3 thousand citizens, instead of spending money on the construction of a modern city hall, decided to create an open information network. According to the mayor, there were good reasons for reforming the archaic decision-making system in the municipality and building an open information network made this system more flexible, with an operational decision-making mechanism and provision of public services. This is a vivid example of citizen participation in management through open channels.

Another example is electronic voting via the Internet. It, in the opinion of a number of scientists, is capable of stimulating political participation. Thus, during the experiment in the state of Oregon in 200sh, when the vote was carried out, and by means of e-mail, voter turnout exceeded 80%. Some scientists believe that electronic city meetings - this is democracy in its best manifestation. However, Internet voting has its drawbacks. Their potential danger lies in the fact that the simplification of the procedure for filing petitions by citizens will make possible the emergence of a whole wave of political initiatives emanating from the population. Thus, it is true that cyber-democracy combined with a tightened e-voting system can bring society back to the direct democracy of the Ancient Athenians.

Among the tendencies typical for the modern stage of the development of democracy, researchers increasingly point to the transition to the network principle of building public-power relations, which has two main features:

1) stable communication in the network, that is, the stable ability of the network to maintain free communication between its components;

2) network consistency, due to the sharing of interests between the objectives of the network itself and the objectives of its components. The implementation of these features in practice creates the conditions for building a network state.

Internet voting systems continue to be actively improved from the technical point of view and from the point of view of securing information in the process of voting and processing votes, enabling the organization of remote voting through any communication channels and any platforms.

Currently, about 40 countries are considering the possibility of introducing different types of Internet gaming systems and electronic voting in general.

1.1 Research Problem

The implementation of Internet voting would allow increased access to the voting process for millions of potential voters who do not regularly participate in our elections, but, technological threats to the security, integrity and secrecy of Internet ballots are significant (California Internet Voting Task Force, 2000). According to world statistics about 90% of all projects that went online were super successful. Good example of this is ZIP2, initially was named as Global Link, that introduced and licensed online city guide software to newspapers (Outing, Steve "Zip2 Plays Up National Network Card"). Author can compare it with such companies like PayPal, Amazon, Uber, Instacart, even Facebook – these companies revolutionised specific businesses into internet and made life for many people more comfortable, saving their money and time. Author believes that Presidential Voting or other types of voting should be provided online as it has not less security as nowadays voting in the United States such as Electronic Voting or Paper Voting. Author's motivation for looking into this research problem is further attempt of Internet Voting introduction in the United States step by step from one state to another. The biggest problem can be hidden in the security that is why the introduced system should be provided with highly secured Internet Voting which will be tested by different genius hackers. Author believes that any system can be developed in terms of demands from this system, namely all voting protocol rules. Appel mentioned that these voting protocols are – (a) allow each person to vote just once, (b) accurately records the votes, (c) accurately counts the votes, (d) voter can be sure his/her vote is counted and (e) secrecy (Appel, 2016).

1.2 Research Questions and Objectives

The master's thesis will concentrate on the following main research questions:

1. What are the external and internal factors influencing Internet Voting introduction in the context of developed countries such as United States of America?

2. What are the benefits, obstacles and risks that influence Internet Voting introduction?

3. What outcomes can be from the Internet Voting Introduction in the United States?

2 Theoretical Background

This chapter introduces the literature background and shows the different explanations of what is e-Governance, what is e-Government, what is Internet Voting in the USA. The goal of this section is to see the definition and differentiate of e-Governance in the USA, in Estonia and in the world overall from researchers and academicians.

According to Tan, - is a broader definition than eGovernment and is defines as transforming the business of government (Tan, 2005). E-governance projects are mostly designed with involvement of many stakeholders both internal and external to the owner organization (Suri, 2017). Axelsson mentions that there are many stakeholders associated with large e-governance projects, the prominent ones include employees in government organizations and the service users of government services which have been the focus of many scholarly studies (Axelsson, 2013).

Electronic voting is defined as voting by electronic means to take care of casting and counting votes (Buchsbaum, 2004).

The California Internet Voting Task Force identifies 3 types of voting - voting at a supervised poll-site using electronic equipment, voting at an unsupervised electronic kiosk and "remote voting"— voting from home or business using the voter's equipment (Goos, Hartmanis and Leeuwen, 2001).

Buchsbaum distinguishes two main types of electronic voting – "e-voting supervised by the physical presence of representatives of governmental or independent electoral authorities, like electronic voting machines at polling stations or municipal offices, or at diplomatic or consular missions abroad; and - e-voting within the voter's sole influence, not physically supervised by representatives of governmental authorities, like voting from one's own or another person's computer via the internet (i-voting), by touch-tone telephones, by mobile phones (including SMS), or via Digital TV, or at public open-air kiosks - which themselves are more venues and frames for different machines, like, e.g" (Buchsbaum, 2004).

Kiayias, Korman and Walluck defines internet voting as remote voting, where the client software communicates over the Internet to the server software from a voter's

PC. However, there are at least two other ways to implement voting over the Internet: kiosk voting and poll-site voting (Kiayias, Korman and Walluck, 2006).

Alvarez mentioned that Internet voting requires understandable rules for how voters will be authenticated, when stakeholders can use the system and rules that explains when and how to tabulate the ballots" (Alvarez, Hall and Trechsel, 2009).

Most people associate the term Internet voting with voting online from remote locations such as home or work and do not often think of kiosks or machines in polling places (Mercurio, 2004).

According to Chiang, "e-voting system is designed to enable users to cast their votes with confidence and to conduct an efficient and effective election" (Chiang, 2009).

Holden mentioned that electronic identity is a "balance between access, security, authentication and privacy" (Holden and Millett, 2005).

3 State of the art

This chapter introduces state of the art about voting and eGovernance in the USA, and what is electronic voting and Internet voting in the USA. The goal of this section is to see the differences of e-identity in the USA and in other countries in the world overall.

3.1 E-Governance in the USA

First question is: "what s e-Governance overall?" E-Governance is a system of ICT (information and communication technology) that provide services in government, communication, information exchange Unwin, Tim (2009). There are different models which works in a manner as G2G - Government-to-government, G2B – Government-to-business, G2C – Government-to-customer and G2E – Government-to-employee, and, thanks to e-Governance, all kind of government services will be conveniently, efficiently and transparently provided to every citizen (Garson, 2006). According to Garson, there are three main kind of target groups which are citizens, government and business. E-Government is defined as technology which is put in the center of government activity, at the same time e-Governance can be defined in broader field which engages and motivates every citizen to take part in it.

As there is no norm determination of e-Government, many academicians and practitioners have tried to set this concept based on the idea, its scope, and use. At the same time Budd and Harris (2004) explained that the appearance of e-Government was as a result of a movement from technology to management as well as the development of scope performance and policy intentions.

The meaning of e-Government can be understood as a tool for making an efficiency higher and for increasing transparency. Different types of applications in the community sectors have helped to support enhancement and gather higher amount of revenue. A presumptive instance is the stakeholder model that can be adopted by organisations in government in the whole world in order to change of power in intercommunication between management and for identifying relevant stakeholders.

To understand the implication and communication between government with civilians through the application of ICT (information and communication technologies) is decisive if talking about E-governance in the United States. Holden determines e-

Government next way - “the transmission of states information and services via electronic method twenty-four hours per one day and all days per week” (Holden, 2003). When the Internet boost and the realization of public governmental websites and portals in times of 3 previous different management in government, Americans got the opportunity to enter any type of programs online from health care to tax declaration and an opportunity to access public data in government which was preliminary unavailable that makes high transparency to the public and government.

