Feasibility Study

On the Introduction of New Elections Technology for Ukraine

February 2020

INTERNATIONAL FOUNDATION FOR ELECTORAL SYSTEMS
IFES
30 Years

Feasibility Study

On the Introduction of New Elections Technology for Ukraine

February 2020

This study is made possible by the support of the United States Agency for International Development (USAID), Global Affairs Canada and UK aid. The opinions expressed herein are those of the author and do not necessarily reflect the views of USAID, the United States Government, Global Affairs Canada, the Government of Canada or the UK government.

Feasibility Study: On the Introduction of New Elections Technology for Ukraine

International Foundation for Electoral Systems
2011 Crystal Drive, 10th Floor
Arlington, VA 22202
E-mail: editor@ifes.org
Fax: 202.350.6701

Cover photo: Glenn Carstens-Peters / Unsplash

Table of Contents

Executive summary

At the request of the Ministry of Digital Transformation, the International Foundation for Electoral Systems (IFES) conducted a Feasibility Study on the introduction of new elections technology for Ukraine. The request was consistent with the July 2019 Presidential Decree calling for, amongst other things, the moving online of the procedure to change voting addresses and the introduction of Internet voting. IFES welcomes the inclusion of the management of elections in the vision to digitally transform Ukraine.

Consistent with IFES' remit and international experience, the study team took an elections-management centric approach to start the study by researching and asking numerous interlocutors not "how do we implement Internet voting" but rather "what are the problems with elections in Ukraine, and how can technology help solve them." The latter approach allowed IFES to engage with multiple stakeholders in an open and candid discussion to fully inform the technology choices and options. Given the enormous scope of the topic and the limited time for the study, the report is concise and necessarily brief. For any new technology under consideration for elections, the impact on core electoral principles must be positive and meaningful. Does it add to electoral integrity? Does it help to bring more voters into the process? Does it make electoral officials and parties more accountable? And does its introduction add to or require greater stakeholder trust?

The interlocutors[1] interviewed for this study included all political blocks in the *Verkhovna Rada*, the Central Election Commission (CEC), the State Register of Voters (SRV), citizen observers, civil society, providers of technical assistance, relevant actors in the identity and eDemocracy field and a variety of other state agencies (ranging from strategic planning to cybersecurity). In meetings, the Feasibility Study (F/S) team followed a semi-structured interview approach, using a visual aid[2] that helped them walk through the entire electoral cycle and prepared questions, while leaving adequate opportunities for open discussion with interlocutors. The F/S team sought to determine, without leading the discussions, social demand for and knowledge of specific new technologies. Further, the F/S team assessed the capacity of and trust in the institutions responsible for any implementation.

While there appears to be no significant bottom-up demand for Internet or electronic voting, interlocutors, by and large, supported the Government's initiative in principle. Objections to Internet or electronic voting were focused on the cybersecurity risks. Most interlocutors cautioned a step-by-step approach, with incremental piloting and introduction, in parallel with efforts to build capacity and trust in voters.

Interlocutors did raise other issues with elections in Ukraine, notably difficulties with voter list amendments and political party access to these lists, as well as with the management of results from PEC[3] through DEC[4] to CEC. Closer analysis of the results management processes reveals human resource and infrastructure deficiencies, whose effective remedy is overdue. CEC has a new technical solution in the pipeline, which can go some ways towards improving results management. There is a

[1] See Annex 9.5
[2] See Annex 9.3
[3] Precinct Election Commission, at polling station level.
[4] District Election Commission, the first point of consolidation of electoral results

need to address the too-little training delivered to too-few PEC members[5], and address the "incessant[6]" and politically-motivated rotation of staff. This training – and maintaining these trained staff - becomes even more essential with anticipated changes to the electoral system and legal framework or if new technology is introduced. The investment in this human capacity must be protected from erosion by eleventh-hour rotation of personnel. As currently resourced, the CEC is not quite ready to implement a high-tech results management system at the PEC level. It follows that the same goes for any electronic voting systems under consideration.

On the voter list issue, the CEC also has a mature and ready-to-implement plan to implement online changes to voter addresses. While some interlocutors think this does not go far enough, and others point to the potential for possible manipulation, the CEC must be encouraged to proceed. Most interlocutors, especially political parties, complained about the poor access of electoral stakeholders to voter lists. In order to build on the success of 2019 elections (where, with minor exception, stakeholders accepted that the CEC and SVR delivered good voter lists), CEC should engage with electoral stakeholders to agree on access mechanisms for future elections.

Turning to electronic or Internet voting, IFES found that most interlocutors spoke of concerns regarding the manipulation of technologies and did so in the context of the elevated cybersecurity threats faced by Ukraine. It is recognized that any new technologies (throughout the electoral cycle) in Ukraine would require greater-than-average risk analysis and more resources for cybersecurity than might be the case in other countries. Unfortunately, the lack of detailed knowledge about Internet (remote/unsupervised) voting led many interlocutors to wrongly assume that if the systems were protected from hackers, there were no other major issues to be addressed. It will take time and significant effort to introduce new voting concepts implied in electronic/Internet voting, and to allow the debate on their introduction to be an informed one. Authentication (identifying the voter) and coercion (protecting the secrecy of the ballot) are issues that need to be more fully understood and widely debated in Ukraine.

The report considers three international case studies, Estonia, Moldova and Switzerland, and lists lessons IFES believes those countries offer to Ukraine. Estonia, for example, built its eVoting solution on top of a long-accepted and mature e-governance and ID platform. The report also outlines some hard and soft international legal obligations, most notably the comprehensive 2017 Council of Europe Recommendations.

Most interlocutors spoke of a lack of trust in the CEC, though the trend in public surveys[7] is positive. This is despite a positive acknowledgement of good 2019 electoral events. Interlocutors spoke of the CEC as lacking autonomy. Recognizing the paradigm shift that would accompany any introduction of electronic or Internet voting, the key question the report asks is how would Ukrainian voters learn to use (a technical question) and learn to trust (a socio-political question) electronic or Internet voting.

[5] IFES partners with the CEC Training Centre to deliver cascade training. CEC's lack of resources at field level constrains both the number of PEC staff who receive training as well as the duration of that training.

[6] OSCE Final Report, Presidential Election 2019 in Ukraine, page 4 https://www.osce.org/odihr/elections/ukraine/439631

[7] For example, IFES' Ukraine Post-Parliamentary National Survey "The percentage expressing at least a fair amount of confidence in the CEC increased from 41% last year to 64% following the 2019 parliamentary elections." https://ifesukraine.org/key-findings-ukraine-post-parliamentary-election-survey-october-2019/?lang=en

The CEC can earn trust by implementing short-term reforms of voter registration and results management processes already under consideration.

Initiatives are underway to further address voters' capacity to use and trust elections technology. The Ministry of Digital Transformation has ambitious plans to raise digital literacy for 6 million Ukrainians in a three-year window. EGAP[8] and TAPAS[9] are engaged in eDemocracy and foundational identity initiatives. CEC must play its part too and lead efforts to research, experiment and pilot appropriate new elections technologies.

The study makes a number of recommendations, of which the following would be considered key. The new CEC should focus its short-term efforts at addressing the long-recognized deficiencies in electoral processes, namely the management of results at all levels, the streamlining of voter list change of address processes and the professionalization of staff in the field. Existing initiatives at the CEC are the perfect starting point and should proceed. These initiatives should be given a legal basis and adequate resources. A significant nationally-owned research and development initiative, led by the CEC, and focused on determining what models of electronic and Internet voting are appropriate for Ukraine, should commence as soon as possible. Finally, experimental use of new voting technologies should be undertaken between 18 and 24 months prior to any election. Piloting in small scale elections may follow and, contingent upon the findings of reviews and prevailing conditions, a decision to offer limited electronic or Internet voting options for Presidential and *Verkhovna Rada* elections in 2024 can be taken.

Background & Introduction

Background

Following the presidential election in March/April 2019, and early parliamentary elections in July 2019, the newly elected government of Ukraine has expressed the desire to intensify the use of technology in elections by instituting Internet voting and online services for citizens to update their voter records. While this type of project would typically require an extended timeline, the government has stated its intention for this to occur as early as the next local elections currently scheduled to take place in October 2020. In this context, the government has requested IFES' support in creating a joint team responsible for assessing the feasibility of developing and deploying new elections technologies in Ukraine.

Introduction

The aim of the "Feasibility Study on New Elections Technologies" (F/S) is to look at potential new technologies available that could be used in Ukraine to strengthen the electoral process. These may include: Internet-based registration and voting, and improvement of the digital result transmission and results management systems. The F/S should provide Ukrainian stakeholders with an important background and risk/benefits analysis, allowing them to make informed decisions regarding possible next steps, while being fully cognizant of the international standards to which they need to adhere. These standards are, in the main, the Universal Declaration of Human Rights, the International

[8] E-Governance for Accountability and Participation (EGAP), see http://egap.in.ua/en/
[9] Transparency And Accountability In Public Administration And Services, see http://tapas.org.ua/en

Convention on Civil and Political Rights (ICCPR), 1990 Copenhagen Document and the Venice Commission Code of Good Practice in Electoral Matters and the 2017 Council of Europe Recommendation CM/Rec (2017)5 on Standards for eVoting.

The F/S was conducted from October 7 – November 30, 2016 by IFES' International Consultants, Ronan McDermott and Thomas Chanussot, and included Vladlen Basysty and Olha Antonova from the IFES/Ukraine team.

The F/S was prepared in accordance with the approved Terms of References stipulated by the Minister of Digital Transformation, and contains the following provisions:

- A series of meetings with the representatives of government officials, Central Election Commission (CEC) and other key government representatives, political parties, civil society and other relevant stakeholders to ensure an inclusive and wide-ranging process (see Annex for full list of conducted meetings);
- An analysis of international good practice in implementation of election technology;
- An analysis of the legal, technical, social and political environment in Ukraine, using the results of interviews, available documentation and personal observations, will be contained in the Key Findings section of this report;
- Short-, medium- and long-term strategy recommendations for implementing the use new election technology will consider all factors: participation, cost, transparency, efficiency, security, verifiability, integrity, credibility, legitimacy, universality, secrecy, accountability, and trust;
- A high-level roadmap of recommended implementation schedules with an estimation of the budget requirements will be included to guide stakeholders.

Methodology

The F/S team reviewed existing literature on elections technology from multiple sources, including international observation reports, mass media pieces, academic publications, vendors' white-papers and election management bodies' (EMB) releases.

The F/S team also reviewed existing legal and technical documentation and conducted interviews with relevant Ukrainian stakeholders in order to understand the maturity and current capacity of the technical infrastructure with regards to cybersecurity, data protection and voter identification.

Key Findings of the Study

The following are the key findings made by the team:

Finding 1

Results management was the most criticized aspect of the election management process, with voter registration processes such as changing voter addresses and access for parties following thereafter. There is still largely a problem of trust with the lower level of administration of the electoral process, with poor training and politically-motivated personnel changes. This lack of trust particularly manifests at the PEC level contributing to the spectrum of error and manipulation of results protocols. **The transparency and efficiency of the transmission and management must be improved.** While any new technology implemented at the local level would be a welcome improvement, **it needs to be complemented with more training and the professionalization of the DEC and PEC staff. Technology that improves the inclusivity and transparency of the election process should take priority in the short term.**

Finding 2

The July 2019 Presidential Decree is the primary driver of all current digitization initiatives. Online change-of-address processes and electronic voting are both explicitly called for in the decree, in the context of wider e-governance. There is no evident bottom-up demand for electronic or Internet voting. **Electronic voting and Internet voting are perceived as solutions for problems that have not yet been defined. Most interlocutors, while supporting their incremental introduction, see voter registration and results management as the priority electoral processes for attention in the short term.**

Finding 3

The CEC has established, ready-to-implement plans to extend the use of elections technology that represent natural evolutions of existing systems. Based on consultations with stakeholders, the feasibility and willingness to launch these plans were not really in question, but security concerns and cost may have been the main arguments preventing the piloting and further discussions of these new technologies. Despite important improvements in 2019 with regards to cybersecurity, the CEC continues to express that new technologies for the electoral process should be accompanied by increased security capacity for the commission. However, technology alone cannot address the issue of professionalization of PEC (and DEC) staff and the elimination of political manipulation of election personnel. **Field-deployable technologies require significant new investments in staff training and support, over and above the solutions themselves.**

Finding 4

The Ukrainian government is currently developing strategies to increase the level of use of information technology globally. **Several interlocutors believe that trainings and incentive programs can create a shift in Ukrainian society and convince a larger portion of the population to use e-services and eventually Internet voting**. It is worth noting that 69.4 percent of the population of Ukraine live in

urban centers, while the remaining 30 percent live in under-developed, low Internet penetration areas that could be left without Internet voting and other e-services.

Finding 5

There are a number of perceived challenges facing the implementation of new technologies, such as infrastructure, cybersecurity, institutional/voter capacities and the likely political polarization on new technologies. However, the challenge raised the most frequently by interlocutors was that of trust. Trust in any new technology is essential, but trust in the institutions implementing the technologies is an even larger issue in Ukraine**. In report after report, and in meeting after meeting, a lack of trust towards governing institutions was directly cited or implied.** Despite acknowledging that **all three 2019 electoral events were managed more efficiently than previous ones**, most interlocutors spoke of the CEC as lacking autonomy. Anecdotally, the CEC was described variously as "a tool, an instrument," "powerless over the actions at [the] PEC level," and "in dire need of professionalization at [the] field-level."

Finding 6

There is no specific program to teach how to use and trust technology in general, and certainly not for election technology. Following extensive local educational campaigns, the E-GAP program has reached 15 percent participation of citizens using e-services. The development of e-services in Estonia took nearly a decade to develop with a much smaller citizen base. New generations will adopt new technologies, but it is recognized from experience in Ukraine and internationally that education has a marginal impact on adoption.

Finding 7

Through partnership and close collaboration with national and international entities, the CEC has increased its cybersecurity resilience. The commission demonstrated its leadership during the 2019 presidential and parliamentary elections, effectively defending the infrastructure on which the elections rely. According to stakeholders consulted during this study, **Ukraine remains a high-risk environment with regards to cybersecurity**, and there should be no complacency. Cyber-attacks, whether state sponsored or criminally motivated, continue to plague Ukrainian critical infrastructure and private business. **Any new technology should hence not be introduced without first conducting a thorough risk analysis** to determine the resulting type of vulnerability that could in turn be introduced and how it can be mitigated. Cybersecurity risk analysis and mitigation strategy should thus be driven by the CEC with support from national cybersecurity agencies.

Finding 8

While stakeholders understand the role that cybersecurity and the perception of cybersecurity can play in the credibility of future elections, there is a **misconception that if the cybersecurity aspects of Internet voting can be fixed, other aspects such as voter information, public trust, coercion, or political buy-in would be easy to address**. Experiences worldwide have shown that, while the technical and cybersecurity aspects are not easy to resolve, it is only one part of the complex jigsaw composed of social and political components as well as cryptographic and technical factors. **New technology introduces concepts (such as cryptography, secrecy, coercion, verification) whose complexity will require time to be fully understood by government bodies, political parties, and the**

public. The CEC will also have to address public concerns and the perception of cybersecurity risks from the perspective of a heterogeneous population. The focus on cybersecurity is understandable from the perspective of Ukrainian stakeholders, as the country has been the victim of several waves of cyberattacks in the context of the ongoing hybrid war with Russia. Several **interlocutors suggested Internet voting as a means to enfranchise Ukrainian citizens in areas out of the control of the government, without considering coercion or authentication issues.** In general, interlocutors with greater knowledge of and experience with elections are aware of such issues, but many others were not.

Finding 9

The cost and timing on the deployment of any new election technology will be tightly linked to the governance model. While stakeholders indicated a preference for developing technology in-country and establishing a pool of experts in the government and academia, the cost and timing imposed on the adoption of technology might not provide the necessary environment for its emergence. The CEC's full ownership and control over election processes will be complicated by the introduction of new technologies. With greater dependence on other agencies and vendors, the CEC will be challenged to retain and demonstrate complete operational autonomy.

