Considerations on Internet Voting:
An Overview for Electoral Decision-Makers

IFES White Paper

April 2020

Considerations on Internet Voting: *An Overview for Electoral Decision-Makers*

April 2020

Meredith Applegate
IFES Program Adviser, Ukraine

Thomas Chanussot
Senior Election Technology and Cybersecurity Expert

Vladlen Basysty
IFES Technology and Cybersecurity Manager, Ukraine

The authors would like to thank Peter Erben, Ronan McDermott, Dr. Beata Martin-Rozumiłowicz, Dr. Staffan Darnolf and Olha Antonova for their contributions and review.

Considerations on Internet Voting: An Overview for Electoral Decision-Makers

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

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

Cover photo: Brett Sayles (Pexels)

Table of Contents

Executive Summary

Societies are increasingly relying on technology across various sectors as more and more transactional processes are digitized. This is also becoming the case with elections, where computers and other technology have become indispensable to their conduct. The COVID-19 pandemic currently taking place has increased interest in and the demand for moving services to remote, online spaces. As this demand increases, election decision-makers must recognize the unique nature of electoral processes and take into account important risk factors when considering the use of internet voting.

Today, most election management bodies (EMBs) use some degree of technology to improve electoral processes. From standard office tools and basic websites to sophisticated biometric voter registration databases and fully online internet voting systems, new technologies can promise new opportunities to deliver more efficient, accurate and potentially more transparent elections. They also bring new risks: Technology that is immature, poorly planned, operated incorrectly by untrained users or creates new opportunities for malicious actors to interfere with the security and integrity of electoral processes could undermine public confidence and trust.

Introducing internet voting – specifically, the use of the internet for casting a ballot outside of a polling station – is probably the most difficult technological upgrade for an EMB, as it touches upon the very core of the entire electoral process. Remote internet voting greatly reduces election officials’ direct control over the electoral process. It does provide an opportunity to resolve some historical electoral problems – such as potential enfranchisement of voters abroad, voters with disabilities and internally displaced persons – and presents an opportunity to potentially obtain quicker results free from human errors due to counting, for example. However, it also introduces a wide range of new risks and concerns from the perspective of security, secrecy, transparency and trust. Consequently, the discussion of internet voting usually triggers more criticism and is more disputed than the use of any other technology in elections. Internet voting is still very much an emerging technology, with very few successful cases from which to study and learn.

The relevance of this technology should be evaluated before it is applied in any context according to five parameters: cost, participation, efficiency, trust and security. Security refers not only to the potential for cyberattacks, for example, but also to personal security – namely, the personal privacy and secrecy needed to cast one’s ballot.

While the **cost of internet voting** could eventually become lower than traditional voting, this would take several election cycles to achieve as there is significant new procurement, training, public awareness campaigning and security involved with the launch of this system. Internet voting often relies on unaccounted costs such as a strong identification infrastructure – biometric voter cards, smart ID cards, etc. – which can be expensive if not already in place.

While internet voting can seem appealing to boost voter turnout, studies have shown that this is not generally the case. This research found that **internet voting may make voting more “convenient” for**

existing voters, but it tends not to attract new voters. Young voters, in particular, appear to be more concerned with why they should vote at all, rather than how.

Most forms of electronic voting, including internet voting, improve the speed and reliability of casting ballots. Internet voting can be beneficial for a wider group of people to exercise their rights, such as voters who are unable to travel to their polling stations or voters with disabilities. However, at the same time, internet voting can effectively exclude other communities – those who either do not have access to or do not know how to use the internet, disproportionately impacting older and rural voters in many cases. If implemented, there would be a need for extensive, robust voter education.

The technology that underpins internet voting is highly sophisticated, involving advanced mathematics and cryptography. Most voters will not understand how it works, and this lack of understanding could undermine **public trust**. This trust can be earned by establishing thorough procedures, including audits, and providing stakeholders with enough information for them to fully comprehend the sequence and mechanisms of the voting process. Careful consideration should be given regarding the views of the public. A lack of trust in an electoral process can dramatically impact the perceived legitimacy of those elected.