3.2 Internet Voting in the World

The best explanation is described by country which is the first and for now one of three countries where Internet voting works well at the whole country level and people are choosing their president via Internet. This country is Estonia and Internet Voting in this country is logically called i-Voting. E-Estonia gives a definition to i-Voting as a service which gives an opportunity for participants to use their ballots from various device, computer or other gadget, which has a connection to the Internet anyplace in the whole world (e-Estonia).

In 2012 a separate Electronic Voting Committee was established who is now responsible for conducting Internet voting while the National Electoral Committee retains a supervisory role. Internet voting was first introduced in the local elections of 2005, when more than 9 thousand voters cast their ballot via the Internet, this corresponded to about 2 per cent of all participating voters (Internet Voting in Estonia).

To understand the I-voting system better, the envelope voting method used in Estonia should be described in a short way as following:

1) A voter presents an ID document to be identified.
2) The voter then receives the ballot and two envelopes.
3) The voter fills in ballot paper and puts it into the envelope, which has no information about the voter.
4) Then he encloses the envelope into an outer envelope on which the voter's information is written.

5) The envelope is delivered to the voter's polling position of residence. After the eligibility of the voter is determined, the outer envelope is opened and the inner (anonymous) envelope is put into the ballot box.

The system guarantees that the voter's choice shall remain secret and recording of the vote in the list of voters in the polling district of residence prevents voting more than once (Internet Voting in Estonia, 2015).

Every national in Estonia own an ID card that has electronic chip, which allows to vote via the Internet. First, the ID card has to be plugged in a special ID card reader that is working with a computer, secondly, after the identity has been done through verification process (using the electronic ID card as a sort of digital signature), a citizen has an opportunity to cast own vote over the Internet. Every vote is not taken into a consideration to the end till the final minute of that day, and citizen has an ability in case of changing the mind cast the vote again so the previous vote will not be valid, when the new has come on the same officially election day.

If taking into account Switzerland, there is also Internet Voting which works very well. According to the article UMIC, in the Federal referenda in 2005 and in 2007, 41% of citizens voted via Internet voting that is higher percentage than that which had normally been the case until then, with the figure not usually going over 30%. A Report from the Council of State on the electronic voting project in Geneva was delivered to the Senate on 24 May 2006. On 31 May 2006 the Federal Government presented a report to the Federal Parliament summarising the experiments which had been carried out, and arguing for the introduction of remote electronic voting in stages for all elections and referenda (*Rapport sur les projets pilotes en matière de vote électronique*). In the Federal referendum on 17 June 2007 17% of the voters cast their vote electronically, 97% of whom via the Internet and 3% via SMS. In September 2007 the Federal Government presented its draft acts regarding electronic voting via the Internet enabling its extension throughout Switzerland, and these were approved (Electronic Voting Experiments in Political Elections around the World, 2008).

Taking into account Australia, J. Alex Halderman and Vanessa Teague discovered serious flaws in the iVote online voting system that would have allowed a malicious attacker to expose voters' secret ballots, substitute replacement votes, and sidestep the

verification mechanism. These findings demonstrate yet again why conducting Internet voting with existing security technologies poses grave real-world risks (Halderman and Teague, 2015).

According to the report of Makedonskiy and Lukjanov, the secrecy of voting in the Internet voting system is at big risk, which is explained by the algorithm used to ensure this requirement as the secrecy of the vote is provided by the fact that the functions for verifying the signature of ballots and their decoding are divided between two state organizations. They claim that in case of collusion between employees who have access to ballots and a secret key, the system will be compromised and the voter does not have a guarantee that his voice will not be known to outsiders.

There is a big variety if Internet voting in the world because every country has it's own path to it since every country has different system with electronic identification.

3.3 Internet Voting in the USA

One of the American states such as Arizona has moved to voting online. Every citizen, that has been made a registry, get an individual verification digits via mail. These people were able to cast ballots at a certain location or to use another option such as to vote via the Internet from any place, for example, at their home, work place or any other place. Citizens that were making votes through the Internet had to paste their PIN and type an answer for a couple of individual questions. When the information is checked and approved, citizens have the opportunity to make voting ("How online voting works").

In 1997, an American astronaut David Wolf was able to make a vote via email from his workplace – from the space. He was allowed to vote in Texas election. From that time, such states as Arizona, Alaska, Michigan are using election via Internet. The electronic voting system via Internet that were conducted in Arizona had these peculiarities:

- Verification providing (an authorisation with a unique number such as PIN);
- Vote coding within a special key to the client machine with the private key held by a trusted 3rd party;

- Vote forwarding to an website server through encrypted pipe secure sockets layer (SSL);

- separation of the voter identity from the vote into 2 tables (Lauer, 2004).

Checking logs are tracked who made a vote, another check-up logged is observed to enter to the data bank server. Only the trusted 3rd party (in this case KPMG) was permitted to encrypt the votes (Mohen and Glidden 2001)

According to history, in 1996 in the USA the Reformation Party RPUSA applied Internet Voting, which was called also as in Estonia I-Voting, for choosing applicant for the presidential post. It is considered to be the earliest internet voting in United States ("Electronic Voting").

There are many security threats that were noticed by many specialists and analysed by researchers and academicians. Thus, voting via Internet establishes a big number of security threats. Lauer makes an example of the most essential threats which are vulnerabilities of the PC platform and connected with the Internet. In Lauer research he mentions that client PCs can be established in homes of voter or in public/commercial organisations, any place where Internet connection is provided. According to that every gadget that is without malware is not practically feasible. Moreover, the privacy of each voter can be under threat.

According to the Washington Post Press in spring 2016, more than 30 states are already ready for Internet Voting but specialists are against it as they think it is still insecure. They think that Internet Voting in huge scope will shake positiveness and reliance of citizens.

Based on to the report of Spakovsky, specialists warned that there are still severe irresistible IT problems to sending data about votes via the Internet in a safe and verifiable way. So scientists do not recommend to introduce Internet Voting until there will be a special tested and certified software. He listed some challenges:

1) Preventing malicious software, firmware, or hardware that can change, fabricate, or delete votes, deceive the user in myriad ways including modifying the ballot presentation, leaking information about votes to enable voter coercion, preventing or discouraging voting, or performing online electioneering;

2) Stopping denial of service attacks from networks of compromised computers (called “botnets”), causing messages to be misrouted, and many other kinds of attacks;
3) Finding a strong mechanism to prevent undetected changes to votes not only by outsiders, but also by insiders such as equipment manufacturers, technicians, system administrators, and election officials who have legitimate access to election software and data;
4) Providing a reliable, unchangeable voter-verified record of votes that is at least as effective for auditing as paper ballots without compromising ballot secrecy; and
5) Designing a system that is reliable and verifiable even though Internet-based attacks can be mounted by anyone anywhere in the world (The Dangers of Internet Voting, 2016).

The extent of vulnerability isn’t just hypothetical; late last summer, Virginia decertified thousands of insecure WinVote machines. As one security researcher described it, “anyone within a half mile could have modified every vote, undetected” without “any technical expertise”. The vendor had gone out of business years prior (America’s Electronic Voting Machines Are Scarily Easy Targets, 2016).