Finding 10

The CEC lacks sufficient resources to undertake the necessary training to ensure adequate numbers of qualified poll-workers. The CEC relies to varying degrees upon other state agencies and international technical assistance in many aspects of its ICT infrastructure and operations, including cybersecurity. **The CEC may be considered to be under-resourced and under-staffed with respect to its current mandate.** Radical change in the electoral system or the introduction of new technologies (or, in a worst-case-scenario, both simultaneously) are beyond the CEC's current capacity. If the CEC is to move forward with planned initiatives (online change-of-address and improvements to results management systems) and take an appropriate leadership role in the piloting and introduction of electronic or Internet voting, the Government of Ukraine must significantly increase the human and financial resources available to the institution.

Finding 11

A technically reliable, universally adopted, nationally owned and widely **trusted ID mechanism is a necessary prerequisite for the conduct of binding elections electronically.** In parallel with the efforts to deliver on a unified national identity mechanism, initiatives in eDemocracy and eGovernance will expose Ukrainian citizens to the concepts and practicalities involved. While still in the early stages, **the e-cabinet, with its identity infrastructure, is a promising project that could serve as a strong foundation for improving the electoral process**, **for example by facilitating access to voter list information for voters as a first step** towards Internet voting. Any new election technology initiative that connects the CEC to the public should be coordinated with these existing e-government initiatives and expand upon them. Conversely, any current or future e-government initiative should be developed in a manner that is electorally compatible. Therefore, initiatives such as the TAPAS[10] project

[10] TAPAS http://tapas.org.ua/

and EGAP [11] are mission-critical prerequisites for the possible introduction of new electoral technologies.

Finding 12

Building on existing initiatives (TAPAS, EGAP, eDemocracy, GoVote, amongst others) consultative, non-binding (politically**) experimental use of new voting technologies can be introduced within a two-year timeline**. **Thereafter, limited piloting** in small elections (perhaps in local government or municipal elections conducted as part of ongoing amalgamation) could be envisioned as a next step. Use of electronic or Internet voting for the 2024 presidential or *Verkhovna Rada* elections would be contingent on the findings of the various pilot exercises, on the level of success of parallel or prerequisite initiatives on infrastructure, digital identity and building the capacity and the prevailing cybersecurity and political climates, including the extent to which solutions piloted measurably improved trust, transparency, and addressed issues such as authentication and coercion. **A majority of interlocutors see 2024 as the earliest possible date for even a partial use of Internet voting in binding elections, with some looking at a five-to-ten-year timeline.**

[11] EGAP https://egap.in.ua/

International Experiences and Good Practice

Estonia

Background

Estonia began building its e-government in the mid-90s, not long after declaring independence from the Soviet Union. A small country of some 1.3 million people, Estonia has spearheaded the development of e-services starting with e-business and e-banking to popularize and foster acceptance of the idea of using services online. They have also worked to extend the e-service possibilities to health care, signing contracts, public transit, encrypting email and voting. To date, Estonia offers over 600 e-services to citizens and 2,400 to businesses.

Estonia's e-government success is testament to the work it did putting the building blocks in place in the late 1990s and early 2000s. These fundamental blocks include:

- Digitizing registers of all public bodies;
- Building the X-road platform connecting public and private sector systems;
- Drastically reducing the amount of paperwork required for any kind of administrative task;
- Providing citizens with a digital ID cards, that can be used to establish one's identity in an electronic environment.

The Estonian Internet voting system fundamentally builds on the Estonian ID card. Rather than an explicit Internet voting program, it is a natural by-product of a large program based on a long-term political decision to embrace e-governance as a model. The ID card is a mandatory national identity document for Estonian citizens. It is in the form of a smart card that stores data about the authorized user, including cryptographic keys and public key certificates that allow its owner to digitally sign official legally-binding documents.

Systems in Use

In Estonia, Internet voting is available during an early voting period (four-to-six days prior to Election Day). It is modelled on the way advance voting and postal voting is handled. Voters can change their electronic votes an unlimited number of times, with only the final vote being tabulated. This ensures some protection against coercion. It is also possible for anyone who voted using the Internet during the early voting period to go to a polling station during the early voting period, thereby invalidating their Internet vote. It is not possible to change or annul an electronic vote on Election Day.

Voters authenticate themselves on a website using the ID card or mobile ID (standard identification mechanism widely used in Estonia). The voter makes his or her choice and encrypts it with the server's public key. The "inner envelope" is anonymous and contains a single vote that can only be decrypted by the server, the "outer envelope" is signed with the voter's ID key before being sent to the voting server. The "outer envelope" is dropped during the count.

In 2014, Estonia established a mechanism for vote verifiability by which voters were able to individually verify the "cast as intended" and "recorded as cast" property of the vote via a mobile device (by reading a QR code from the screen of the desktop client, after which the smartphone verification application will display the name of the candidate the vote was cast for). There are no

direct means for the voter to verify that the vote was also tallied as cast. Thus, requirements for both individual and universal verifiability are only partially met.

It is worth noting that while Estonia uses Internet voting, it does not use any other sophisticated election technology: ballots are paper based, counting is done manually, candidate registration is not automated, and the paper poll books are manually marked off for each voter who comes to vote.

Current Status

Estonia became the first country to offer the possibility for citizens to vote by Internet in nationwide elections in 2005 and has conducted nine elections since. In the 2019 parliamentary elections, 247,232 people, or 43.8% of all participants, voted over the Internet, while the remainder of 56% voted by other means. For the first time, the Internet voting scheme was the most popular mechanism to vote through in 2019.

The Estonian ID card program and online voting system has not been without controversy. The discovery in 2017 of a critical vulnerability in the hardware underpinning the ID cards could have impacted the Estonian infrastructure well beyond the electoral process, allowing anyone who knows the *public key* of an ID card to compute the *private key* at a relatively low cost and use it to take full control of a person's identity without being in possession of the physical ID card. The government moved quickly to convene a press conference to inform the country of the risk and of the need for citizens to quickly renew their ID card certificates to reduce the risk of identity theft.

While multiple studies have been made to try to determine the impact of Internet voting on participation, there is, to date, no conclusive study that controls all variables (every election is different, with different political personalities, different socioeconomic contexts). Perhaps more importantly, Internet voting in Estonia as been determined to be habit forming: whomever voted online once will most likely vote online again.

Lessons for Ukraine

Estonia presents a singular showcase of how Internet voting works at the national level, although strict caution should be exercised when attempting to transpose this success to other countries and contexts.

The Internet voting experience in Estonia is the by-product of a complex and holistic e-governance program. It relies on an infrastructure and technology that has been tested and progressively deployed to non-political services for nearly 20 years.

As Internet voting has become more popular in Estonia, the cost of protecting the voting infrastructure against cyber-attacks is also substantially increasing. Hence the country might be the first to experience the fact that the cost of Internet voting is actually bell-shaped rather than linear; while the cost is high at the beginning of the deployment, and decreases progressively, it increases again as the stakes rise for election interference. Ukraine might face a different profile, with a continuously high cost due to its unique security concerns.

Moldova

Background

Concerning electronic voting as it pertains to population movement and transitory migration, Moldova offers an interesting case in examining the possibilities of introducing eVoting to a modestly-sized electorate. Data shows that immigration of non-citizens or foreign-born persons as well as irregular migrants to the EU using Moldova as a transit country are in very low number.

Figure 1 demonstrates the most common countries to which Moldovans travelled for short-term employment in 2015. According to various estimates, up to ¼ of the population were on permanent or temporary emigration, mainly in Russia, Italy, Spain, Portugal, Greece, France, UK, Germany, Turkey, Israel, USA, Canada and Belgium.

Legal Framework

In May 2008, the Parliament of Moldova approved Law No. 101 on the State Automated Informational System "Elections" (SAISE). The long-term objective of the SAISE was to achieve full automatization of elections in Moldova. This includes development of the possibility for citizens to vote in any polling station, possibility to vote through electronic voting machines (e.g. using an electronic pen, scanner or other electronic reading device) and/or possibility to vote via Internet (using identification devices that can read electronic documents).

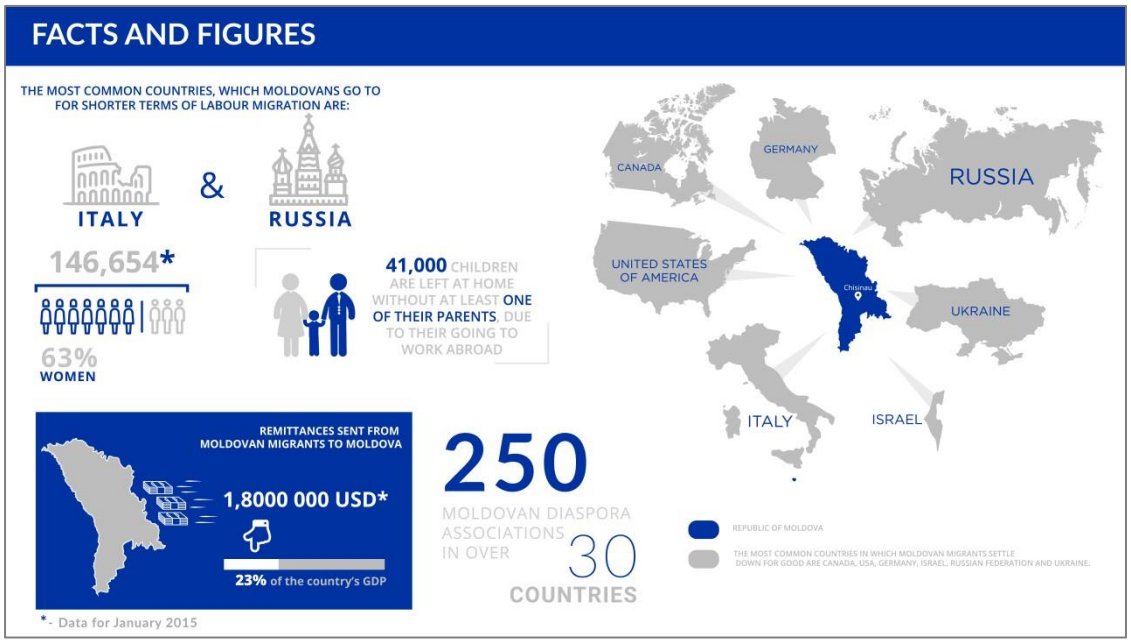


Figure 1 Moldova Demographics (source: https://www.iom.md/most-common-countries-which-moldovans-go-

According to Law No. 101, the electronic voting system was to be developed, tested and piloted by Moldovan authorities in time for the 2018 Parliamentary elections. In this regard, the CEC planned to develop an action plan and a roadmap for implementation of an eVoting system in Moldova, including a cost analysis. (See National Studies for implementation of Internet Voting system in Moldova).[12]

[12] http://www.undp.md/jobs/jobget_doc/3670

1) Feasibility Study on Internet Voting for the CEC of the Republic of Moldova

The aim of Internet voting it is to make elections in Moldova more democratic, and transparent. This ambitious project is still in the CEC's Strategic Plan 2016 -2019 and is included in the official plan of the CEC as "work to be implemented."

In 2016, the UNDP Moldova Democracy Programme/Elections agreed to support the CEC's Internet voting initiative by conducting a feasibility study on eVoting and its viability in Moldova. The main objective of this study was to assess the feasibility of developing and implementing a remote Internet Voting Informational System in Moldova for Moldovan voters residing abroad, as well as many voters who cannot come to the polling stations on election day and who would not benefit from other methods of electronic voting (e.g. electronic voting machines).[2]

According to the results of the F/S, in 2016 Moldova had the basic preconditions for introducing Internet Voting soon, such as: a well-developed Internet infrastructure, a high degree of mobile network coverage; good level of public ICT literacy and a reliable voters' list (SRV). Additionally, all polling stations are equipped with Internet – connected computers that are continually online and communicating with SAISE.

The authors of that study identified the following benefits for introducing new voting technology in Moldova: they believed that it will likely increase accessibility to vote among people with disabilities and limited mobility and increase participation among Moldovan citizens living abroad. Finally, the authors believed that it would reduce the "cost per voter" rate for voters living abroad and reduce the number of required polling places in highly populated areas.

However, amendments to the Electoral Code for introducing Internet Voting were required that would have included regulation of advance voting, remote voting and multiple voting (last vote counts) for the Internet Voting, and other relevant changes to the legislation. The Existing Data Protection legislation in 2016 was in place and the introduction of Internet Voting as an extension to the existing State Register of Voters (SRV) and SAISE system was legally possible. However, the piloting of the Internet Voting project might have required preliminary permission from the National Centre for Data Protection (NCDP).

The authors of that study (international consultant Jonas Edris and national consultant Iulian Groza) recommended that the Internet Voting Information System (IVIS) be created under the auspices of the CEC and owned and managed by it as a Module of the SAISE based on the SRV. They also recommended that a fully-functional IVIS be presented to the general public as well as experts and auditors to test before its actual use in legally binding political elections.

At the time of that study, the level of use of government e-services in Moldova was very low in comparison to other European countries, despite Moldova's high level of Internet penetration and mobile coverage. The introduction of Internet voting may have increased public trust in e-services. In the opinion of the experts involved in the study, the introduction of Internet voting in Moldova could have a positive impact on the country's image internationally as the second country in the world, and the first country outside the European Union, to introduce remote Internet voting on a national level.[13]

[13] https://promolex.md/wp-content/uploads/2018/10/studiul_Votul-prin-Internet_EN_.pdf

2) Survey on Moldova's Population's Perception of Information Technology Tools in the Perspective of Implementation of Internet Voting

As the follow up to the 2016 Feasibility Study, a "People's perception of the information technology tools in the perspective of implementation of Internet voting" survey was conducted under the "Democracy, Transparency and Accountability" Program funded by the United States Agency for International Development (USAID) in 2018 in Moldova. The overall objective of this study was to measure the use of information and communications technology tools by the citizens of Moldova and to assess their knowledge, attitudes, trust and opinions about Internet voting, building on the 2016 Feasibility Study. It presents a detailed analysis of international experience on the perception and trust in information technologies and Internet voting, of the specific situation in Moldova, and the potential of Moldovan voters using Internet voting.

The interviews conducted within the study reveal that the existing e-governance infrastructure in Moldova could facilitate the implementation of Internet voting or, at least, its testing through pilot projects.

In the same context, the study data shows that 100% of respondents of the online survey use social networks, 91% use e-commerce services, and 86% use Internet banking. In addition, 68% of respondents said that they use or know about electronic public services such as e-criminal record, e-declaration of income, etc. The author of the study, Ms. Livia Turcanu, pointed out that "the previous experience of interaction with various electronic processes, either online trade, payment with cards, use of electronic mail and social networks might positively influence people's decision to also use electronic voting, in addition to these tools." As for the decision of whether to use Internet voting or not, 86% of respondents said that they would use this voting option if it was introduced for future elections in Moldova.

On the other hand, the current social-political context of Moldova and the level of trust in public institutions do not favour the implementation of Internet voting. The study shows that only 11% of respondents fully agree, and 21% partially agree, that the level of people's trust in state institutions is sufficiently high for the implementation of an Internet voting system. The study also points out that even the testing of Internet voting would imply considerable cost and effort from stakeholders.

In conclusion, the author of the study says, "at the legislative level it is necessary to amend the legal framework to include both the regulation of the technical aspects of Internet voting and the procedures of the election process management, as well as other operations in the context of a voting mechanism that is based on information technologies as well". At the same time, people's trust in the public administration and the democratic processes are at the basis of Internet voting that is practiced successfully in countries such as Estonia and Switzerland. In this regard, the relevant institutions of the Moldova should work hard to increase people's trust in the democratic processes, thus ensuring a fair and transparent election system.