Security – as well as the perception of security – should be a key consideration before implementing internet voting. Several countries have moved away from limited internet voting programs – including France, the Netherlands and Norway – over security concerns. Countries that experience frequent and sometimes devastating cyberattacks must take all necessary measures to increase the resiliency of their election infrastructure. Personal security, as it relates to voters' privacy, must also be a consideration. With remote internet voting, measures must be taken to ensure that the secrecy of the vote is respected and enforced.

Technologies can strengthen electoral processes if carefully considered and implemented; this process should not be rushed due to the enormous consequences of failure. The first stage in the process of considering the adoption of electronic voting and counting technologies is a robust feasibility study and testing of the new technology on a small constituency, before deploying to scale on a binding election.

Introduction

As technology advances and more transactions become electronic, many have questioned when voting will truly enter the digital age. After all, many internet users trust websites and mobile apps with financial information and social interactions – it seems only natural to have the same level of trust when casting a vote online.

During the COVID-19 pandemic, entire businesses, workplaces, government offices and educational services rapidly moved online. However, elections have unique characteristics. There are many complex, serious issues to consider when it comes to voting through a computer or a phone in an uncontrolled environment – these issues substantially impact the perceived legitimacy of those elected, and the integrity of democracy itself. These issues include public trust, secrecy of the ballot, coercion, intimidation and reliable identification mechanisms. A system needs to be completely verifiable to ensure that all votes are cast as intended and tabulated as cast without jeopardizing the secrecy of the ballot.

This paper does not intend to state whether internet voting should be used or avoided: The International Foundation for Electoral Systems (IFES) is not universally for or against internet voting. Rather, by providing a review of case studies and existing literature, this paper aims to assist election stakeholders in asking the right questions to identify whether internet voting would further improve electoral integrity and democracy, or whether it would instead undermine public trust in and security of the electoral process.

History and Uses of Internet Voting

While internet voting for remote voting has potential in the future, it is a new approach that has only been successfully implemented in very few cases. Internet voting is still a developing technology when it comes to security and trust; many countries have chosen not to use it after conducting feasibility studies or pilots due to these concerns. Internet voting was first used for binding political elections in 2000 in the United States (U.S.) in a pilot across several states targeting out-of-country voters. Since then, approximately one dozen countries have experimented with this technology. This paper does not examine the use of internet voting in controlled environments, such as polling stations, as this is similar to a variety of other electronic voting methods on which there is significant research already.

Estonia is the only country that uses internet voting nationwide. A few others use internet voting in some parts of their country or for certain members of the electorate (Armenia, Australia, Canada, Panama, Switzerland and the U.S.). Some countries have done limited pilots of internet voting and decided not to continue its use (the United Kingdom and Norway). Others initially adopted internet voting but decided to discontinue it (India, France, the Netherlands and Spain).[1] See Annex 2 for further information on how individual countries have used or piloted internet voting. Countries that use internet voting tend to target specific categories of voters – for example, out-of-country voters, diplomatic or military personnel posted abroad, absentee voters or voters with disabilities. In general, internet voting is offered to voters in advance of Election Day for a period that varies from country to country but usually comprises between one and two weeks.

Thematic Analysis

To assess whether internet voting is appropriate, a country must undertake a feasibility study that analyzes how this change impacts critical facets of the democratic process. This study should specifically focus on what issues a country is trying to fix or improve by implementing this technology: e.g., cost or voter turnout. Generally, technology should only be introduced as a “solution” if there is a problem that it could help to mitigate. While Estonia utilizes internet voting nationwide, there are a number of serious reasons that other countries have chosen to not implement this mechanism. Any decision must not only look at the technology that will be required, but also the pros and cons that implementation will have on the electorate and the integrity of the election process. The opportunities – and risks – of this technology should be evaluated before it is applied in any context according to five parameters: cost, participation, efficiency, trust and security.