According to report of Jones, until such time as Internet connectivity becomes nationally ubiquitous some form of reasonable access should exist for those voters without connectivity in their homes or places of work. Programs that could increase Internet voting access could include the following:

1) Kiosk or transportable computer that is designed, dedicated and available exclusively for voting;

2) Computer already installed in a public facility that can be made available to the voting public during an election period (Jones, 2000).

3.4 Voting in the USA

Some words about voting in the United States as the whole thesis will be centered about this such as different kinds of electronic voting particularly in the USA. In order to have right to vote in the United States of America the voter has to be at least 18 years old at the day of elections and different kinds of residency. Many of the states require also

from the vote to mentally competent and not to be committed a serious crime. In addition in all states of America voting is private, free, voluntary and nobody can make anybody to vote without his or her will. Comparing to Estonia, a citizen in the USA can vote only once, when in Estonia a voter can revote as many times as he or she wants as every next vote cancels previous. Every state, county, city or a ward, which is division of a city, is separated by precincts (voting districts). Firstly, citizens have to fill out a form with name and address plus other information to make a vote in the voting district where they live. Usually voters can fill the form to make a register via mail. Every state in the US has various laws according voting process. For example, in some states people can be registered on the same day of elections. But usually people can register themselves several weeks before election. During the Election Day, many citizens go to a polling place such as public building, such as a school, recreation center, city hall, or firehouse to cast ballots. Citizens present themselves to the poll workers, provide identification, and receive the materials needed to vote. Elections may take place at many different times. In the United States, general elections (for federal officials) are held every two years in even-numbered years. They are held on the Tuesday that falls between November 2 and 8 (Maxwell, 2015). Nowadays citizens who are qualified to vote in the USA do not take part. In 2000, only fifty one percent of electorate appeared. Another case in Florida, the same year, there found huge amount of shortcomings in the voting as the vote in that state demanded a second counting that was held during two and a half days. The observations showed that a lot of citizens vote not properly and a big number of other votes were obscure.

In 2002, Congress adopted the law in order to remove voting mistakes and to invest money for upgrading voting systems. Anyway, some experts continue to ask the question about accuracy of voting machines with a computer in it.

Later, in 2004, a proposition to give an opportunity military personnel and US people living abroad to vote through the Internet was abolished in terms that computer specialists examined the process and understood that it would be unlikely to hinder hackers from interfering with election counting.

Nowadays the voting methods in the USA is a combination that are not technical or electronic. Voting methods are dependent on the election places and have paper ballot, paper ballot with assisting devices and optical scanners which read special paper ballots

at local precints or central scanning locations, DRE machines (Direct Recording Electronic), etc. Every method has its own number of vulnerabilities (Santos R., 2018).

In 2014, a report by The Presidential Commission on Election Administration made this recommendation to the President. They supported their argument by asserting the following: "Jurisdictions that use electronic voting machines usually deploy machines for a few days per year and then lock them up in storage for the rest. For cash-strapped jurisdictions that wish to keep pace with evolving technology, the purchase of hundreds of expensive, specialized pieces of hardware good for only one purpose — elections — no longer makes sense" (2014, PCEA).

3.5 Electronic Voting in the USA

At the beginning, it is good to understand what is voting overall. Cambridge University Press gives next meaning: "Voting is an activity of choosing someone or something in an election" (Cambridge University Press). Voting helps group of people decide and show their view, following discussions, debates or election campaigns.

Next definition of an application is significant as it is used from 60s till nowadays in some parts of United States. It is e-Voting or Electronic Voting which is explained as voting applying electronic tools to help and keep the routine work of accepting and estimating the number of votes. Electronic voting can be included by either electronic voting machines in the polling stations, which are used in the US, and also Internet voting, that is more automated and convenient from the side of user, as it can be used remotely. So, electronic voting is a broader definition. Further we will research, analyse and describe what are the advantages and disadvantages of using electronic voting machines such as DRE and Internet voting.

DRE voting machine is a direct-recording electronic voting machine. This voting machine makes protocols about votes with a touchscreens and simple buttons by which the voter can authorize and make vote for each candidate. This machine has a computer inside that programmed separately from others. It is not connected via Internet and this considered to be more secure as usually hackers use Internet to connect to the users equipment to steal he vote. Anyway there were a lot of incidents when these machines were hacked even without Internet connection.

If we consider to observe most spread DRE voting machine, we can notice that its system is consisted of an embedded PC which has a touch screen that is provided in a secure way to avert inserting anything (such as keyboard or a mouse). It is inserted to the webhub which has an eternal energy deliver and sits in a booth where a private screen and sits are provided. Other words, this is a voting machine with a computer in it. Citizens have to visit places where the voting process is organised. Then voters are going through verification process and are assigned by identification cards or PIN which allow to enter the machine system. Every vote is saved in the system and afterward transferred to the system that manages election process. Comparing to I-Voting in Estonia there is no opportunity to make a recount.

In 2000 in Florida electronic voting was held during election of the President. According to Riera and Brown, there were a lot of problems during these elections such as faulty equipment of electoral, systems for use, errors in operations with polling, blended registration, hard to understand ballots and not existing ballot issues made the loss of approximately five million votes. That facts made the people to trust less in electronic voting processes. As a result, all around the world many governments decided to improve the voting equipment or to try brand new election methods.

In 2002 government of the USA invested several billion dollars for improving the old machines. During that time, many countries in the European Union were testing new electronic elections and studying projects for introduction.

Again if we observe the weaknesses of electronic voting machines such as DRE, the researchers, specialists and academicians were skeptical for many times as voting machines are not reliable and can be easily hacked even without leaving a mark. According to article, their claims have been backed up by repeated demonstrations of the systems' fragility: When the District of Columbia tested an electronic voting system in 2010, a professor from the University of Michigan and his graduate students took it over from more than 500 miles away to show its weaknesses; with actual physical access to a voting machine, the same professor—Alex Halderman—swapped out its internals, turning it into a Pac Man console. Halderman showed that a hacker who has access to a machine before election day could modify its programming—and he did so without even leaving a mark on the machine's tamper-evident seals (How electronic Voting Could Undermine the Election, 2016).

According to the Beth Clarkson's review, we can observe the minuses of electronic machines that are really vulnerable and insecure. The voting machine software used is proprietary and even the election officials are not allowed to inspect it. This is termed Black Box Voting and combined with Direct Recording Electronic (DRE) voting, which permits touchscreen machines and does not require a paper trail allows a situation ripe for exploitation (Clarckson, 2015).

Harper's Magazine reported in 2012, the security of these machines is so lax that: As recently as September 2011, a team at the U.S. Department of Energy's Argonne National Laboratory hacked into one of Diebold's old Accuvote touchscreen systems. Their report asserted that anyone with $26 in parts and an eighth-grade science education would be able to manipulate the outcome of an election….Johnston's group also breached a system made by another industry giant, Sequoia, using the same "man in the middle" hack - a tiny wireless component that is inserted between the display screen and the main circuit board - which requires no knowledge of the actual voting software (How trustworthy are electronic voting systems in the US, 2015).

According to USA.gov, there are procedures for Voting Without ID. It is said that if a citizen do not have a form of ID that his or her state asks for, he or she may be allowed to vote. But some states require you to take additional measures after you vote to make sure that your vote counts.

In the USA.gov also mentioned that some states may ask citizen to sign a form affirming his or her identity, other states will let a citizen cast a provisional ballot, which is used when there is a question regarding a voter's eligibility. In some states, election officials will investigate the voter's eligibility and decide whether to count the vote.