The study also makes a set of recommendations, including:

- Obtaining the trust and participation of the key stakeholders who are interested in the development of the Internet voting system;
- Providing access for the diaspora to the electronic signature tools;

- Ensuring a high level of transparency of the process; Gradually implementing pilot projects, etc.

These conclusions are meant to contribute to enhancing people's trust in information technologies with a view to implement Internet voting.[14]

Current Status

Piloting of an Internet voting system in Moldova ultimately did not happen due to a lack of funding for the technical implementation. According to Feasibility Study findings in 2016 and depending on the features, complexity, level of security, project management and logistics involved, the project could cost anywhere from EUR 400,000 to EUR 2,000,000 EUR. Political instability during the last two years and changes in the election law in 2018 have also prevented Moldova's authorities from following through on this project.

Lessons for Ukraine

A successful deployment requires a broad political acceptance of all major political parties. Additionally, any "eVoting systems or iVoting (remote voting)" implementation scheme should be included in the Electoral Code in Ukraine.

State financial support to the CEC is required to proceed with Internet Voting System development, its piloting and implementation in the country.

The national survey on the population's perception for implementation on new electoral technology provided useful insights and should be conducted to determine the non-technical feasibility of the project.

Switzerland

Elections in Switzerland

"*We do not vote once every four years – we vote four times every year*" – Swiss voter

Switzerland has a population of 8.48 million[15] and is a federation[16] consisting of 26 Cantons. These are further subdivided into 2,212 communes (or municipalities). The smallest communes have less than one hundred citizens, with the largest exceeding four hundred thousand. Cantons are highly autonomous (indeed, largely independent) republics, responsible for administering their own elections. The Swiss enjoy representative democracy at all levels and elect their local, cantonal and Federal government representatives. Citizens of Switzerland also enjoy high levels of direct democracy right down to the commune level. There are two main instruments of Swiss direct democracy, both put to the electorate only when sufficient signatures to a petition are received. Popular initiatives, if passed, amend the constitution, while Referenda allow a piece of legislation to be recalled. Further, financial matters above a certain threshold may also be put to a referendum at the commune or

[14] https://www.md.undp.org/content/moldova/en/home/library/effective_governance/feasibility-study-on-internet-voting-for-the-central-electoral-c.html

[15] https://www.bk.admin.ch/bk/en/home/dokumentation/the-swiss-confederation--a-brief-guide.html

[16] The .CH in the Swiss Internet domain and on vehicles registered in Switzerland is from "Confoederatio Helvetica" which is the Latin for "Helvetic Federation"). Swiss postage stamps also say "Helvetica"

cantonal level. Swiss voters get the opportunity to exercise these democratic rights on a regular basis – typically four times per year. Accordingly, Switzerland introduced postal voting (for cantonal elections in 1978 and national elections in 1994) and commenced piloting Internet voting as a means of facilitating citizen participation. Postal voting is used by a significant majority of Swiss voters.[17]

History of Internet Voting in Switzerland

Beginning with non-binding test pilots (for example in 2002, 16,000 students participated in a non-binding test of an early Internet voting system in Geneva), use of Internet voting was gradually introduced into binding referenda and initiatives, and later into political elections and direct democracy votes. At one point, three different systems were in use across multiple cantons. Low numbers (proportions) of resident and higher numbers of overseas Swiss voters were allowed to use these systems.

As the remainder of this section describes, the trend towards greater use and wider adoption of Internet voting ran parallel with increasing elaboration of security and verifiability requirements.

From an initial pilot to the current situation, almost two decades have passed. Switzerland has applied its considerable financial and human resources to deliver what it considers to be the state-of-the-art in electronic voting solutions – which recognize the challenges of competing requirements – in a fast-changing technical and political environment.

Legal Framework

From the OSCE report on the 2015 elections in Switzerland:

"*Federal legislation specifies the use of Internet voting in elections. The 1976 Federal Act on Political Rights (last amended in 2015) provides minimum standards for Internet voting pilots, which is regulated in more detail in Article 27 of the 1978 Federal Council Decree on Political Rights (last amended in 2013) and the new 2013 Federal Chancellery Decree on Electronic Voting. Relevant provisions are also found in the 1992 Federal Data Protection Act (last amended in 2014)*"

Elections, and Internet voting, in Switzerland are governed by the Constitution, by Federal law, and by cantonal regulations. Not all cantons offer iVoting, while some offer it only to overseas Swiss citizens. The Federal law places caps on the proportion of votes that may be cast using Internet voting. The higher the proportion of votes cast using electronic voting systems, the stricter and more comprehensive are the technical and procedural requirements.

Since late 2013, the legal ordinance has been updated with enhanced security and verifiability requirements[18] and, for a system to be available to more than 50% of voters (that is, no limit is placed, or 100% is permitted), must include:

- End-to-end encryption
- Individual verifiability (cast-as-intended, recorded-as-cast)
- Universal verifiability

[17] https://eprint.iacr.org/2017/325.pdf "CHVote System Specification" version 2.3, Haenni, et al, May 2019, Bern University of Applied Sciences, page 13.
[18] https://www.admin.ch/opc/en/classified-compilation/20132343/index.html

- Distribution of trust (shared decryption key, mix-net)

Both Geneva and the Swiss Post set about meeting these requirements, in order to allow for maximum usage by voters.

Since 2018, the legal ordinance has further required publication of source code,[19] which development led to the Source Code Review and Public Intrusion Test described hereunder.

Public Intrusion Test / Source Code Review 2019

In early 2019, the Swiss Post/Scytl Internet voting system was the subject of two distinct, but related, technical exercises, the Public Intrusion Test (PIT) and the Source Code Review.

A Public Intrusion Test (PIT) (described as a resilience test) saw the system challenged by "hackers and other independent IT experts". Participants were asked to register and be given credentials necessary to use the system in a simulated federal election. Any issues discovered by participants could be submitted through an online portal. The PIT offered financial rewards depending on the scope and nature of any problems identified. Full details are available at the referenced website.

Category	Approximate Compensation UAH
Best Practice (non-critical optimization possibilities)	2,400
Intrusion into the eVoting system	24,000
Corrupting votes or rendering them unusable	120,000
Successful attack on voting secrecy on the servers	240,000
Manipulation of votes detected by the system	480,000
Undetected manipulation of votes	720,000-1,200,000

Table 1. Swiss Post Public Intrusion Test Compensation Levels

In parallel with the PIT, Swiss Post published the source code of its Internet voting system, as required by law. The precise terms and conditions were the subject of some controversy in the field, with Swiss Post requiring registration, a commitment to responsible disclosure:

"Source code disclosure is a mandatory precondition of the Federal Chancellery for the use of advanced electronic voting systems. The aim of publishing the source code is to establish and build confidence among the general public, while obtaining feedback from professional experts and the opportunity to make improvements."[20]

A number of submissions were received, of which three were considered critical. Table 2 summarizes:

[19] Ibid, Article 7a

[20] https://www.post.ch/en/business-solutions/e-voting/publications-and-source-code/e-voting-source-code?shortcut=evoting-sourcecode

Public Intrusion Test		Source Code Review	
No of Participants	3200, from 137 countries	Submissions Received	84
Findings Submitted	173	Accepted for revision	28
Of which Confirmed[21]	16	of which Optimizations	25
Critical Findings	0	of which Critical	3
Non-critical optimization proposals	16		

Table 2 Numbers on Swiss Post Internet Voting System Public Intrusion Test and Source Code Review

None of the critical vulnerabilities identified in the Source Code Review were exploited as part of the Public Intrusion Test, despite the significant financial incentive. Nevertheless, the critical issues discovered by researchers[22] who reviewed the source code were sufficient to trigger the suspension of the use of the Swiss Post Internet voting system for the May 2019 elections. Upon the discovery of critical flaws in the source code, Swiss Post announced that their suppliers would make corrections and have the new code reviewed by independent experts. This process would take some time, so the system was not provided to Cantons for use in the May 19 vote.

The Federal Chancellery announced a review of licensing and certification procedures, taking into account the results and findings of the Public Intrusion Test and source code review. Despite software fixes being available rapidly after the vulnerabilities were discovered, the Swiss Post system was still not used for the October 2019 Federal elections.

Separately from the Swiss Post PIT and source code review, the other main system in use, that of canton Geneva, was also seeing changes. Citing the high cost of developing and supporting a sophisticated voting system (meeting the enhanced security and verifiability requirements), the government of the Canton of Geneva decided in November 2018 to stop further development of its system.[23] Geneva offered to continue using its system until 2020. However, in response to the Federal review of electronic voting, Geneva decided to stop the use of its systems in 2019. Accordingly, in both May 2019 (referenda/initiatives) and October 2019 (political elections), for the first time in sixteen years, no Internet voting systems were used in Switzerland.

[21] See https://www.onlinevote-pit.ch/stats/ for details and descriptions of submissions
[22] See https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/berichte-und-studien.html
[23] https://www.ge.ch/actualite/geneve-met-terme-au-developpement-sa-plateforme-vote-electronique-chvote-28-11-2018 In French.

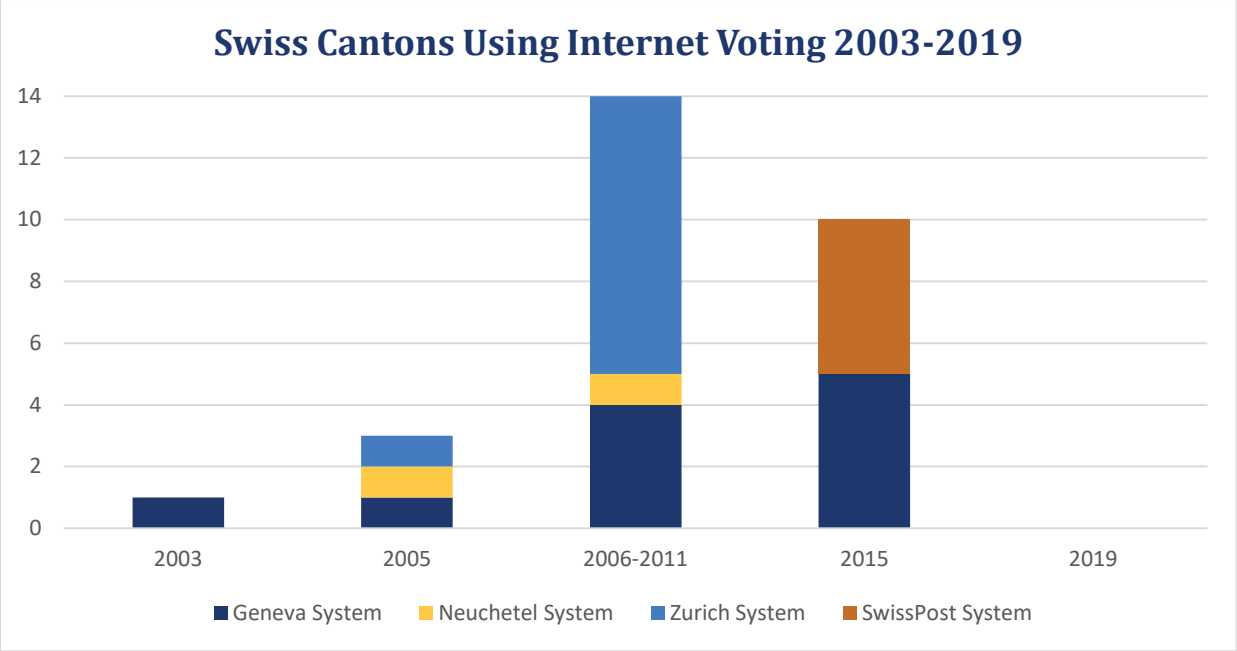


Figure 2 Number of Cantons using Internet Voting 2003-2019

Current Status and Future Prospects for Internet Voting in Switzerland

Currently, no Internet voting system is certified for use in Switzerland. A number of Cantons have declared their intention to resume Internet voting as soon as their chosen system has been certified. In parallel, the Swiss Federal Government is reviewing systems and certification and authorization procedures and has commissioned several reports by experts, both Swiss and international.

Separately, a direct democracy initiative has been launched, seeking to amend the Swiss constitution to place a moratorium on electronic voting until various criteria are met.[24] If enough signatures are gathered, this initiative will be put to the Swiss voters and would, if passed, have a significant impact on the future of electronic voting in Switzerland.

Otherwise, under current law and regulation, any system that is certified can be used to conduct Internet voting. It is likely, though not certain, that Switzerland will see a resumption of Internet voting in the medium term.

Lessons for Ukraine

Pre-existing remote voting (postal voting) was widely used and trusted prior to the piloting of Internet voting.[25] The Swiss Internet voting system relies on paper credentials delivered to voters by Swiss Post. There was gradual introduction of the new technology. Individual verifiability adds complexity. Public Intrusion Tests and Source Code Reviews contribute to more secure and resilient systems. Multiple interruptions and suspension of Internet voting system use require careful contingency planning. Political opposition to Internet voting may not be immediate. Successive recommendations from OSCE

[24] In German only, https://www.bk.admin.ch/ch/d/pore/vi/vis493.html
[25] https://eprint.iacr.org/2017/325.pdf page 2.

observer and expert missions to Switzerland offer valuable insights into developing good practice and international obligations.

International Obligations and Good Practices

Good practices with regards to international obligations

New technology and eVoting, in terms of how they are chosen and implemented, should respect high level provisions of the corresponding laws. Constitutional principles of universal, equal, free, secret and direct suffrage, election-related fundamental rights and procedural guarantees are guidelines and founding principles that should be embodied by new technology and not go against it.

The inclusion of technical details of implementation of technology should go into administrative regulations, rather than in the law. There is a legitimate concern shared among different countries implementing eVoting whereby detailed technical measures in the (higher-level) law could be problematic in the light of the rapid development of technical standards. Switzerland and Estonia, for example, have adopted multiple layers of legislation, with the more technical details being regulated by the lower levels. The stability of the law is a key property for the CEC to be able to plan ahead the introduction of new technology to improve the electoral process.

There are a number of international references that can be reviewed when contemplating changes to the legal framework. IFES' report on Norwegian Internet voting provided a framework for verifying compliance of Internet voting with international standards. [26] The 2017 Council of Europe Recommendation is perhaps the most important set of standards to date, with more than 49 points (grouped by *Universal Suffrage, Equal Suffrage, Free Suffrage, Secret Suffrage, Regulatory and Organizational Requirements, Transparency and Observation, Accountability and Reliability and Security of the System*).[27] There is also an emerging body of other electronic voting standards, [28] particularly with regards to electoral[29] observation,[30] but also applicable as guidelines[31] for EMBs.

The implication of non-state actors (software development company, hardware, cybersecurity service providers, etc.) becomes inevitable when dealing with high technology solutions. The CEC and other relevant government bodies [32] should determine a clear framework with regards to the responsibilities, criteria and procedures for ascertaining the competence and independence of

[26] The "Electronic Voting – challenges and opportunities" report from the Norwegian Ministry of Local Government: https://www.regjeringen.no/globalassets/upload/krd/prosjekter/e-valg/evaluering/topic7_assessment.pdf

[27] Council of Europe's Recommendation on Standards for E-Voting, 2018: https://www.coe.int/en/web/electoral-assistance/-/council-of-europe-adopts-new-recommendation-on-standards-for-e-voting

[28] IFES and NDI guide for "Implementing and Overseeing Electronic Voting and Counting Technologies", 2013: https://www.ndi.org/sites/default/files/Implementing_and_Overseeing_Electronic_Voting_and_Counting_Technologies.pdf

[29] The Carter Center Handbook on Observing Electronic Voting https://www.cartercenter.org/resources/pdfs/peace/democracy/des/Carter-Center-E_voting-Handbook.pdf

[30] ODIHR's Handbook For the Observation of New Voting Technologies, 2013: https://www.osce.org/odihr/elections/104939?download=true

[31] For example, https://www.idea.int/publications/catalogue/cybersecurity-in-elections?lang=en

[32] https://www.zora.uzh.ch/id/eprint/133915/1/2016_ElectoralExpert_Legality-Separation-of-powers-Stability-of-electoral-law-and-ICT_ADrizaMaurer.pdf

certification bodies. The CEC should take appropriate steps to avoid circumstances where the election is dependent on a few major vendors.