Some other states require thata citizen return to an election office in a several days and show an acceptable form of ID but if not, the vote will not be counted (usa.gov, 2016).

3.6 E-Identity as an essential infrastructure for e-voting

A digital identity is information on an entity used by computer systems to represent an external agent. That agent may be a person, organization, application, or device. ISO/IEC 24760-1 defines identity as "set of attributes related to an entity (2011, ISO). In addition, the use of digital identities is now so widespread that many discussions

refer to digital identity as the entire collection of information generated by a person's online activity, this includes usernames and passwords, online search activities, birth date, social security, and purchasing history (retrieved 2018, What does digital identity mean).

The establishment of Internet Voting is important as it has several benefits, such as convenience, transparency, money and time saving. Krimmer mentioned that "development of an electronic democracy with transnational character needs the further development of e-enabled instruments of democracy, i.e., e-initiatives, e-referenda and of course also e-voting instruments" (Krimmer R., 2007). Internet voting system needs to be employed on the already existing electronic system where residents have electronic identities. For instance, Estonia has electronic identity management which is based on X-Road.

3.6.1 Digital Identity in the USA

In the United States there are 5 main electronic identity perspectives. The most popular identity in the USA is driver's license. Americans can use driving license as main identity almost everywhere even when flying to another state. Government once wanted to make driving license to be main identity but it failed. Another identity is non driver's license identity – identity card, which can be issued at the same place where driver's license ID. The United States passport card and the USA passport can also be an identity. The USA Passport can be used outside of the USA, while the USA Passport Card can be used only for domestic flights and between member states of Western Hemisphere Travel Initiative Social Security Number in the United States is required almost everywhere when the case is concerned the documents, such as applying for a job, paying taxes, issuing driver's license or state id, opening an account in a bank, applying for a credit card, for a new credit line or buying a house or a car or even for some discount program in the store.

Right now there is no official electronic identity in the United States for US people. There were some attempts to introduce but nothing was brought to the end. According to company Gemalto, the only ID card that is used in the USA is the military CAC card which is used by the Department of Defense staff.

3.6.2 Digital Identity in different countries

Estonia has electronic ID card which can be used not only as an identification of a person but also in digital environment and for encrypted electronic signatures. This card can be used as a travel document within European Union. This ID card can be used by its citizens even outside of its country when it comes to digital using. As Estonian ID card allows to make Internet authorization securely by its encrypted chip in it, citizens can do many things online such as signing documents, making deals in e-Governance process, check medical records, submit tax return and participate in presidential vote elections through the website or even via a phone.

According to the latest news, Singapore is going to introduce digital identity system in the second half of 2018 (Straits Times, 2 march 2018). The SingPass Mobile application will give an opportunity to Singapore citizens use e-Government services such as filling taxes or paying parking fines with higher security and without physical token and one-time phone message. GovTech will also be working in private sector, for instance, signing document agreements and storage of digital documents (Kevin Kwang, Chanel NewAsia).

Japanese digital identity “My Number” was issued to several citizens in 2015. “My number” is an individual number, which have 12-digit ID number issued to all citizens and not foreign and foreign residents in Japan. This system is used for social security, taxation and disaster responses (The Japan Times, 2015). Still, Japan is going to go forward in the security of My Number system, as the data is vulnerable and the system needs further improvement.

4 Research Methodology and Observations

This Chapter presents various perspectives that could be adopted in the use of electronic government implementation. The objective of the research is to identify and evaluate factors influencing the use of Internet Voting systems in some countries, using USA as a case study. For this research work, a conceptual model has been prepared based on previous literature to test and validate this specific area services.

4.1 Research Design

The researcher employed appropriate research design to collate data to address the methodological issues as identified in the research problem. Scholars have supported the use of research design, which is often viewed as a structured set of rational decision making choices or guidelines for generating valid and reliable research results, and for ensuring information is obtained through an objective procedure and its relevance to the research problem. Thus, research design is concerned with enabling a problem to be researchable by setting up a study in a way that will produce accurate answers to specific questions (Hakim, 1987).

4.2 Research Method

Qualitative analysis, unlike quantitative, is useful for describing multiple realities, developing deep understanding, theory building, and capturing everyday life. A qualitative approach is inductive with specific instances used to arrive at overall generalizations. The types of data collected include text, pictures or sounds since interpretation of its meaning is in text or images (Bogdan & Taylor, 1975).

The author decided to use qualitative analysis as it will show more accurate concerns and reasons why people would choose or vice versa prefer not using Internet Voting.

Qualitative observation is best done when the observer becomes part of the process, conducting qualitative research is about participating in other people's lives and writing about that participation (Ezzy, Qualitative Analysis).

Qualitative research is based and focusing mostly on the human elements of the social and natural sciences, the goal of qualitative research is to answer the questions how and why in human experience (Given, 2008). Qualitative methods are giving explanations of the particular cases studied.

4.3 Interviews

The questionnaire is a special tool that helps to gather the information via the questions by respondent's answers to them. The questionnaire can be also used for gathering information for a statistical purpose. The questionnaire is entirely dependent on the response of the respondents (Johnson & Christensen, 2004). Qualitative data are collected through closed and open-ended sets of questions in the questionnaire (Root & Draper, 1983).

According to our thesis the author decided to create own questionnaire in order to attempt to discover the main barriers to the stable or rapid introduction of Internet Voting in the USA. The aim of the collecting information from these interviews is to get answers on questions within this research. These interviews were conducted face to face in person in informal and formal ways with different people who agreed to be interviewed for the purpose of research. The interviews are consisted of several questions where there is a choice to choose one answer for statistical purposes and also there is one question where the respondent can add his opinion in more wide answer.

Questionnaire was held in a form of several interviews that were conducted mostly among 50 people living in the state of Illinois.

5 Results from Conducting Interviews

According to the following observation of interviews with almost 50 participants, 39% of respondents from age 51 prefer to vote by ordinary voting, by fax and by electronic machine, all 61% prefer to vote online. To the question why they have chosen Internet Voting, the answer was due to convenience. To the question why they did not choose Internet Voting is due to security concerns.

80% of middle age respondents prefer to vote online, but the trust is 70%.

79% of young respondents prefer to vote online and the trust is 91%.

Among all respondents were a small amount of people who were concerned about security of Internet Voting system. As we are living in the computer age there are a lot of hacking attempts and processes going in the world. Although some respondents expressed their interest as they are partially involved in Internet Voting introduction.

As the observation was made amongst 50 respondents participated in the questionnaire, we consider that observation can be objective but the more number of interview participants will be asked the questions about Internet Voting in other states.

According to the Verified Voting, both e-mailing voted ballots and transmitting them through a Web portal are forms of "Internet voting" and with the proliferation of Internet fax services, we can presume that many voted ballots returned to election officials via fax have in fact been transmitted through the Internet. Thus, 4 states have Internet portal for online voting, 5 states have an opportunity to vote via fax, near 19 states have an opportunity to vote via fax and email and other states, which is approximately half of all states in America do not have any kind of Internet Voting.

Internet voting thus can mean voting from an Internet browser in one's personal computer, or by email attachment, or electronic fax, remote kiosk, or other means of remote electronic transmission and a voted ballot sent through the Internet is no more verifiable than a polling place ballot cast on a paperless direct-recording electronic voting machine – and in fact is exposed to a far greater number of security threats including cyber-attacks such as modification in transit, denial of service, spoofing, automated vote buying, and viral attacks on voter PCs (Verified Voting, 2016).