Ukrainian stakeholders should consider regulating the timing of the introduction of new technology. It is widely recognized that new technology is disruptive, and with elections it is not possible to have a do-over should a technology fail to perform. Any decision to adopt a new technology, whether it is a strategic decision or a change of vendor, should be planned in advance, with sufficient time for determining the feasibility, piloting and progressively deployment, with the exception of *force-majeure*.

According to the Council of Europe's Venice Commission, the fundamental elements of electoral law should not be open to amendment less than one year before an election. This principle has been interpreted by the Venice Commission, among others, as meaning that any reform of electoral legislation to be applied during an election should occur early enough for it to be really applicable to the election.

In the eVoting area, practical experiences and research suggest that, when envisaging introduction of eVoting, one should think of the impact not the next election, but rather the one after that. However, while some degree of stability is necessary at the high level, the electoral law must be capable of adapting to changing circumstances, a new threat environment, new technology and all other elements that might impact the integrity of the electoral process.[33]

Specific Internet voting concerns

Internet voting raises a number of important legal issues. In most cases, Internet voting cannot be adopted by an election management body without amending existing laws and regulations.

The following legal points can be raised:

- **Coercion resistance**[34] is an international principle enshrined in Art. 7.7 of the 1990 OSCE Copenhagen document[35]. Internet voting creates a new paradigm and raises the question of conflicting requirements when it comes to vote verifiability and coercion resistance.
- The **secrecy of the vote**. One of the most controversial issues touches on whether voting in uncontrolled environments is consistent with the principle of secret suffrage, and how the secrecy of the vote can be ensured when a vote is cast from home on a personal computer;[36]
- **Electronic population registries**. Legal considerations should be made regarding the use of an electronic population registry, and the implications of this for an Internet voting system;
- **Audits, recounts and administration.** Consideration should be given to the legal framework governing the audit and administration of the election and the competence of election administrators, including certification of the systems, audits and recounts, a voter verifiable audit trail, and more;

[33] Ibid.
[34] Coercion is the practice of persuading someone to vote in a specific way by using force or threat. More information is provided on the legal aspects of Coercion in section 5.3 End-to-end verifiable systems
[35] https://www.osce.org/odihr/elections/14304 page 6. "voters should be casting their vote free of fear of retribution"
[36]This discussion also pertains to postal voting.

- **Local, regional and national responsibilities.** Consideration should be given to the responsibilities related to Internet voting from a local, regional and national perspective; and,
- The impact of Internet voting on invalid and blank/protest votes.

Eventually, introducing any kind of eVoting requires substantial changes to the national legal framework governing elections. However, initial pilot projects may warrant special provisions pertaining to these experimental projects before an overall revision of the legal framework is implemented, if such voting is to be introduced nationwide.

Lessons from Germany

The German Constitutional Court[37] deemed that any kind of electronic voting is unconstitutional for a number of reasons: voters have to place blind faith in technology and have no way of actually knowing how the computers are counting their ballots, and any electronic or new system has to be as understandable and usable to the lay person as the system it is replacing (pen and paper for a physical ballot). This essentially makes any new electronic voting system impossible to implement in Germany with current levels of technology.

It is, however, interesting to note that Estonia and Switzerland both appear to implicitly accept that the comprehension of central steps of the election and its reliability/verifiability cannot always be understood by the layperson, but only by (democratically-appointed) specialists.

Proposed New Election Technologies

Electronic Voting/Internet voting

Terminology

The terminology used to describe voting and counting technologies is not authoritatively defined; similar phrases, like “eVoting,” are used inconsistently by different organizations and experts. The broader and clearer use of the term defines electronic voting as the use of electronic means to mark a ballot paper. Internet voting is a form of electronic voting and involves casting a ballot through the Internet.

While often presented as a natural evolution, transitioning from manually-marked and counted paper ballots to electronic vote recording and tabulating machines, to finally a fully online Internet voting system, it can be said that that there is nothing natural about this. While some pieces of technology may be adopted by one society, it may not be acceptable in another for various socioeconomic, political or security factors.

37 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html

Overview of the technology

There are different types of electronic voting systems which have evolved from mechanical voting machines of the early 20th century. The following are the main systems that are the most commonly used:

- A **Direct Recording Electronic voting system** (DRE) is where a voter marks his vote directly into an electronic device, using a touch screen, push buttons or a similar device. The vote is stored electronically in a removable memory component of the machine. While most DRE systems do not use paper ballots, recent concerns over the reliability and security of the machines have pushed the development of a method of providing feedback to voters. Voter Verified Paper Audit Trail (VVPAT) allows voters to verify that their vote was cast correctly, to detect possible election fraud or malfunction, and to provide a means to audit the stored electronic results. Some DREs are directly connected to a public network, and vote data is transmitted automatically to a central server.
- **A ballot marking device** is used by voters to record votes on a physical ballot, usually in the form of a small receipt with or without a barcode. **A ballot scanning device** will be used to scan the receipt before putting it in a standard ballot box. Manually filled ballots can also be scanned at the end of polling to speed up the counting process.
- **Internet voting** involves logging on to a website through a computer or a mobile application with access to the Internet. The general trend in most countries which have adopted or piloted Internet voting is not to make it compulsory and allow paper balloting as an alternative to Internet voting. Internet voting was first used for binding political elections in 2000 in the United States in a pilot across several states targeting overseas voters. Since then, approximately a dozen countries have experimented with this technology.

Introducing Internet voting is probably the most difficult upgrade, as it touches the core of the entire electoral process—the casting and counting of the votes. Internet voting greatly reduces direct human control and influence in the electoral process. It provides an opportunity for solving some old electoral problems, but also introduces a wide range of new risks and concerns from the perspective of trust and transparency. As a consequence, Internet voting usually triggers more criticism and opposition and is more disputed than any other information technology applications in elections.

Thematic Benefits and challenges

Cost

The argument of the cost effectiveness of electronic voting is not definitive. While the initial cost of the machine and the cost savings from reducing the number of staff required to count votes manually can be calculated, these are often others costs that are under-evaluated by most EMBs. Machines need to be regularly maintained against natural wear, and firmware and software need to be updated with security patches regularly, sometimes with the support of qualified technicians. Unpredictable costs can occur when the EMB falls prey to vendor lock whereby they become unable to use another vendor

and are at the mercy of arbitrary cost required by the vendor to maintain usable systems.[38] The cost of storing voting machines is also often forgotten and can be substantial for large countries.[39]

For Ukraine, the infrastructure of the PECs would need to be thoroughly audited. While most urban centres can fulfill the necessary requirements when it comes to power and connectivity, it would not be the case for many rural and remote areas. Improving these facilities to allow electronic voting machines would represent an important investment.

With regards to Internet voting, the idea of digitizing electoral operations is attractive due to the enormous logistical cost and the use of infrastructure. However, any calculation of the cost will need to consider multiple factors such as the cost of developing or acquiring the voting software, the electronic identity infrastructure used by voters, and the increased cybersecurity needs to protect online aspects of the electoral process.

Ukraine has major plans to develop e-services for its citizens. The government, with support from the international community, is currently making a substantial investment towards developing a global strategy to digitize Ukrainian society. While still in the early stages, this investment could represent the building blocks and be a first step towards piloting Internet voting. It would also require some kind of connection between the existing State Registry of Voters and the new digital identity infrastructure.

Attention should also be paid to infrastructure, both in terms of levels of publicly-available Internet as well as personal infrastructure, i.e. whether or not people have mobile phones with sufficient data plans, whether they have computers with connection to sufficient bandwidth, etc.

Recent studies from Estonia show that the cost per internet voter is not linear.[40] Early investments required to establish the fundamental pieces of infrastructure for Internet voting are costly and should be part of a broad initiative for e-government services. Once this infrastructure is in place, the cost of the Internet tends to decrease. However, with more voters adopting this voting scheme, the cost of securing it from cyber-attacks increases. This is an important finding for Ukraine, as it has been considered by all experts as a sort of 'ground zero' for weapons testing in this cybersecurity in general, and cybersecurity and elections in particular.[41, 42]

Voter accessibility

The right to vote independently and in secret for elected representatives is a cornerstone of democracy, enshrined in numerous international commitments including the 1990 OSCE Copenhagen Document and the United Nations Convention on the Rights of Persons with Disabilities (CRPD). However, for home-bound voters, and for voters with disabilities whose polling stations and polling materials are not accessible, this right is largely not respected.

---

[38] http://aceproject.org/ace-en/topics/vc/vc32/mobile_browsing/onePag

[39] https://www.irishtimes.com/news/cost-of-storing-voting-machines-696-000-a-year-vice-chairman-of-d%C3%A1il-committee-suggests-machines-should-be-scrapped-1.1288949

[40] How increasing use of Internet voting impacts the Estonian election management, Iuliia Krivonosova, Radu Antonio Serrano Iova, David Duenas-Cid, and Robert Krimmer. Tallinn University of Technology.

[41] Cybersecurity and Electoral Integrity: The Case of Ukraine, 2014-present, Beata Martin-Rozumilowicz and Thomas Chanussot, Fourth International Joint Conference on Electronic Voting E-Vote-ID 2019

[42] https://www.cepa.org/cyber-resilience-in-ukraine

Electronic voting machines can provide improved accessibility for disabled voters (including the visually impaired) by using a tactile ballot, which is a ballot system using physical markers to indicate where a mark should be made as a form of voting via a secret paper ballot.

Internet voting has also clear benefits for those who have mobility difficulties or those who cannot express their will without external help, by allowing them to vote on their own, with equipment that is often adapted to their special needs. New South Wales in Australia has made Internet voting available for blind and low-vision persons since 2007.

Efficiency

Electronic voting technology can present several advantages. It notably simplifies and speeds up the process of counting ballots. This is substantial, particularly in democracies with complex ballots that include multiple races and questions, although any type of ballot will be counted faster.

Electronic voting machines should also provide a more accurate tabulation of results. Manual counts very often involve manual errors on account of arithmetic errors or due to a low understanding of the protocols. A well-designed electronic voting machine or ballot scanning should reduce counting errors, as calculations are automatically done by a machine. It will also reduce the number of invalid votes by reducing the possibility for voters to spoil the ballot, recognizing that there is a valid discussion on whether such systems should allow voters to cast protest spoiled votes.

In the Ukrainian context, interlocutors met by the F/S team criticized the count at the PEC, which is formed by political appointees that change regularly. Deploying electronic voting machines would most likely be a massive challenge for the CEC in terms of training PEC staff on how to use and configure machines. Further, manipulation or other “unforced” errors by PEC staff could damage the trust in the accuracy and efficiency of the election process as a whole.

Internet voting can potentially make the voting process significantly quicker for voters who are able to use it, saving the time and perhaps physical challenges it takes to travel to and from the polling station, avoiding potential queues, and allowing voters to vote quickly from home. However, it is important to note that not all voters are necessarily comfortable with computers or technology; as such, particular care should be exercised to understanding the level of technological literacy in the different parts of Ukrainian society. While results and voting itself are much quicker via online voting, it is essential to consider what is sacrificed for this immediacy and convenience and what steps must then be taken to mitigate them.

Risk-limiting audits, as well as the ability to conduct any kind of recount, are strongly limited if not impossible when ballots are cast online. While modern eVoting machines can provide a paper audit trail, it is not the case for Internet voting. In a political and social environment that requires trust and transparency, this is probably the **single most important disadvantage of Internet voting**. A risk limiting, post-election audit requires manually checking a random, statistically-relevant sample of paper ballots to see if electronic voting machines and ballot scanners interpreted them correctly. The most common type of risk-limiting audit - *ballot comparison* - also requires independently counting all computer ballots, not just the sample, to check whether election computers added up the totals correctly. Post-election audits are paramount for elections with an electronic vote count and are part

of good practice worldwide. Their benefits have been promoted by political scientists, statisticians, and election security experts.

Security concerns

There are also major concerns over the use of any electronic voting or counting machines, as they involve complex software and hardware components. They are extremely difficult, if not impossible, to secure. Most electronic voting machine vendors have proprietary products that are not open to public scrutiny, and over the years, researchers have identified numerous vulnerabilities, as well as cases where machines were making unpredictable and inconsistent errors. Verifiable ballots are necessary because computers can and do malfunction, and because voting machines can be compromised. The recent progress made with the development of paper records (VVPAT) address these problems, but paper ballots need to be transparently audited to ensure trust in the count produced by the electronic voting machine.

Software can be hacked, and it is acknowledged by all experts that a fully secure electronic voting system is a myth. While mitigation strategies are possible, election stakeholders have to carefully consider the perception and its impact on trust that voting technology has on the public.

For Ukraine, the risks of piloting Internet voting would have to be carefully assessed, particularly in light of the security challenges Ukraine has faced during the last 10 years. Internet voting is distinct from other methods of voting in the sense that ballots become completely dematerialized, and it is not possible to produce a paper-based audit trail that voters can use to validate and verify that the machine correctly interpreted their choice. This introduces a substantial and unsolvable security risk. Given how much is at stake in an election, it is not unreasonable to assume that adversaries may specifically create and deploy malware designed to manipulate the vote.

Legal

Internet voting raises a number of important legal issues. In most cases, Internet voting cannot be adopted by an election management body without amending existing laws and regulations.

The coercion resistance and secrecy of the vote are the most controversial issues and touch on whether voting in uncontrolled environments is consistent with the principle of secret suffrage, but other points should also be raised, such as the legitimate use of electronic populations registries for Internet voting, the possibility to conduct audits and certifications, and the impact of Internet voting on blank and invalid votes[43].Eventually, introducing any kind of eVoting requires substantial changes to the national legal framework governing elections. However, initial pilot projects may warrant special provisions pertaining to these experimental projects before an overall revision of the legal framework is implemented, if such voting is to be introduced nationwide.

Education of the public

The introduction of technology is happening at an increasing pace in our societies. From the perspective of the young, urban populations, it seems that the whole country should be adopting modern voting technologies such as ones they are using for banking and communicating. At the same

[43] See 4.4.2 for more details on the legal implications of internet voting

time, young, technically literate citizens who better understand the risks can often be the most opposed to such elections technologies.

Aside from security concerns that make elections different from any other transaction, the need for education is probably the second most important argument in favor of pacing the speed of technology. Literacy in rural areas is an issue, and polling there takes time and suffers delays even with paper balloting. Educating rural voters to have them vote on a touch screen for example would represent a major challenge.

Good practice indicates that any effort taken towards the digitalization of the Ukrainian voting system should start with addressing education and awareness to promote online public service with no political impact. When trust has been established with voters, authorities could then begin to roll out new polling processes. There is still some mistrust from the population with regards to the CEC and other central government bodies, but especially with PECs, in Ukraine that could have a negative impact on the introduction of technology.

End-to-End Verifiable Systems

Technology introduces new concepts that will require time to be fully understood by most stakeholders.

End-to-end (E2E) verifiability is a requirement for any credible eVoting system. Without it, there is nearly no way to ensure trust in the process and to audit a ballot. E2E uses cryptographic functions to allow the voter to verify that the ballot was cast as intended (recorded) and tabulated (counted) as cast (individual verifiability). E2E also allows third parties to check the election results to confirm they are correct (universal verifiability). This makes the results auditable for correctness, potentially by all stakeholders (individuals or independent organizations, such as media outlets, political parties or nongovernmental organizations). It also involves, advanced technical and mathematical concepts for experts need to be trained in academia and at the government level. It is not easy for the public to absorb the concept of mathematical proof.