The lack of credible, peer-reviewed publication outlets is not just an academic concern. Under the present circumstances, it is difficult for policy makers and election officials to distinguish between legitimate and illegitimate research. We have heard this

complaint frequently from election officials and policy makers in recent years. They clearly need access to a publication or research distribution system that identifies credible research (Alvarez and Antosson, 2008).

According to the Rob Philbrick report, Scientific American explains:
"Whereas monetary transactions are based on a firm understanding of your identity, a vote is supposed to be anonymous. [With] bank trouble, investigators can trace a credit-card purchase back to you, but how can they track an anonymous vote? . . . [Banking] fraud goes on constantly [and is built in to the] cost of doing business. But the outcome of an election is too important; we can't simply ignore a bunch of lost or altered votes." Further, personal computers on which votes would presumably be cast are not secure. One need only search the terms "personal computer hack" for recent news on federal hacking charges and major cybersecurity issues. Election officials receiving votes cast entirely online may not be certain that the ballot received even matches the ballot the voter completed (Philbrick, 2016).

According to the surveys that were conducted by the researcher mostly face to face with the respondent, we can make a conclusion that most Americans will definitely use Internet Voting in a secure way, such as using encrypted chip in the ID cards and Driver's License Cards. Citizens are willing to use more convenient way of voting as life in the United States is considered to be super busy, especially in metropolices such as Chicago, New York, San Francisco, Los Angeles, etc. Also many respondents admitted that they are concerned about transparency of voting and its legitimacy process. They underlined that Internet Voting will make government process the vote fairly. The respondents also added that they are willing to see more money saving in Voting processes that make Internet Voting be in priority among all other types of Voting in a long term sence.

Many respondents told in addition that big issue with deploying Internet Voting will be political view. They explained it by the fear of politicians who do not want fair and transparent voting. Other people claimed that there too many hackers that are willing to derail the vote which can mean that they also can steal somebody's identity that can not be reimbursed like usually banks reimburses money to the owners that were stolen by hackers or stock exchange that reimburses stolen funds to stock holders. There were not a lot of respondents that are really against to Internet Voting but critics that they are giving is very essential and crucial to take into account for future introduction of Internet Voting.

6 Recommendations for a Better Implementation Process of Internet Voting in the USA

In this chapter we will attempt to discover recommendation steps that have to be followed to introduce Internet Voting. The researcher in this part will make find out the benefits of Internet Voting and make the conclusions.

According to American citizen's untrusted experience to Internet Voting and Internet overall and taking into account non-stopping rise of every individual privacy saving, we recommend to start Introduction of Internet Voting from the smallest sized places of voting such as universities, schools and small villages. Later on after these pilot testing's are going well we recommend to proceed to a larger amount of voters such as middles-sized towns and then to big cities.

As most of American voters usually voted the whole life at the special places such as precincts we think it will be hard mentally for these citizens to vote from their own computers, laptops and other gadgets from their homes, workplaces and other places. In this case we recommend to make a gradual introduction of Internet Voting next way. The election should be done via Internet but there will be precinct also. A citizen will have a chose to vote at his or her home or to vote from the usual precinct. But at the precinct the voting will be also online and instead of usual voting machines DRE there will be touch-pad and laptops with assistants.

Another way we think can to be counted for consideration is almost the same way as it was described before but additionally to voting online from the precincts, citizens will have an opportunity to choose also to vote as usually they voted with electronic machines. We do not recommend use this way of voting as this will make more complicated counting votes that has to be gathered after. If we use the only Internet Voting, it will be much easier to process and to gather all necessary data. Also, it will make the process more transparent as there will be less inter-processes for gathering the data, namely, identification number, number of votes and other important and sensitive information.

Our view of the Internet Voting from precincts and remote points such as from home, workplace with laptops, tablets, computers and other gadgets, looks like this:

1) There should be a single intuitively understandable interface for the voter, so that the voter does not have the feeling that he is in a different environment

According to the first point, the interface must have all UX (User Experience) standards and also must have state tones. An intuitive understandable interface should have an authorization point where the Social Security Number will be entered, as well as the passport number or ID that will be checked via database through the server. There will also be a photo taken to fix and trace the face of the person who voted on this Social Security Number and the passport number or ID. In case if the voter has a passport number attached to the mobile number, then after entering the Social Security Number, the system will offer additional verification via SMS code, namely to enter the mobile number to which the SMS will be sent. After entering the code with sms, a window for voting will be available.

Also, in the near future it will be possible to introduce an authentication system through the recognition of the retina. But for this it will be necessary to make a number of changes in obtaining passports and the Social Security Number.

2) The interface should be easy to load and have the basic languages of the country and local state

According to the second point, the interface should contain a minimum load on the device of voting owner and should not be heavy for any gadget. The interface must be localized, namely, it must be in the language that is systemic for the device of the voting owner.

3) The web page of the voting site, the device application and the program at the stationary voting stations should be protected as much as possible by the most advanced Internet Security Systems

According to the third point, stationary points of voting should be connected through a special state vpn tunnel (one of the most secure technologies, providing client-server connection at a sufficiently high level, is specifically considered by IPsek because for this task the technology is one of the most protected) and protected by a special Internal encryption key.

Mobile devices must be connected through a special application using the same way wired into the vpn application, or via the browser using the *https* encrypted protocol (currently the simplest for the user and the most common type of protection against man-in-the-middle attacks and, accordingly, from phishing attacks) and save the session with one key.

If the connection is lost, the SMS-based authentication or other types of authorization listed in the first point should be re-passed. Similarly, on stationary computers and laptops, traffic protection through *https* should be used.

4) Internet voting through the online banking system of the most common US banks

No decision has been made in Iowa, but it is only natural that Internet voting is in our future, financial institutions, from banks to the New York Stock Exchange, already securely move trillions of dollars via fiber optics, breaches in security usually come from third parties, such as retailers like Target failing to properly secure stored credit card numbers (Moulitsas, 2014).

It is known, citizens of the United States are very connected with their banks and have a high level of trust in the banking system and its resources. One of the most reliable options of trustworthy voters, will be to introduce a special API to online banking sites of popular banks of the USA.

Firstly, this will give an additional level of protection in the voting, secondly it will serve as a good impetus and push for people's trust for remote Internet Voting. It will look something like this:

a) The voter visits his bank's website;

b) The voter authorizes in the online banking system through his or her an existing account;

c) On the website page, next to the tabs "e-Bills", "Payees" and others, there will be an e-voting tab, the voter goes to this tab;

d) The voter enters the authentication data for voting at the elections mentioned in the point a).

e) The voting is processed. Then this tab will be frozen.

5) Receiving server data for voting

It is supposed that because of the contagion of the real voting system and which are going to be represented in the future, there will be a need to rework the server portion of the Internet voting. In addition, due to the mobility of the vote, the people will be able to take an active part not only in the presidential elections but also less significant ones.

The server part should be reworked as follows:

a) The central server that processes and counts all the votes at the final stage must be in the most secure network, blocking any incoming traffic from outside, except for the encrypted VPN traffic of the regional servers (the state's central servers that count state voices) on the server stand located directly next to the server. And any access to it is restricted until the end of the election.

b) The central server of the state, it is necessary to place in the state capitals, which receive data from all devices and stationary points of voting. They will be the main load, because it will handle and check keys, identifiers and other data. They will also be intermediate servers for reconciling data with those who voted and did not vote, referring to the central server.

6) Sending client-server information

The transfer of this information will be done by encapsulating the voting result, the identifier, the special encryption key, the geo-tag, the IP device from which the voting was carried out or the identifier of the stationary voting station, as well as the photo from the devices captured during authentication.

7) Voting from abroad

Voters who are outside the country at the time of the elections with internet voting will have to undergo additional authorization. And they should be on the lists of citizens temporarily or permanently leaving the United States of America. All the data on the citizens who left the country is given by the relevant authority the day before the election.

8) Feedback system as an added security

But what if to introduce the system of feedback into process of voting? What are politics and people afraid of most? They are afraid that the vote will go to the wrong direction and nobody will even know about it. So, what if after there is a special confirmation of voters?

This should be look like in Figure 1.

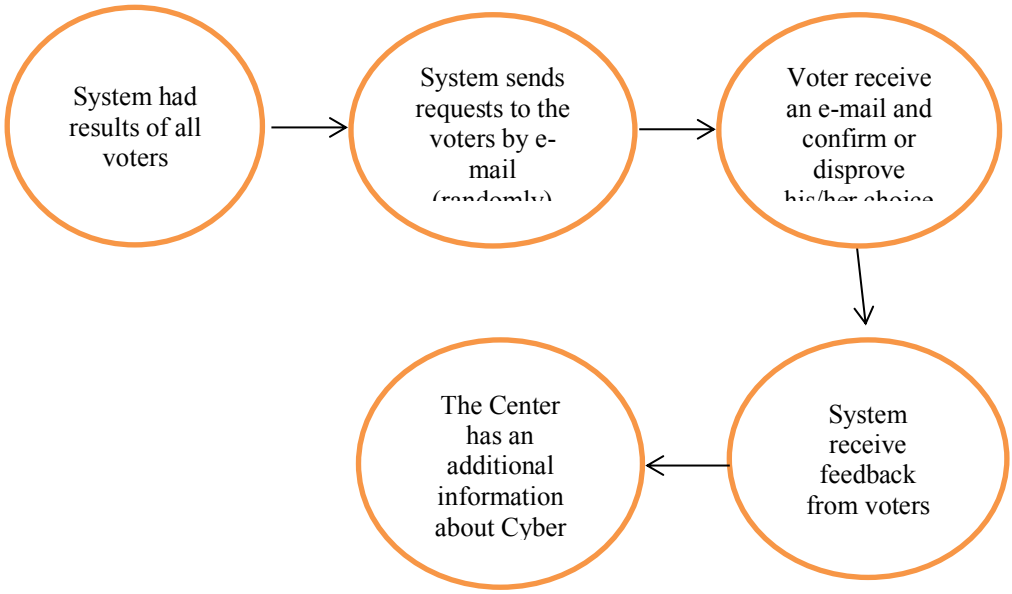

Figure 1. Internet Voting with feedback system

After the process of voting closed the system makes the counting of votes. When the process will be finished, the system will send the message-inquiry to the voters that were selected randomly (in this case it is exclusively about that who used Internet Voting). In that message there will be indicated information about to which candidate the voter gave his or her vote with a request to confirm is it true by following the link or disprove by clicking another link.

Thereby, Center of counting votes will get feedback or responsiveness from voting citizens and will be able to form statistics. If more than 50% of voters did not approved their choices then we can assume that system has been cyber attacked by hackers and we have to undertake appropriate measures.

In my opinion, such process of a feedback will complicate and puzzle possibility for hackers to fake the votes. Respectively it will give a chance for rapid development of Internet Voting in the USA.

By the present time, there are a number of works devoted to the creation of secret e-voting protocols. All existing protocols are divided into three types:

1) Voting protocols with mixing;

2) Voting protocols using blind-letter technology;

3) Voting protocols with separation, in which personal ballots are divided between different counting commissions so that none of them can falsify the results of counting the votes.

Another good idea of introducing Internet Voting in the United States is adopting Internet Voting system from a different country which is already successfully conducting voting online not the first year. One of the first steps is to employ base similarly to X-Road in Estonia. Parallel with that base state should produce the card with chip in that will secure the identity from every citizen.

6.1 Benefits from Recommended System

Considering the recent elections in the USA in 2016 and the sensational story of the so-called "Russian hackers," the new system will be more resilient to hacking, as in addition to the usual voting result, information will be transmitted about the location of the voter, his or her IP address, photograph, social security number, Passport ID or mobile phone numbers, considering these data it will be extremely difficult to crack and/or replace the voice.

Even if somehow the system is hacked and the voices are replaced or added, it will be easy to find out if there are no identifiers and data.

But when was the last time Goldman Sachs was hacked? We have the technology and know-how to secure our most vital digital assets, creating an online voting system, while not trivial, would be possible given current technology, and that technology improves every day (The Hill, 2014).

According to the report of Galois, E2E-V offers a dramatic improvement in the security of voting systems. E2E-V is an End to End Verifiable Internet Voting. In this report he said that while it is necessary for any online voting system for public elections, it is by no means sufficient and once it is embedded in a larger Internet voting context

fundamental new security vulnerabilities appear for which there are no solutions today, and no prospect of solutions in the foreseeable future.

In his report he also added that these include vulnerability to authentication attacks, client-side malware attacks, and DDoS attacks that can be perpetrated by anyone in the world unless and until those additional security problems are satisfactorily and simultaneously solved—and they may never be—we must not consider any Internet voting system for use in public elections (Galois, 2015).

Many researchers, experts, academicians, politics, scientists do not believe in the future of Internet Voting in the USA giving arguments that at any stage (beginning from building server at the factory and finishing by installation of software) it is possible freely expect Cyber Attack. Such arguments that in that process there will be involved so many people that to control from the very beginning till the very end everybody will be almost impossible. They cannot be sure 100% that every involved person or organization of the process will not be corrupted. I cannot agree with this opinion. Yes, to believe in the future of Internet Voting in the USA is becoming harder after listening so strong arguments. But the examples well working and functioning realizations Internet Voting in Estonia, Switzerland and Australia make think the other way. There should be the right ways of solutions.

The main and most distinctive feature of the USA from above mentioned countries is its size, the number of living people in the country and global attractiveness at the world arena. By attractiveness we mean that the USA is most interesting country for hackers. This indicates that to plan, organize and control such a huge number of people more complicated that temptation for a hacker to brake and hack the above system of Internet Voting.

7 Conclusion

The development of Internet voting systems, which began in the last decade of this century, was due to the rapid development of information and communication technologies, the expansion of citizens' access to the Internet and was accompanied by an increase in hopes for further strengthening of democracy. As Lauder notes in this connection, the Internet is able to provide both a higher level of transparency and new ways of political communication. An idea was also put forward to use it for holding elections and referendums. It was assumed that interactive elections could make the election process simpler and cheaper, and vote counting was more rapid and reliable. Reducing costs, as expected, could also give a new impetus to the development of direct democracy tools.

Existing systems of electronic voting presuppose both direct application of Internet technologies to take into account the will of citizens, and the use of special devices, like electronic urns.