Like all Internet-facing systems, E2E does not protect against sophisticated malware that could have been specifically designed to spy on the voter's selections and compromise ballot secrecy. The system would also would not prevent or be able to detect fraudulent votes from being inserted into the vote tally.[44]

Coercion is the practice of persuading someone to vote in a specific way by using force or threats. While ballot casting secretly in a polling station, as it is largely the norm in all democracy, has been a good deterrent from voter coercion, the introduction of technology has forced researched to re-examine how the concept of coercion resistance has been redefined with electronic voting. An election mechanism that is coercion-resistant needs to be receipt-free, but also needs to prevent a voter from being forced to abstain from voting, to cast a random vote or to give away secret keys she possesses, to allow a coercer voting on her behalf.

[44] In fact, various academic studies have shown how this can happen. See, especially, recent work by Vanessa Teague from University of Melbourne, at https://people.eng.unimelb.edu.au/vjteague/

Coercion resistance is still a subject of intense study and debate to this day, and no perfect solution resolves voter coercion while fulfilling all other requirements of Internet voting such as secrecy of votes, end-to-end verifiability and security.

Voter turnout

Turnout in electoral events is decreasing worldwide. Many governments are seeking ways to improve traditional voting systems to counter what they perceive as a threat posed by declining democratic participation. Internet voting may seem like a reasonable answer to these concerns, particularly considering the potential ease of access and time-saving factors for some voters. There are many studies that assume that providing different channels for voting to voters increases turnout. Unfortunately, these studies are usually highly partisan, considering only the benefit technology can bring, while mostly relying on hypotheses and opinion polls rather than evidence-based research. Often these studies make broad conclusions without looking at specific political or country context, the social implications, or other factors that determine voter turnout (e.g. a lack of belief in the system, satisfaction with the status quo, etc.).

It is hence very difficult to use the increase of voter turnout as an argument in favor or against Internet voting. What is certain, however, is that the impact of this new scheme is marginal with respect to Internet voting, although the trend observed from Estonia appears to indicate a small increase in turnout. More importantly, it has been determined to be habit forming: whomever voted online once, will most likely vote online again.

Electoral system processes must deliver results that reflect the will of the voters in an environment that establishes sufficient trust so that these results are accepted as valid. The perception of fraud can be just as damaging to the credibility of an election as actual fraud. The CEC and Ukrainian stakeholders must be vigilant in maintaining a transparent process that allows all stakeholders to trust that the casting of votes, counting process and the results themselves are legitimate despite domestic and foreign disinformation campaigns aimed at destabilizing the country and delegitimizing the electoral process.

Perception of the country as a leader in digital society

The government of Ukraine is taking steps towards increasing the e-services it offers to citizens from the new web portal developed by TAPAS and the E-Gov initiative. The introduction of new voting technology and in particular Internet voting is often considered as a measure to strengthen the country's IT image and to position it as a leader in the region. This can be seen as a counter narrative to both the cybersecurity threat the country has been facing during the last 10 years, as well as the bureaucratic and archaic government infrastructure. It aims to creates a positive image to promote the new government as modern and innovative.

Legitimate risk of cybersecurity

Over the past decade, there have been numerous high-profile cases of attacks on Internet portals as well as viruses that have shut down the websites of government agencies and major corporations. Given how much is at stake in an election, one can reasonably assume that malicious actors – particularly in countries with specific geopolitical adversaries - may specifically create and deploy attacks and/or malware designed to manipulate the vote.

A virus, not detected by an antivirus program on a voter's computer, could manipulate the victim's vote in favor of the specific attacker's party. It's also possible for attackers to build a fake voting client, which could trick users into thinking that they have voted, even though they never actually accessed the official system or cast their vote. If either of these attacks occurred on a large scale, they could undermine the validity of an election or whole election system.

Potential malicious activities could include: the prevention of voters from casting their ballot, altering a voter's choices, monitoring how a voter votes, using the voter's credentials to gain access and expanding that access to damage the voting system, changing election results, or harming the credibility of the election results. Credential stealing, phishing, and social engineering are other possible ways of attacking the election system, even though they might not affect a large number of voters.

Broad timeline

Establishing a timeline to the deployment of electronic voting machines is a difficult exercise. Emerging and fragile democracies have seen too many cases of rushed procurement, pushed by political agendas involving corrupt officials. Notwithstanding the technical challenges that the selection of the right type of equipment presents, a procurement of this size will require critical political consultations.

With regards to Internet voting specifically, successful deployments of this technology have shown that it needs to be built on a strong existing infrastructure, which citizens are familiar with and rely upon for other services (Estonia), rather than a new platform created specifically for Internet voting. Thus, Internet voting should be tied to the deployment of other e-services and a well-established identity infrastructure.

Ukraine should also determine whether it should outsource the development of the source code on which the Internet voting scheme will rest, or whether it should identify resources in-country. This would have an impact on the time required to finalize a product fit for the task.

Online Voter Registration

The CEC, in October 2019, published[45] its proposals on the new mechanisms for change-of-address transactions in the State Register of Voters. The significant technical innovations proposed relate to the electronic submission of digitally-signed applications. While this restricts online transactions to those who are in possession of the digital signature, it nevertheless represents a step forward and is therefore recommended. The full draft procedure is available online. It must be recognized that the proposals are all subject to legislative reform currently before the *Verkhovna Rada*.

OPORA's analysis[46] recognizes these new features:

- Voters can file an application for the change of voting location in either paper form or in electronic using digital signature;

[45] https://www.cvk.gov.ua/novini/dostupnishi-vibori-tsvk-proponuie-doluchitisya-do-sproshhennya-poryadku-timchasovoi-zmini-mistsya-golosuvannya.html

[46] https://www.oporaua.org/en/news/vybory/19502-opora-zaproponuvala-tsvk-shche-bilshe-sprostiti-zminu-mistsia-golosuvannia

- A request to change the voting location can happen either for the first or the second round of elections or for both;
- The application can be done by an authorized third person if a voter lacks mobility;
- Individuals residing or staying abroad now have a simplified application procedure, through the relevant foreign diplomatic agencies of Ukraine;
- Where a voter doesn't have an election address in the voter list, a temporary change of voting location is possible.

OPORA goes further makes further suggestions. It is assumed that OPORA submitted its suggestions to the CEC under the provided consultation mechanism.

The SRV and CEC have a new system ready to deploy that will permit online transactions for change-of-address requests as previously discussed. OPORA (on the referenced web page) and a number of other interlocutors raised concerns about possible abuses of the online/electronic submission mechanisms including, for example, where large numbers of transactions could be undertaken just prior to an election in a small constituency, with a view to influencing the outcome.

Most interlocutors (not just political party blocs) complained about poor access to and lack of information about voter lists. The proposed automation would facilitate rapid and easy data sharing with responsible stakeholders of at least meta-data (the number and location) of change-of-address transactions. This would allow political parties, candidates, citizen observers and media scrutiny of the voter list update process and contribute to increased confidence in the voter lists used on election day.

Globally, there is a full spectrum of approaches to sharing voter list data with electoral stakeholders. This ranges from zero sharing whatsoever (voters lists appear in the polling stations only on polling day) to complete sharing in database or similar machine-readable format with political parties and other stakeholders. The first approach leads to low or no trust in the lists, while the second opens up questions about data protection and potential for abuse. A middle ground, which offers responsible stakeholders' access to the lists for legitimate electoral purposes, while at the same time protecting voter privacy, might be the system used previously in Kenya. In this system, the lists provided are redacted in three simple ways:

- Only the last four digits of the Voter ID number are included;
- Instead of full date of birth, the voter's age is given;
- Instead of full address, just the street or village name is given.

Ukraine should debate how much-desired access to voter lists can be achieved, perhaps subject to fair non-disclosure agreements and possible sanctions for abuse. This debate should take place in the framework of existing and potential future legislation on data privacy in Ukraine, and should consider possible future international obligations under the EU's General Data Protection Regulation (GDPR) framework.

There are no technical feasibility obstacles with any of the proposed innovations. As with any movement towards online or electronic submission, all necessary cybersecurity precautions must be taken to protect against unauthorized access and denial of service.

Building on the improvements already proposed by the CEC, greater access to voter list data both by voters themselves and by responsible electoral stakeholders can be easily and inexpensively facilitated. IFES recommends an early working consultation between the CEC and stakeholders on this issue.

Results Management Systems

A results management system (RMS) contains all the elements related to the count, aggregation, analysis and publication of votes once they have been counted at the lowest level. In Ukraine, this would refer to all the activity and processes that take place from the completion of the results protocol at the PEC to the publication of the final result of any election by the CEC. RMS can be all-paper, all-electronic or, more typically, and in keeping with good practice, a hybrid of paper and electronic processes.

Over multiple electoral cycles in Ukraine, issues with the management of election results have been raised by a wide variety of stakeholders, including political parties, citizen and international observers and those providing technical assistance to CEC. In the IFES study, most interlocutors again stressed the need to improve RMS at the CEC. Technology has a role to play, certainly, but IFES's findings show that poor remuneration and training of PEC and DEC staff coupled with the "incessant"[47] and often deliberate last-minute replacement of PEC and DEC personnel are major factors. Any introduction of technology for RMS (including the results module that would be a component of any PEC-level electronic voting solution) would likely fail unless the human resource issues mentioned above are fully addressed.

Any field-deployable technology implemented for RMS should be piloted, and the decision to proceed following such pilot tests, should be informed by the findings of the pilot.

As seen in the Kenyan 2017 presidential election petition, a lack of legal or regulatory clarity on what constitutes official and non-official results is a huge risk with RMS. In early deployments, electronic RMS are typically non-binding – they are there to:

1. Provide the EMB with capacity to supervise and monitor the work done in the field;
2. Provide the EMB with the means to rapidly publish preliminary, partial or interim results to hungry media and stakeholders;
3. Inhibit malfeasance by poll workers and others in the RMS chain.

As confidence in the electronic systems grows, the law can be amended to make paper the "backup" and raise the status of electronic results to officially-binding. In very mature scenarios, paper can be dispensed with completely, though redundancy mechanisms are still required in all-electronic RMS.

The CEC has a stated commitment to enhanced transparency and accountability of results management. Previously, the CEC has proposed an RMS initiative involving the use of a computer at each PEC into which the data from the signed results protocol would be entered, along with scanned images of the same. The data and scans would be digitally signed by PEC official(s) and the data transmitted securely to central CEC servers. The system would allow for printing out copies of the

[47] OSCE Final Report on Presidential Election 2019 in Ukraine, page 4

protocol for sharing with accredited party/candidate agents and, presumably, citizen and international observers present at the PEC.

The use of dual-channel (paper and digital protocols) represents good practice. Harnessing existing Ukrainian ID and digital signature infrastructure is appropriate. Measurable improvements in elections results management are therefore achievable. Digital Signature technology is mature but has not achieved the penetration nationally that might be required to use the proposed system in over thirty-thousand polling stations. Risks (including authentication, security, connectivity) are known, and can be mitigated. But mitigation adds complexity which adds cost and raises the level of training required for proper operation and support. The CEC hasn't fully articulated how the independent verification of digitally-signed protocols will work, and full disclosure/publication of results coming via this channel is a key feature if political parties, media, citizen/international observers and individual voters are to play their part in the scrutiny of the process.

Given the potential and radical changes to the electoral systems in Ukraine, the precise nature of RMS going forward remains unclear. Certainly, any changes to the electoral system will have impacts on polling, counting and on the management of results. These impacts should be carefully considered by the *Verkhovna Rada* and CEC, with particular emphasis on the human resource requirements at the PEC and DEC levels. Any use of technology should then be subject to piloting as per good practice.

The sensitivity of the management of results means that key stakeholders must be brought into the loop early and often. Controversial or failed RMS in other countries have revealed in lessons learned exercises that stakeholder distrust is closely correlated with stakeholder ignorance.

Other Electoral Applications

New information communication technologies (ICTs) could help Ukrainian electoral system to improve /upgrade/simplify major electoral processes which as of current time requires certain human resources, a lot of financial input and of course timeframes for arrangement of all needed steps to accomplish set goals for successful conducting their presidential or parliamentary elections campaigns.

If we look at the current national elections cycle in Ukraine (Figure 3), we can see the only e-technology implemented so far is web-based platform at the State Register of Voters (SVR) web-site where Ukrainian voters can check if they are registered in SVR system for voting.

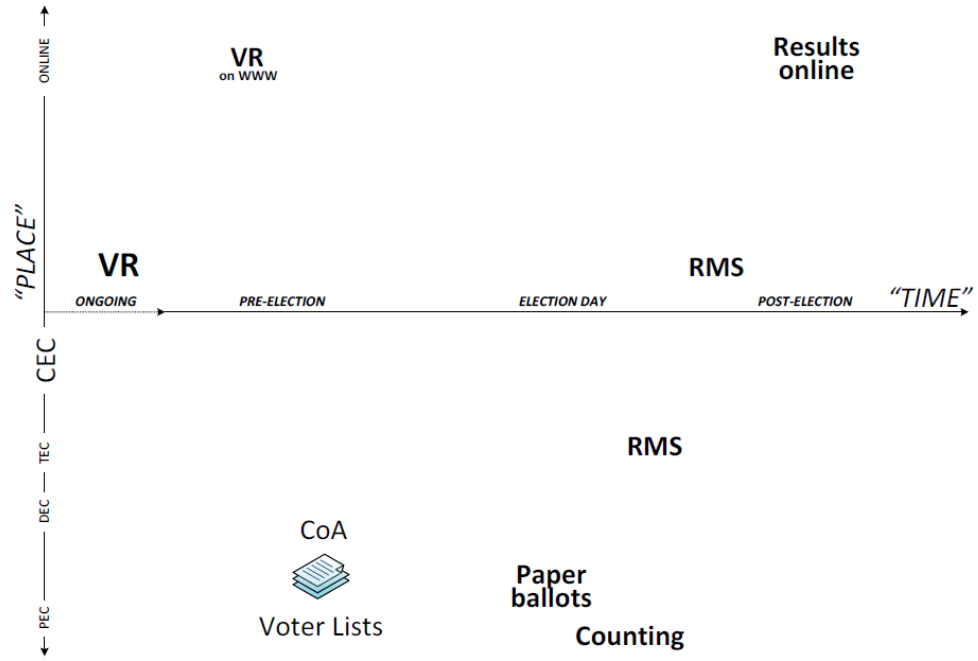


Figure 3 Time and Space - Election Cycle in Ukraine

Except implementing Internet voting technologies in the electoral area of Ukraine, the CEC needs to be empowered to consider piloting and implementing possible other elections technology for the electoral cycle in Ukraine.

In the brackets of Figure 4, below are indicated possible technology developments and their implementation into elections in Ukraine.

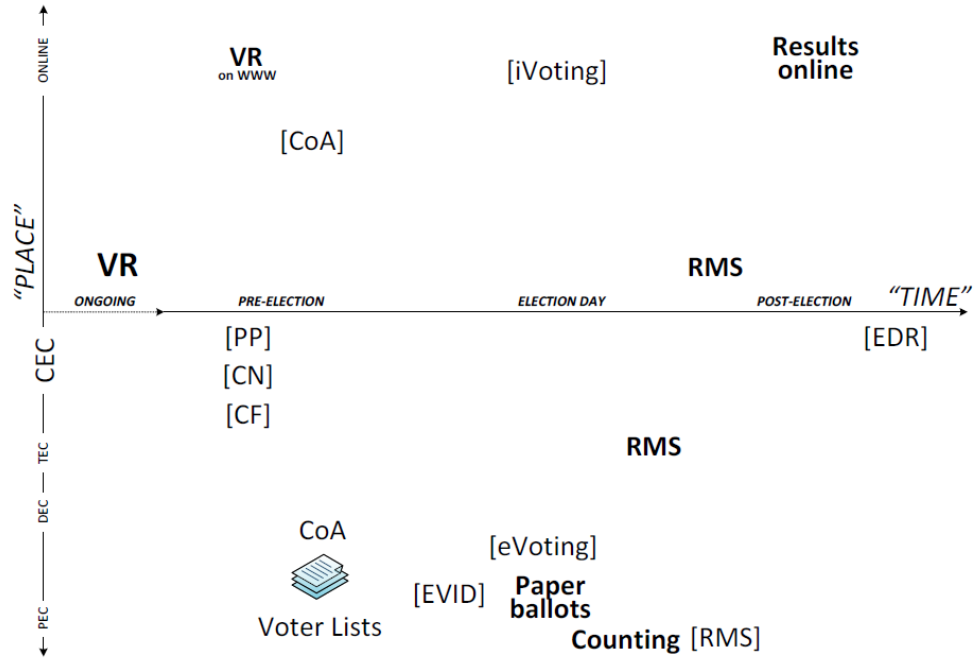


Figure 4 Other potential areas for technology in electoral processes [in square brackets]

Figure 4 Key:

CEC – Central Election Commission
TEC – Territorial Election Commission
DEC – District Election Commission
PEC – Precinct Election Commission
VR – Voter Registration
CoA – Change of (Voting] Address
PP – Political Party Registration
CN – Candidate Nomination
CF – Campaign Finance
eVID – Electronic Voter Identification Device
eVoting – Electronic Voting (at PEC)
iVoting – Internet Voting (remote/unsupervised)
RMS – Results Management System
EDR – Electoral Dispute Resolution

Interesting parts of new technology implementation that may be considered in the Ukrainian electoral process could be technical developments in political parties' registration, candidates' nominations, candidates financing and election dispute resolution system.

Some good examples that could be considered by Ukrainian counterparts is the development of software and online systems for political parties' management, as was done together with IFES for the Independent Electoral and Boundaries Commission (IEBS) in Kenya.

Political Party Registration

IFES assisted IEBS Kenya in the creation of a software solution that was given to political parties for data entry and the data from the exercise would then be forwarded to the IT personnel at the office of the registrar of political parties for verification, processing and importing. The process flow of political party registration via this new tool is illustrated below:

Process flow

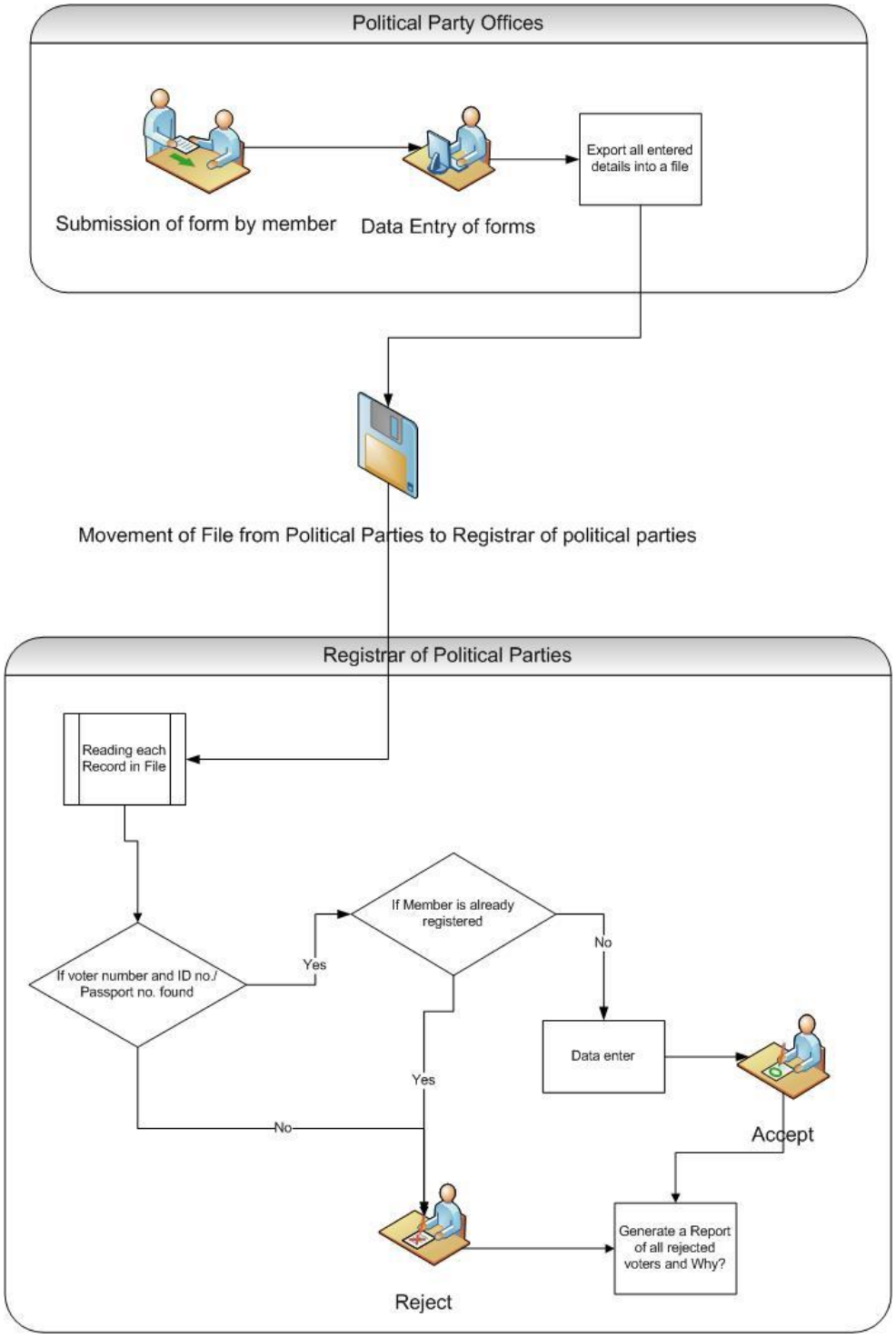


Figure 5 Example process flow, Kenya Candidate Nomination System (Source: IFES)

The algorithm to validate, process and import the data from each political party is illustrated in Figure 6:

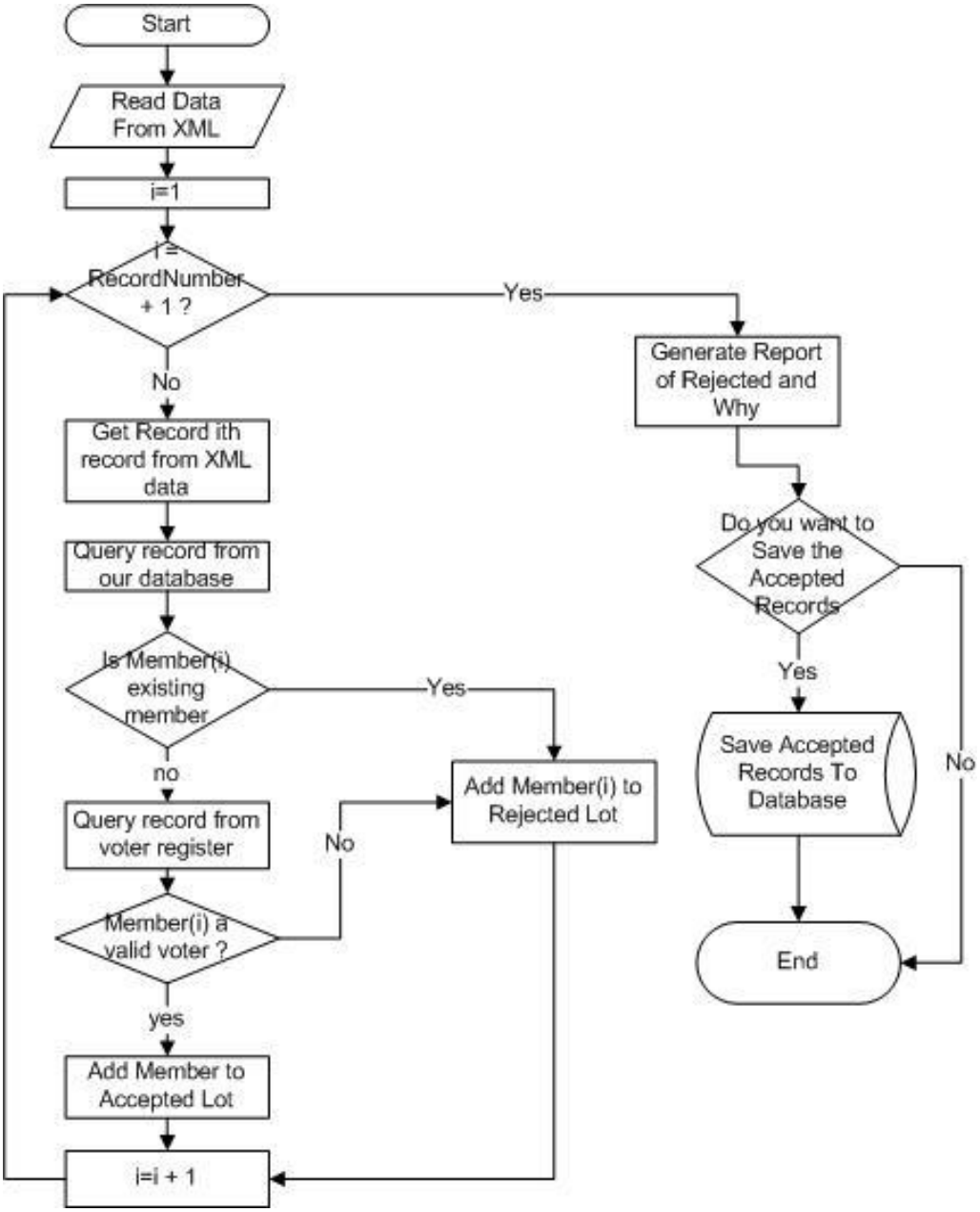


Figure 6 Political Party membership data import and validation process, Kenya (Source: IFES)

Candidates Nominations

In many countries, a candidate has to be nominated by a specified number of registered voters or by a specified office holder of a registered political party. An Electoral Management Body can verify that a candidate's nomination has met the relevant criteria by using technology to assist in analyzing the candidate's nomination.

In Kenya, for example, the Candidates Registration System (CRS) ensures that primary data on candidates nominated by political parties are entered in a format that makes it easy for IEBC to verify the accuracy of the candidate details, compliance and generate ballot paper proofs. This is achieved by cross-matching the voters register and political party register. Overall, the CRS strives to improve data exchange from political parties and independent candidates to IEBC returning officers enhance the efficiency of the nomination process through accurate data capture and processing of records by the returning officers improve accuracy of processing of the ballot papers how CRS works.

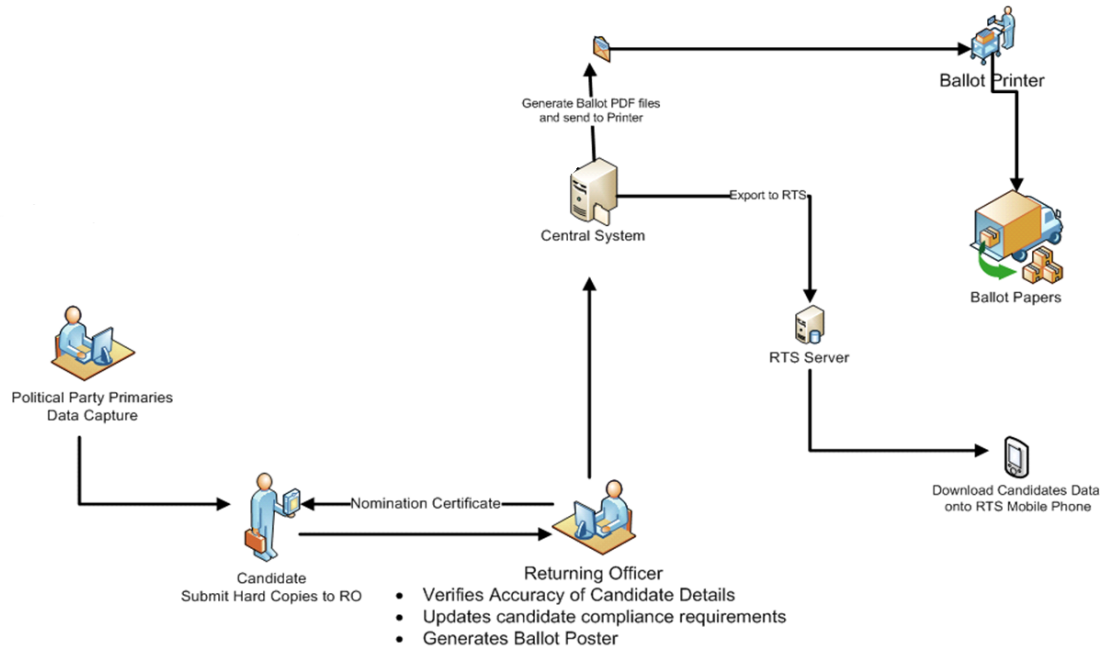


Figure 7 Source: https://www.iebc.or.ke/election/technology/?Candidates_Registration_System_(CRS)

Political Party Financing

Certain prototypes of the digital solutions can be used to facilitate the reporting requirements of a party and campaign financing scheme. Party and campaign financing reports may require detailed and complex data to be produced. Electronic data capture of report details can greatly assist an EMB in its regulatory and reporting requirements. Electronic submission of data by candidates and parties can also help them fulfil their requirements correctly and expeditiously.

In *Estonia*, a Supervisory Committee on Party Financing[48] requires that all political parties to report to report all their expenses of the accounting via web based X-Road system[49], which is part of national e-reporting system. This system is mandatory for use by political parties for election coalitions and independent candidates (except where reports can legitimately be filed by hand). Parties report income, expenditures and campaign funding quarterly.

[48] http://www.erjk.ee/en
[49] https://www.erjk.ee/is/

Political parties in *Brazil* are obliged to use a "Sistema de Prestação de Contas Eleitorais" software, which openly available for download by party from Tribunal Superior Electoral website[50]. This is the system used by candidates, political parties and financial committees during election campaigns. Party reports are published for the previous calendar year. Campaign finance data are searchable and can be filtered by candidate, municipality, party and donor.

More information on existing and used by political parties worldwide the web-based and software applications system you can see in the tables: A.1 and A.2 below, – these are samples, and both sourced from International IDEA.[51]

Table A.1. Web-based systems (sample – see website for full table[52])

Country/ oversight agency	Online reporting	Online disclosure
Australia (Australian Electoral Commission, AEC)	**Name: 'eReturns'** Use is voluntary Available to political parties, candidates, third parties, donors, associated entities and senate groups	Summary and detailed data available for parties, candidates, donors, associated entities and third parties Data available for both donations and expenditures, although only summary expenditures for political parties
Brazil (Tribunal Superior Electoral, TSE)	**Sistema de Prestação de Contas Anuais (SPCA)** Used by political parties to file annual financial reports	See entry on Brazil below under 'Software-based systems' for information on disclosure

[50] http://www.tse.jus.br/partidos/contas-partidarias/entrega-da-prestacao-de-contas/sistema-de-prestacao-de-contas-anuais-spca

[51] https://www.idea.int/sites/default/files/publications/digital-solutions-for-political-finance-reporting-and-disclosure-a-practical-guide.pdf

[52] ibid

Table A.2. Software-based systems (sample - see website for full table[53])

Country/ oversight agency	Online reporting	Online disclosure
Argentina (National Electoral Chamber)	**Name: Informe de Financiamiento de Partidos Politicos (INFIPP)** Use is mandatory Excel sheets can be imported into the system	Political party financial data published on website of the Justicia Nacional Electoral, but only available as PDFs published online by National Electoral Chamber in Excel online format
Canada (Elections Canada)	**Name: Electronic Financial Return (EFR)** Use is voluntary Software available in English and French	Both summary and itemized data is available for party, candidate, registered associations, nomination contestants and leadership contestant reports All electronic financial data are downloadable

Elections Dispute Resolution System

On March 1, 2019, the electronic court web-platform system was launched in Ukraine. The electronic court subsystem provides for the exchange of procedural documents (sending and receiving documents) in electronic form between the courts, bodies and institutions of the justice system, between the court and the participants of the trial, between the participants of the trial. With the help of the E-court service, litigants can file procedural documents (claims, motions, etc.) in electronic format. Upon successful submission, the litigant can track the motion and status of their case in court. Information on the delivery of the document, its registration and other information is sent to the Author's Electronic Cabinet in automatic mode.