Internet voting is designed for remote participation of voters in elections. Instead of voting at a polling station, citizens can use either special computers that are installed in the polling booths, or by an ordinary computer at home or at work, which has an Internet connection. Having joined the network with the server of the local election state and having passed the procedure of electronic authentication, the voter instead of marking the candidate's name in the regular bulletin simply pushes the necessary buttons on the computer or gadget.

To implement the electronic provision of services, by using Internet voting as an alternative to providing voting types, even waiting for the submission of proposals that are mandatory for consideration by the relevant public authorities, but not for a positive decision, constitutional changes are not required.

As a last resort, it is only necessary to issue an all-state normative act regulating these issues. Constitutional changes are obviously required for the implementation of the electronic type of voting as a concept of innovative legal mechanisms for the exercise of democracy, the final result of which is mandatory in the legal sense.

Nevertheless, despite the above criticisms, international recommendations are a significant source and, probably, the main one in the absence of comprehensive and

understandable domestic regulation, in order to determine the compliance with the constitutional requirements of the electronic voting system and the system of electronic democracy.

That is why the replacement of traditional voting by electronic need to be carefully considered. It seems that in general, within the framework of the election voting system, it is necessary to single out several basic concepts that determine the degree and level of legal regulation, in particular, the definition and modification of constitutional duties and even the powers of officials.

In order to come to some kind of common denominator, we need to analyze the relationship between the benefits of introducing Internet voting from the possible external and internal problems and risks. At the beginning we will look at the external and internal problems and risks.

According to the conducted interviews among US residents, the biggest external risk is in hackers that are willing to hack the system and mask their location so it will be almost impossible to track them. One of the interviewers noted that he is afraid that "Russia can take control over US elections, I know because I am programmer over 10 years". Based on that answer author can assume that the biggest problem is not an external but internal as it can be hidden inside the USA. According to the results received from the conducted interviews, author can mention that a lot of people do not trust system of internet voting. One of the reasons of such scare is that during running elections in the US candidates and their sponsors spend billions of money and try to win by any opportunity using corruption schemes. One of the respondent mentioned, "So why not having an opportunity to control the count over the Internet". Based on that the author can assume that having such thoughts in people's minds, introduced internet voting can be easily blacken by political party as a not fair elections. Therefore there is a link between people's mistrust and scare, hence there is a connection between people's scare and unawareness of reliability of the proposed Internet voting system and how it works.

One of the benefits is money saving. In 2009, cost estimates from Internet voting vendor Everyone Counts were so large that a legislative proposal in Washington State to allow Internet voting for military and civilian voters was killed in committee. The estimated costs, obtained by John Gideon of VotersUnite, included proposed up-front

costs ranging from $2.5 million to $4.44 million. After that, each county would have been hit with an annual license fee of $20,000-$120,000, plus $2-$7 per overseas voter (DeGregori, 2009).

More that 46 thousand people voted via Internet voting system iVotes in 2011 election in the state of New South Wales, Australia, also an Everyone Counts product (Report on the Conduct of the NSW State Election, 2011). The implementation and development costs for using iVotes in the election exceeded $3.5 million (Australian dollars), resulting in a cost of about $74 per vote cast. With a contrast, the average cost for all forms of voting in the same election was $8 per vote, though the cost per Internet vote would have decreased if amortized over more voters (Simons and Jones, 2012).

Second benefit of the voting is increasing the voting turnout. Finally the Internet can bring full voter participation. The more convenient and timesaving voting will be the more citizens will be motivated to participate. At least, security is at the high level so everybody will trust the Internet Voting System. But despite warnings about insecurity of Internet Voting there are more issues with citizens and experts untrusty to electronic Voting Machines such as DRE, voting via Fax and others. According to that we can assume that there is no voting system today in USA which is 100% secure and the reason why we should continue to take the direction in the Internet Voting is as it has more benefits than other types of voting.

Third thing why Internet voting is better than any other kind of voting is that it is web-based voting. Web-based voting is considered to have more security by its transparency and verifications. To avoid such risks like bugs or hack-attack there should be a special check of the software that will show if the system is working well even during the election.

In conclusion we can mention that Internet Voting is money saving, increase the voters' engagement by their turnout, is more secured by its web-based voting.

At the same time there a lot of risks that are lied in the nature of Internet itself. According to the interviews there was a number of respondents that are concerned about security issue of Internet Voting, specifically security of identity of every person and his or her vote.

Based on surveys from many interviews we can conclude that Internet Voting is more transparent, is more feasible to see the errors and mistakes during the election period and is able to trace any hackers track. According to the interviews Internet Voting will be

introduced after serious checks from hackers and other professionals that will ensure the highest security level of Internet Voting system.

Eventually, all the existing voting systems except Internet Voting are not more secure than Internet Voting itself. Thus, we can admit that Internet Voting in the United States should be applied in the very near future.

References

"i-Voting", accessed March 2017 e-Estonia http://e-estonia.com/component/i-voting/

Alvarez M., Hall T. and Trechsel A. (2009) *Internet Voting in Comparative Perspective: The Case of Estonia*

Appel A. (2016) *Internet voting? Really?*

Axelsson, K., Melin, U., & Lindgren, I. (2013). *Public e-services for agency efficiency and citizen benefit—Findings from a stakeholder centered analysis*

Andreu Riera and Paul Brown (2003) *Bringing Confidence to Electronic* Voting Online World Security, S.A., Barcelona, Spain

Barbara Simons, Douglas W. Jones (2012) *Internet Voting in the US* https://cacm.acm.org/magazines/2012/10/155536-internet-voting-in-the-u-s/fulltext#comments

Beth Clarkson (2015*) How trustworthy are electronic voting systems in the US* https://www.statslife.org.uk/politics/2288-how-trustworthy-are-electronic-voting-systems-in-the-us

Bill Jones (2000), Report on Feasibility of Internet Voting *California Internet Voting Task Force* California of Secretary Bill Jones

Bogdan, R. & Taylor, S. J., (1975) Introduction to Qualitative Research Method – A Phenomenological Approach to the Social Sciences, New York: John Wiley & Sons.

Budd, L. & Harris, L. (2004). E-Economy: Rhetoric or Business Reality, Routledge, London.

Buchsbaum T. (2004) *E-Voting: International Developments and Lessons Learnt*

California Internet Voting Task Force, *A Report on the Feasibility of Internet Voting*, January (2000), p. 2, http://elections.cdn.sos.ca.gov/ivote/final_report.pdf

Cambridge Advanced Learner's Dictionary and Thesaurus, Cambridge University Press. http://dictionary.cambridge.org/dictionary/english/voting

DeGregorio, P. (2009) *UOCAVA Voting Scoping Strategy*. Washington Secretary of State Public Record, http://www.votersunite.org/info/WA-PRR-scopingstrategy.pdf

Electronic Journal of e-Government Volume 2 Issue 3, (2004)

"Electronic Voting". lorrie.cranor.org/pubs/evoting-encyclopedia.html

Ezze, D. (2015) Qualitative Analysis

Galliers, R., (1994) Information systems research, Waller

Galois Joseph R. Kiniry, Ph.D., Daniel M. Zimmerman, Ph.D., Daniel Wagner, Ph.D., Philip Robinson, Adam Foltzer, Shpatar Morina (2015) *The Future of Voting End-to-End Verifiable Internet Voting* U.S. Vote Foundation

Garson, D.G. (2006). *Public Information Technolpgy and E-Governance*. Sudbury, MA: Jones and Bartlett Publishers

Given, Lisa M. (2008) *The Sage Encyclopaedia of Qualitative Research Methods*

Goos G., Hartmanis J. and Leeuwen J. (2001) *Sowtware Engineering for Secure Systems: Industrial and Research*

Hakim, C., (1987) Research Design Strategies and Choices in the Design of Social Research. London/New York: Routeledge.