The litigant can also pay the online fees, fees and other payments through the E-Court service, form and submit an electronic order to another person, and additionally receive:

- web-links to the texts of all the procedural documents in the case in which the participant takes part in the case: court decisions, subpoenas, calls, etc.;
- information on received and registered incoming case documents, together with documents in electronic format;
- information about received documents on the case from other participants together with documents in electronic format;

[53] Ibid

- electronic documents that have caused a change in the status of the case, automated distribution protocols, etc.

The litigation participant's e-mail also displays a calendar of litigation events.

It would be worthwhile for the CEC to consider the including for the above-mentioned web-based platform an additional option for a Elections Dispute Resolution System, similar to Kenya's Political Parties Disputes Tribunal (PPDT) cases management system. The PPDT is an institution in Kenya that aims to realize a democratic political system founded on issue-based politics that respect the rule of law and protect the rights and freedoms of every individual. The implementation of the case management system which was developed through assistance from IFES is one of the items in the tribunal's strategic plan. In addition to resolving disputes, the PPDT works closely with other stakeholders in the political process (registered political parties, the Independent Electoral & Boundaries Commission, the Registrar of Political Parties and the Political Parties Liaison Committee) to promote issue-based politics and people-centered democracy in Kenya.

The PDDT case management system consider the following nature of cases:

1) Complaint

- disputes between the members of a political party;
- disputes between a member of a political party and a political party;
- disputes between political parties;
- disputes between an independent candidate and a political party;
- disputes between coalition partners;
- disputes arising from party primaries.

or

2) Appeal from decision of the Political Party Registrar.[54]

[54] http://ppdt.judiciary.go.ke/case-procedures/

Risks and Mitigation

Legend: Risk – a narrative description of the Risk as assessed by the FS team. Likelihood – Low/Medium/High of the Risk manifesting, Impact – Low/Serious/Critical, plus narrative description of undesirable consequences of the Risk manifesting; Mitigation – a narrative description – [aligned with IFES recommendations] of actions to reduce the risk, or better deal with the consequences.

The following Risk Analysis is not aimed at the risks associated with any given technology, which analysis can accompany the recommended CEC-led research and development and outreach activities. Rather, this analysis focuses on the risks associated with, and therefore relevant, to the consideration of feasibility of the introduction of technology into electoral processes:

	Risk	Likelihood	Impact	Mitigation
1	Cybersecurity incidents compromise electoral integrity of election.	Medium	High	A risk assessment should be led by the CEC for each new technology deployed for the election, in collaboration with national cyber agencies.
2	The perception of the process being free from foreign or external cyber influence has a negative impact on the trust in the electoral process.	Medium	High	Engage in disinformation mitigation, progressive deployment of technology in non-binding election to establish a baseline.
3	CEC fails to ensure the trust of political parties in the new technology. Agents attempt to discredit the new system based on political interests.	Medium	High	Pilot, transparent procurement process, transparent review of the pilot lessons learned, potentially open the source code to external review.
4	Failure to deliver a working software solution for the CEC by the respective department or service provider	Low	High	Strategic planning, early procurement, effective project management, piloting for all systems.
5	Proposals for new innovative election technology is used as a political tool against the CEC as a proxy against the government. Credibility of the election put in jeopardy.	Medium	Medium	New technology introduction lead by CEC. Early, inclusive consultations and buy-in from all stakeholders.
6	CEC budget or timeline is not sufficient to ensure research and piloting before deployment of new technology, having the Commission cancel the deployment	High	Medium	Properly plan budget ahead of activity. Commitment to investigating new technology should be contingent to budget allocation.

	Risk	Likelihood	Impact	Mitigation
7	The CEC does not take appropriate action to amend the election code, and legal challenges are made to the use of technology.	Low	Medium	Special provisions should be made to ensure that piloting will be possible, and review and appropriate reforms are made before the full deployment.
8	Inadequate IT infrastructure (Internet coverage all over Ukraine and needed Elections software/hardware coverage) will undermine the implementation either eVoting or iVoting technologies	High	High	IT infrastructure/Internet coverage Nationwide assessment need to be done and appropriate technical steps to be done to solve issues with lack of technology on the uncovered areas of Ukraine.
9	If iVoting is introduced in Ukraine also for citizens who live and work abroad and in the annexed /occupied territories, there are big risks of uncontrolled voting and coercion from Russia side as well as from Belarus and countries who are members of the CIS customs union	Medium	High	Conduct iVoting system development, piloting and implementation in the areas controlled by Ukrainian authorities. Introduce iVoting for Ukrainians who live and work abroad (except in Russia, Belarus, CIS custom union countries) in the secure environment like Embassies premises with a circled cyber environment.
10	A poorly developed voter identification system for voter verification for eVoting or iVoting by CEC and responsible agencies	Medium	High	Consider involving number of national registers (State Voter of Register, State Demographic Register, State Migration Service Biometrical Register, Ministry of Interiors Register) to be used for voter identification to be able to implement e/ivoting systems.
11	Lack of acceptance by citizens of Ukraine of new already implemented technology in the electoral process	Medium	High	Population perception survey need to be done before new voting system implementation, develop strategic communication campaigns for population and clearly explain what is going to be implemented, why, and what benefits new system will bring to Ukrainian society, develop roadmap for citizens awareness campaigns

	Risk	Likelihood	Impact	Mitigation
12	Possible selling of e-votes by Ukrainian voters online because of financial reasons or just a desire to earn additional funds to the interested political stakeholders that will distrust all efforts on the implementation of I -Voting technology by CEC and State offices and already earlier successful implemented e-services platforms in Ukraine	High	High	Not to rush to implement new system before major public services are implemented into e-platform services, educate population on the usage of e-tools for their daily needs and implement iVoting when major part of citizens of Ukraine will be using e-services and have trust to State on implementing new technology in the country

Recommendations

In the following list of recommendations, the word “immediate” means “without delay.” Short-term means within two years, medium-term between two and four years and long-term meaning five to ten years hence.

Recommendation 1. [Immediate] An inclusive, wide-ranging consultative process with all Ukrainian electoral stakeholders should commence. This should be preceded by or include in-depth knowledge-sharing and informative workshops and seminars to raise stakeholders' understanding of the many issues surrounding electronic and Internet voting. The small number of highly knowledgeable Ukrainian stakeholders should be augmented by relevant international experts and practitioners.

Recommendation 2. [*Immediate*] The new CEC should focus its short-term efforts at addressing the long-recognised deficiencies in electoral processes, namely the management of results at all levels, the streamlining of voter list change of address transactions and the professionalization of staff in the field. Existing initiatives at CEC are the perfect starting point and should proceed, given a legal basis and adequate resources.

Recommendation 3. [*Short term and ongoing*] Recognising the cost and human resource implications for CEC of planned and future initiatives in electoral technology, the Government of Ukraine should make adequate and sustained budgetary increases to ensure the institution is capable of delivering.

Recommendation 4. [*Short term*] A comprehensive survey of citizens' knowledge of, and trust in e-Democracy and elections technology should be undertaken in order to baseline attitudes and inform policy decisions. First surveys should measure the potential impact on voter turnout, subsequent surveys should seek to determine the actual impact.

Recommendation 5. [*Short to medium term*] A significant nationally-owned research and development initiative, led by the CEC, and focussed on determining what models of electronic and Internet voting are appropriate for Ukraine, should commence as soon as possible. Fundamental questions to be researched and, hopefully, answered, include:

a. Electronic voting in supervised locations or remote/Internet voting or both?
b. How will voters be identified in eVoting or iVoting scenarios?
c. How will new technologies facilitate voting by internally displaced voters, by urban, rural, diaspora and other voters living in non-Government controlled areas?
d. What protections against coercion, intimidation and vote buying are possible and suitable for Ukraine?
e. How will any new electoral technologies be protected against cyber-attacks?
f. How will Ukrainians learn to use, and to trust new electoral technologies?

Recommendation 6. *[Short to medium term]* In parallel with or following (but not during) the activities proposed in 0, competent international vendors could be invited to attend a trade show, focussed on relevant electoral technologies and solutions.

Recommendation 7. [*Immediate to Short term*] The legal framework for Cybersecurity in Ukraine should be finalised so that the appropriate agencies with whom CEC must liaise to protect any new electoral technologies are established.

Recommendation 8. [*Immediate and Short medium term*] The CEC should be invited to engage with every proposed initiative under the Digital Transformation vision, in order to ensure that every innovation is electorally compatible.

Recommendation 9. [*Short to medium term*] Experimental use of new voting technologies should be undertaken no sooner than between 18 and 24 months. Piloting in small scale elections may follow and, contingent upon the findings of reviews, and prevailing conditions, a decision to offer limited electronic or Internet voting options for Presidential and *Verkhovna Rada* elections in 2024 can be taken.

Recommendation 10. [*Long Term*] A comprehensive review of all deployed systems should be undertaken in the post-2024 review and long-term policy on electoral technology set accordingly.

Timeframes/Indicative Roadmap

Indicative Roadmap and Timeline - Elections and Technology in Ukraine 2020-2030

Year	...2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Electoral Events												
Amalgamation			???									
Local Government												
Presidential												
Verkhovna Rada												
Referenda	???	???	???	???	???	???						
Digital Transformation												
ID initiatives												
eGovernance Initiatives												
CyberSecurity Initiatives												
Legal Framework				Review			Review			Review		
CyberHygeine Nationwide												
????												
????												
????												
CEC-led Initiatives												
VR CoA Pilots												
VR CoA Rollouts												
RMS @ PEC Pilots												
RMS @ PEC Rollout												
Enabling Legislation												
CEC-led Feasibility Study												
Stakeholder Consultations												
e-Vote Experiments												
i-Vote Experiments												
Milestone 1 - Decision												
e-Vote Pilots												
i-Vote Pilots												
Review												
Milestone 2 - Decision												
Legal Framework												
						????						

ANNEXES

Annex 1 – Terms of Reference for Feasibility Study

IFES August 2019

Context and Background

Following the presidential election in March/April 2019, and early parliamentary elections in July 2019, the newly elected government of Ukraine has expressed the wish to intensify the use of technology in elections by instituting Internet voting and online services for citizens to update their voter records. While this type of project would typically require a longer timeline, the government has stated their intention for this to happen as early as the next local elections expected to take place in October 2020. In this context, the government has requested IFES' support in creating a joint team responsible for assessing the feasibility of developing and deploying new elections technologies in Ukraine.

The "Feasibility Study on New Elections Technologies" (F/S) will look at potential new technologies available that could be used in Ukraine to potentially strengthen the electoral process. These may include: internet-based registration and voting, and improvement of the digital result transmission and results management systems. It will provide Ukrainian stakeholders with important background and risk/benefits analyses that should allow them to make more informed decision regarding possible next steps, cognizant of the international standards that they need to adhere to, particularly the UDHR, ICCPR, 1990 Copenhagen Document and the Venice Commission Code of Good Practice in Electoral Matters and the 2017 Council of Europe Recommendation CM/Rec (2017)5 on Standards for eVoting.

Scope of work

Methodology

The F/S team will review existing literature on elections technology from multiple sources, including international observers reports, media, academic publications, vendors white-papers and election management bodies (EMB) releases. It may consult with EMBs of countries where programs were implemented to identify good practices or lessons learned that could be applied in the Ukrainian context.

The F/S team will liaise with potential suppliers of systems to determine cost and the size of the pool of vendors that have the capacity to deliver technical solutions investigated as part of the F/S.

The F/S team will review existing legal and technical documentation and conduct interviews with relevant Ukrainian stakeholders in order to understand the maturity and current capacity of the technical infrastructure with regards to cybersecurity, data protection and voter identification.

The F/S should provide an opportunity to strengthen multi-stakeholder consultation and dialogue on the feasibility and perception of elections technology in Ukraine. Hence, the team will consult with government officials, Central Election Commission and other key government representatives, political parties, civil society and other relevant stakeholders to ensure an inclusive and wide-ranging process.

Outcome

The F/S report will explore the different possible options for implementing elections technologies. It will address the following points:

4. Based on the government's request and stated intentions, analyze the social demand for and the perception/trust of election technology based on available research and surveys in Ukraine. Seek to identify what problem is being solved by a given intervention and, on this basis, to establish any potential benefits for Ukrainian society.
5. Evaluate the technological maturity of Ukrainian infrastructure and institutional capacity to support new elections technologies in the long term, including internet penetration and availability of skilled technology, cybersecurity and cryptography experts.
6. Review the technical and legal challenges and opportunities for the modernization and of voter registration and voter identification mechanisms. Particularly to improve citizen's capacity to update their voter records online, but also to address risks of multiple voting and impersonation.
7. Review of the technical and legal challenges and opportunities for digital voting and possible improvement to the voting and results management system.
8. Look at the cost and opportunities of acquiring (via international vendors) vs developing in-house. Analysis of the procurement challenges, particularly in light of the compressed timeline and its implication with regards to cost, time to pilot, possible vendor dependence, procurement transparency, and stakeholder buy-in. Recommendations on potential mitigation strategies to these procurement issues.
9. Review of the possible models of governance, including their impact on cybersecurity and ownership in terms of operation, maintenance and incident response. Outline potential long-term cost implications of introducing new technology and risks associated with governance models specifically for the Ukrainian context.
10. Estimate the cost, human, and financial, of introducing new technologies factoring in medium- and long-terms costs together with any short-term gain.
11. Establish a risks matrix with potential mitigation strategies for the electoral process based on Ukraine's specific experience with regards to cybersecurity and elections.
12. Outline applicable recommendations from an international standards perspective in the context of Ukraine, to include cybersecurity considerations and legal compliance.
13. Recommendations with regards to awareness and trust building (access to observers, transparency, public information and awareness campaign, etc.).

Objectives and Expected Outputs

The F/S team will deliver the following documents as key outputs:

- A detailed feasibility study, based on updated information analyzed and incorporated;
- Short-, medium- and long-term strategy recommendations for implementing new elections technologies considering all factors: participation, cost, transparency, efficiency, security, verifiability, integrity, credibility, legitimacy, universality, secrecy, accountability, and trust;
- A high-level roadmap of recommended implementation schedules with an estimation of the budget requirements.

Deliverables will be submitted to the President of Ukraine's Advisor on State Digitalization office and IFES Ukraine Country Director.

Duration of the assignment

One-month desk review, prior to a one-month feasibility study.

Composition of the team

(Proposition, with the possibility to add 1 or 2 co-authors depending on their specialty, could include representative from Ukrainian institutions + CEC + IFES)

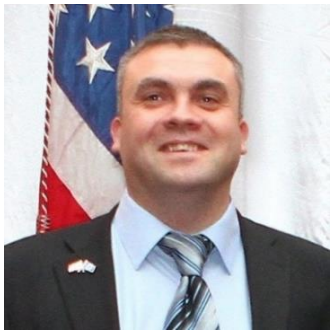
One team leader/coordinator (overall management, maintain priorities, serves as liaison between interviewers and interviewee).

Two or more co-authors/writers (conduct interviews, compile findings and edit report), specialties: election technology, legal and technology, (if available) cryptography and cybersecurity.

One support officer (assist in scheduling interviews, logistics).

Annex 2 – Biographies of Feasibility Study Team Members

***VLADLEN BASYSTY*, Technology and Cybersecurity Manager, International Foundation for Electoral Systems (IFES)**



Vladlen has 16 years' experience managing IT projects with organizations including the International Organization of Migration, US CGI, United States Embassy to Ukraine, Office of US Department of Homeland Security, Federal Law Enforcement Training Center (FLETC), John Snow Institute/United States Agency for International Development (USAID) Project, "AIDS Foundation East-West", US Peace Corps to Ukraine and others.

***THOMAS CHANUSSOT*, Senior Voter Registration and IT Advisor, International Foundation for Electoral Systems (IFES)**

Thomas has been working in the field of elections since 2004. An experienced project manager and software architect, Thomas graduated from French University Paris Dauphine in IT applied to management. He has a strong background in web technologies data analytics and cybersecurity. He has been involved in more than 12 electoral operations around the world, during which he has held diverse roles including system development, database analytics/fraud investigator, security audit and team management. He has worked extensively on mission critical electoral infrastructure designing and securing biometric and non-biometric voter list databases, as well as result management systems. He has worked in Europe, Central Asian and Asia/Pacific, Africa and the Middle-East, for diverse organizations such as IFES, UNDP, OSCE or the EU.

***RONAN McDERMOTT*, International Expert on Electoral Technologies, International Foundation for Electoral Systems (IFES)**

Ronan has worked extensively with elections management bodies in developing and post-conflict countries for almost twenty years, in Africa, the Americas, Asia, Europe and in the Pacific. He has participated in regional and global electoral support initiatives and has contributed to many publications and competence development efforts. In several countries, he developed and delivered voter registration, results management and poll-worker management systems. In others, he has provided advice to elections management bodies to enable them to specify, develop, procure, deploy and support a variety of technologies, including biometrics, in support of electoral processes, particularly voter registration and results management systems. He has been directly involved in the procurement of electoral technology and ancillary services whose value exceeds one hundred and fifty million dollars.

OLHA ANTONOVA, Cybersecurity Project Assistant, International Foundation for Electoral System (IFES)

Olha graduated from Taras Shevchenko National University of Kyiv in 2017 and participated in a number of volunteering activities in the field of Informational Technologies. She has been working in IFES since 2018, being involved in various activities related to cybersecurity and technology, providing support to the project.

Annex 3 – Overview of Electoral Cycle and Processes

The classic Electoral Cycle Diagram is shown in Figure 8

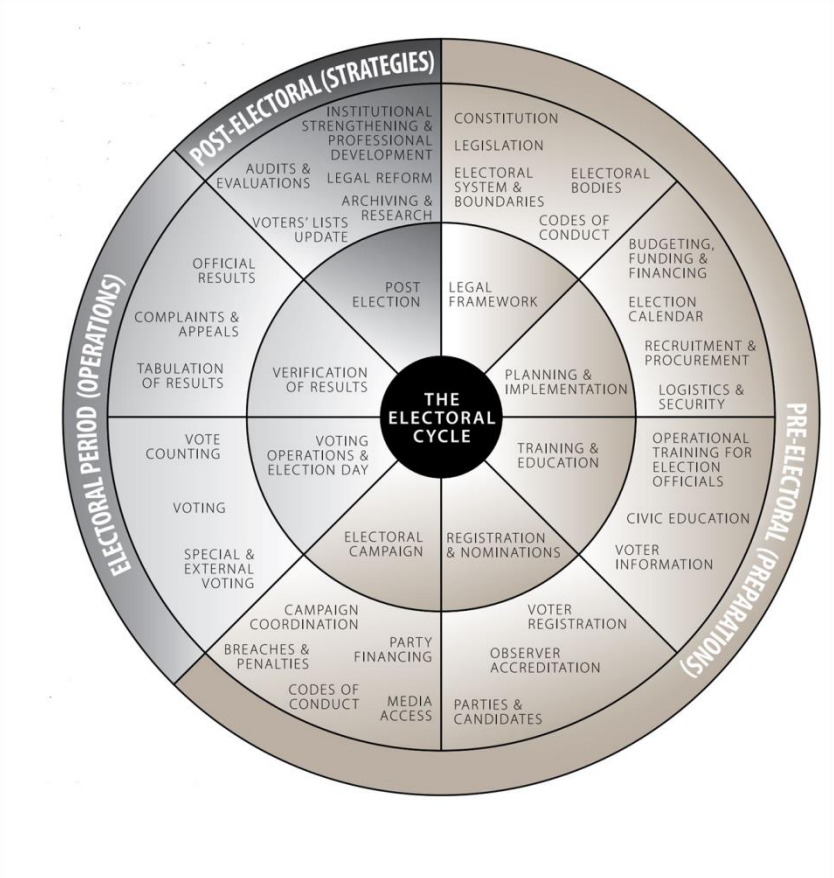


Figure 8 The Electoral Cycle (Source: UNDP)

For the purposes of our meetings with stakeholders in Ukraine, we evolved the electoral cycle into the diagram shown in **Error! Reference source not found.**. This very roughly approximates time (left to r ight) and space (below the centre line moves further away from CEC HQ through DEC and to PEC, while above the centre line into "virtual" space with the WWW.

In this diagram, electoral processes in square brackets, e.g. [PP] are areas for the potential introduction of new technologies. The diagram was used as a conversation starter and helped our study capture stakeholder inputs in a semi-structured manner.

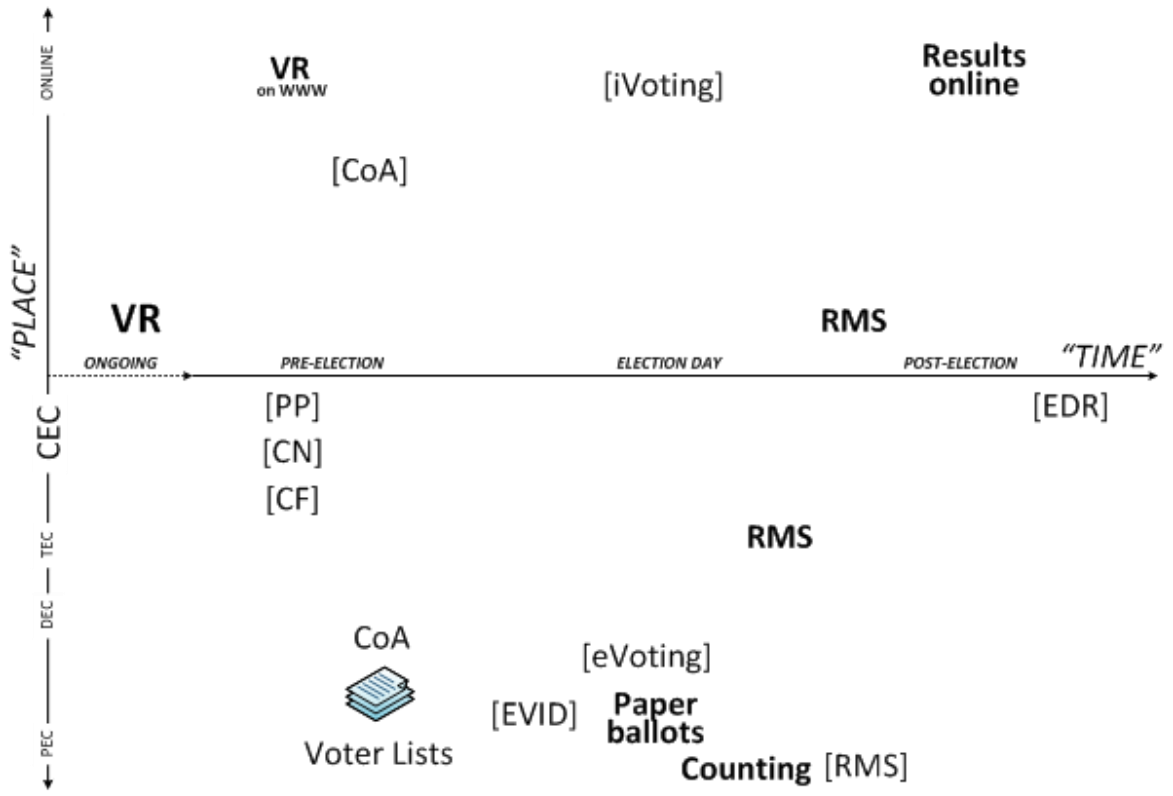


Figure 9 Electoral Cycle Showing Place and Time (Source IFES Ukraine)

Figure 8 Key:

CEC – Central Election Commission
TEC – Territorial Election Commission
DEC – District Election Commission
PEC – Precinct Election Commission
VR – Voter Registration
CoA – Change of (Voting] Address
PP – Political Party Registration
CN – Candidate Nomination
CF – Campaign Finance
eVID – Electronic Voter Identification Device
eVoting – Electronic Voting (at PEC)
iVoting – Internet Voting (remote/unsupervised)
RMS – Results Management System
EDR – Electoral Dispute Resolution

Prepared Questions (sample)

14. What, in your opinion, are the areas of elections management that are most problematic?
15. How do you see new technologies supporting key electoral processes?
16. Have you considered benefits and challenges of new electoral technologies?
17. On what timeline would you like to see implementation of these technologies?
18. What legislative reforms do you anticipate in relation to elections and possible new technologies?
19. How, in your opinion, is CEC different from other institutions of state?
20. What are the cybersecurity implications of new technologies in elections management?
21. How will Ukrainian citizens and voters learn to use, and to trust new technologies applied to election processes?

Annex 4 – Support Letter from Minister of Digital Transformation Office to Feasibility Study Team

МІНІСТЕРСТВО ЦИФРОВОЇ ТРАНСФОРМАЦІЇ УКРАЇНИ

вул. Ділова, 24, м. Київ, 03150, тел. 207-17-30
Web: http://www.e.gov.ua,
код ЄДРПОУ 43220851

1-1/04 № 24 10 2019 На _____ від _____

До уваги зацікавлених сторін,
залучених до виборчого процесу в Україні

Щодо проведення дослідження доцільності
запровадження нових виборчих технологій

Доводимо до Вашого відома, що Міністерство цифрової трансформації України (МЦТ України) проводить дослідження доцільності запровадження нових виборчих технологій спільно з Міжнародною фундацією виборчих систем (IFES) в Україні.

МЦТ України підтримує дану ініціативу та просить Вас сприяти даному процесу та надавати необхідну допомогу команді міжнародних експертів IFES, Ронану МакДермотту, Тома Шанюсо та Владлену Басистому, залучених у проведенні дослідження та необхідних консультацій з усіма ключовими представниками державного сектору, політичними партіями, громадянським суспільством та іншими відповідними зацікавленими сторонами для забезпечення інклюзивного і широкомасштабного процесу в рамках оцінки економічної доцільності та сприйняття використання технічних засобів при проведенні виборів в Україні.

З повагою

Віце-прем'єр-міністр України – Міністр **Михайло Федоров**

Annex 5 – Meetings Held

1. October 7, 2019 – Meeting with representatives of Security Service of Ukraine;
2. October 8, 2019 - Kick off meeting with Vice Prime Minister - Minister of Digital Transformation Mykhailo Fedorov and his team;
3. October 9, 2019 - Meeting with OPORA;
4. October 10, 2019 – Meeting with TAPAS;
5. October 10, 2019 – Meeting with IFES Ukraine consultant on cybersecurity matters;
6. October 10, 2019 – Meeting with National Democratic Institute;
7. October 11, 2019 – Meeting with GoVote;
8. October 15, 2019 – Meeting with EGAP;
9. October 16, 2019 – Meeting with political party “European Solidarity”;
10. October 17, 2019 – Meeting with political party *Holos* (Voice);
11. October 18, 2019 – Meeting with State Special Service on Communication and Information Protection;
12. October 18, 2019 – Meeting with NGO “E-Democracy”;
13. October 22, 2019 – Meeting with OSCE office in Ukraine;
14. October 23, 2019 – Meeting with the representatives of the Central Election Commission (CEC);
15. October 23, 2019 – Meeting with National Institute of Strategic Research;
16. October 24, 2019 – Meeting with political party “Opposition Platform – For Life”;
17. October 24, 2019 – Meeting with Deputy Minister of Digital Transformation Oleksii Vyskub;
18. October 28, 2019 – Meeting with IFES CEC Training Center;
19. November 6th, 2019 – Meeting with political party "Servant of the People";
20. November 7, 2019 – Skype Call with Moldova Expert on perception of Moldova population of iVoting implementation survey;
21. November 12, 2019 – Meeting with political party *Batkivschyna* (Motherland).

Annex 6 – Bibliography and Further Reading

Essential Reading on Electronic Voting

1. Securing the Vote, Protecting American Democracy by the National Academies of Sciences,
2. Engineering, and Medicine, 2018: https://www.carnegie.org/media/filer_public/34/9d/349d3207-d994-4838-8b79-5f8d88e0e412/nas_report.pdf
3. Bruce Schneier essay on Voting Security, 2004: https://www.schneier.com/essays/archives/2004/07/voting_security.html
4. IFES and NDI guide for "Implementing and Overseeing Electronic Voting and Counting
5. Technologies", 2013: https://www.ndi.org/sites/default/files/Implementing_and_Overseeing_Electronic_Voting_and_Counting_Technologies.pdf

Conference Proceedings

The E-Vote-ID Conference is one of the leading international events for e-voting experts from all over the world. In 2016 the two previously bi-annually held conferences, EVOTE and VoteID, were merged into the annual E-VOTE-ID conference. The fourth joint conference took place in October 2019. The proceedings of previous eVote and VoteID conferences are available online and represent a significant resource on the subject of electronic voting and identity:
https://www.e-vote-id.org/proceedings/

Other Important Resources and Documentation

1. Online Voting: Rewards and Risks, report from the Atlantic Council and McAfee, 2014: https://www.atlanticcouncil.org/images/publications/Online_Voting_Rewards_and_Risks.pdf
2. Internet Voting: Past, Present and Future, IFES Ben Goldsmith, 2013: https://www.ifes.org/news/Internet-voting-past-present-and-future
3. European Parliament Brief: Digital technology in elections Efficiency versus credibility, 2018, https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI(2018)625178_EN.pdf
4. Introducing Electronic Voting: Essential Considerations, International IDEA, 2011: https://www.idea.int/sites/default/files/publications/introducing-electronic-voting.pdf
5. Email and Internet Voting: The Overlooked Threat to Election Security, Susan Greenhalgh – National Election Defense Coalition, Susannah Goodman - Common Cause Education Fund, Paul Rosenzweig-R Street Institute, Jeremy Epstein- ACM US Technology Policy Committee, 2016: https://www.acm.org/binaries/content/assets/publicpolicy/jtreportemailInternetvoting.pdf
6. Feasibility study on Internet Voting for the Central Electoral Commission of the Republic of Moldova, 2016: https://www.undp.org/content/dam/moldova/docs/Publications/MD-IVOTE-FSand-Roadmap_cleanENG.pdf
7. Hacking the D.C. Internet Voting Pilot, 2010 by J. Alex Halderman, https://jhalderm.com/pub/papers/dcvoting-fc12.pdf, https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-

offeronline-voting-but-experts-warn-it-isnt-secure/, https://www.youtube.com/watch?v=tHJlRkwOd4U and https://www.youtube.com/watch?v=G4myYkbtkuk

8. OSCE needs assessment mission report for the November 2019 Federal Assembly Elections, providing an analysis of the issues recently identified and further recommendations and context on Internet voting, https://www.osce.org/odihr/elections/switzerland/425009?download=true
9. Evaluation of the e-voting pilot program by the Ministry of Local Government of Norway: https://www.regjeringen.no/en/historical-archive/Stoltenbergs-2nd-Government/Ministry-ofLocal-Government-and-Regiona/tema-og-redaksjonelt-innhold/kampanjesider/e-votetrial/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trials-in-201/summary-of-the-isfreport/id685824/

Global Expertise. Local Solutions.
Sustainable Democracy.

IFES | 2011 Crystal Drive, 10th Floor | 10th Floor | Arlington, VA 22202 | www.IFES.org