Hans von Spakovsky (2016) *The Dangers of Internet Voting*
http://www.heritage.org/report/the-dangers-internet-voting#_ftn38

How Electronic Voting Could Undermine the Election (2016) https://www.theatlantic.com/technology/archive/2016/08/how-electronic-voting-could-undermine-the-election/497885/

How online voting works retrieved from usatoday.com.

Holden, S. J.; Norris, D. D.; Fletcher, P. E. (2003). *Electronic government at the local level: Progress to date and future issues*. Public Performance and Management Review (36): 325–344.

Holden S. and Millett L. (2005) *Authentication, privacy, and the federal E-Government*

Internet Voting in Estonia (2015) http://www.vvk.ee/voting-methods-in-estonia/

ISO/IEC (2011), A Framework for Identity Management – Part 1

J. Alex Halderman and Vanessa Teague (2015) *The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election* University of Michigan and University of Melbourne https://www.verifiedvoting.org/wp-content/uploads/2016/08/Teague_Halderman_2015.pdf

Johnson, B., & Christensen, L., (2004). Educational research, 2nd edition. USA: Pearson Education.

Kevin Kwang Chanel NewAsia (2017) *National Digital Identity system to be cornerstone of Singapore's Smart Nation vision*
https://www.channelnewsasia.com/news/singapore/national-digital-identity-system-to-be-cornerstone-of-singapore-9140090

Kiayias A., Korman M. and Walluck D. (2006) *An Internet Voting System Supporting User Privacy*

Knowledge Society Agency UMIC (2008) *Electronic Voting Experiments in Political Elections around the World*
http://www.english.umic.pt/index.php?option=com_content&task=view&id=3113&itemid

Krimmer R., Triessnig S. and Volkamer M. (2007) *The Development of Remote E-Voting Around the World: A Review of Roads and Directions*

Markos Moulitsas (2014) *Voting Online Is the Future* The Hill http://thehill.com/opinion/markos-moulitsas/206047-markos-moulitsas-voting-online-is-the-future

Maxwell, K. J. (2015). Voting. *The New Book of Knowledge*. Retrieved from Grolier Online http://nbk.grolier.com/ncpage?tn=/encyc/article.html&id=a2031120-h&type=0ta (use the date you accessed this page)

Mellenbergh, G.J. (2008) *Tests and Questionnaires: Construction and administration.* In H.J. Adèr & G.J. Mellenbergh (Eds.) (with contributions by D.J. Hand), Huizen, The Netherlands: Johannes van Kessel Publishing.

Mercurio B (2004) *Democracy in decline: can internet voting save the electoral process?*

Mohen J. and Glidden J., 2001 *The Case for Internet Voting* Communications of the ACM, 44, 1, 72 – 85.

New South Wales Electoral Commission (2011) *Report on the Conduct of the NSW State Election;*
http://www.parliament.nsw.gov.au/Prod/parlment/committee.nsf/0/67f2055c4d085409ca25795a0017cf2c/$FI

Osaki, Tomohiro (2015) *Ready or not, government will soon have your My Number*

Patton, M., (1990) Qualitative Evaluation and Research Methods, California, CA: Sage Publications.

PCEA, (January 2014) https://www.supportthevoter.gov/files/2014/01/Amer-VotingExper-final-draft-01-09-14-508.pdf.

R. Michael Alvarez and Erik K. Antonsson (2008) *Bridging Science, Technology, and Politics in Election Systems*
https://www.nae.edu/Publications/Bridge/VotingTechnologies/BridgingScienceTechnologyandPoliticsinElectionSystems.aspx

Rob Philbrick (2016), *Flying Pigs to Precede Comprehensive Federal Internet Voting Regime in United States* Privacy, Technology, University of Washington School of Law https://wjlta.com/2016/11/08/flying-pigs-to-precede-comprehensive-federal-internet-voting-regime-in-united-states/

Root, R. W. & Draper, S. (1983). Questionnaires as a Software Evaluation Tool Interface Design 4 -- Analyses of User Inputs. Proceedings of ACM CHI'83 Conference on Human Factors in Computing Systems 12 December 1983: 83-87.

S.A.Makedonskiy and V.S.Lukjanov (2007) *Analysis System of Electronic Voting* Volgograd State Technical University

Santos R., (2018) The Holistic Cyber Security Approach

Tan, C. W., Shan, L., Pan, S. L., & Lim, E. T. K. (2005) *Managing stakeholder interests in E-Government implementation*

The Straits Times (2018) *National digital identity system to be rolled out in second half of 2018*

https://www.straitstimes.com/politics/national-digital-identity-system-to-be-rolled-out-in-second-half-of-2018

Thomas W. Lauer, (2004) *The Risk of e-Voting* School of Business Administration, Oakland University, Rochester, USA p169-178

Unwin, Tim, (2009) ICT4D: *Information and Communication Technology* Cambridge University Press. p. 9

Usa.gov (2016), https://www.usa.gov/voter-id

Verified Voting (2016) https://www.verifiedvoting.org/internet-voting

Voting online is the future (2014) http://thehill.com/opinion/markos-moulitsas/206047-markos-moulitsas-voting-online-is-the-future

Wired (2016) America's Electronic Machines are Scarily Easy Targets https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/

Appendix – Interview questions and results

These questions were provided by the researcher among 50 respondents in Chicago state of Illinois.

1) What is your first name?
2) How old are you?
    a) 18-30
    b) 31-50
    c) from 51
3) Do you vote in the government elections?
    a) yes
    b) no
4) What kind of preferences you have to log into the online system?
    a) State ID card
    b) Driving ID
    c) State ID card/Green Card ID/Passport/Passport Card
    d) Green Card
    e) Passport / Passport Card
    f) Social Security code
    g) Email account
    h) Mobile phone number
5) What type of voting do you use?
    a) Electronic voting or DRE voting machine
    b) Internet registration online
    c) Regular paper voting at the precinct
    d) Mail paper voting
    e) Fax voting
    f) Email voting

6) Which method of voting do you prefer to use?
   a) Internet voting via website
   b) Internet voting via mobile application
   c) Only Internet registration
   d) Electronic voting machine or DRE
   e) Paper voting at the precinct
   f) Mail voting
   g) Email voting
7) Would it be convenient for you to vote via smartphone or laptop/pc?
   a) Yes
   b) It would be convenient voting via website
   c) It would be convenient voting via smartphone
   d) No
8) How often do you use pc/laptop/smartphone, for example, checking emails?
   a) Every day
   b) Once a week
   c) Rarely
   d) Never
9) How often do you use pc/laptop/smartphone for log into Internet Banking?
   a) Every day
   b) Once a week
   c) Rarely
   d) Never
10) How often do you use pc/laptop/smartphone for online purchasing?
   a) Every day
   b) Once a week
   c) Rarely

d) Never

11) Will you vote online if voting via the Internet would be secure?

a) Yes

b) I will vote through the website

c) I will vote via smartphone

d) No

12) If you do not want electronic voting, what is the reason?

a) I do not trust

b) I do not vote

c) *Personal opinion*