Cost

Elections are often considered the biggest logistical challenge a country faces during peacetime. The total cost of an election is difficult to estimate as public infrastructure is often used to support operations during Election Day and the counting process. Due to this enormous logistical cost and the

[1] More details and an up-to-date list of countries and models of implementation are available in Annex 2.

use of infrastructure, the idea of digitizing electoral operations is attractive. Cost savings may indeed appear in the long term, assuming that, if voter turnout remains constant, the number of internet voters increases and the number of traditional voters decreases.[2] However, it is unlikely that internet voting would reduce the costs of otherwise expensive items, such as voter registration, boundary delimitation and candidate nomination. In addition, it is likely that remote internet voting would not be the only polling option available for the first one or two election cycles, meaning that election administration would have to offer both in-person polling and internet voting, and therefore rather see an increase rather than decrease in cost in the short term to midterm.

Lessons from Estonia

The Estonian ID card program and online voting system has not been without controversy.

An audit published in 2014 by a team of international researchers criticized lax operational and procedural security. It demonstrated key vulnerabilities that could potentially be exploited to overwrite votes and take control of the servers.

A critical vulnerability identified in 2017 in the ID card system, allowing anyone who knows the public key of an ID card to copy the private key at a relatively low cost and use it to fully control a person's identity without possessing the physical ID card. The impact of this vulnerability on the election process could have been extremely damaging had the timing of the disclosure been different. Estonian authorities recovered from the crisis by adopting a policy of maximum transparency about the impact of the vulnerability and the actions they were taking to mitigate it. This is only possible in a context where the public trusts the authorities and where the population is relatively small and homogeneous – Estonia had 887,420 eligible voters in 2019.

A number of studies and publications demonstrate that the cost of internet voting is much lower than standard voting – approximately half. However, *they do not account for the cost of training and public awareness exercises nor the cost of establishing a trusted electronic identity infrastructure*, such as the one on which the Estonian internet voting system relies.

The Estonian internet voting system is fundamentally built on the Estonian ID card. It is not possible, therefore, to reasonably separate out the cost of internet voting from the decades of investment in a large-scale e-governance ecosystem that includes the inter-agency data exchange system (X-road), a mandatory electronic ID document (both of which the Estonian government has been developing since the 1990s) and the provision of internet voting (eesti.ee).[3] The Estonian card is a mandatory national ID for citizens, which is a smart card allowing for both secure remote authentication and legally binding

[2] International Foundation for Electoral Systems, Ben Goldsmith, *Internet Voting: Past, Present and Future, 2013*; https://www.ifes.org/news/Internet-voting-past-present-and-future

[3] Estonia has made a substantial investment in their e-governance ecosystem, the full cost of which is difficult to estimate and not publicly available. Some estimates place maintenance of x-road alone at 50 to 60 million USD per year https://www.innovations.harvard.edu/blog/estonia-one-small-country-digital-government-having-big-impact-x-road

digital signatures for use in the Estonian state-supported public key infrastructure.[4] The smart cards were introduced in 2002 and the services have been progressively expanded over years. This infrastructure can be used for identification and authentication for all government services, such as tax declarations, proof of identity to access bank accounts, check medical records and use e-prescriptions and more. There has been criticism during audits[5] and disclosure of vulnerabilities[6] (see "Lessons from Estonia" in the text box above)[7]. In Estonia, voters authenticate themselves on a website to cast their electronic votes. They use additional hardware: the ID card reader, connected to their computer, reading the encrypted key on the card. Voters can change their electronic votes an unlimited number of times, with their final vote being the definitive one that is tabulated. It is also possible for anyone who votes using the internet to vote at a polling station during the early voting period, automatically invalidating their internet vote, but requires polling stations that can accommodate voters whether they have voted online or not.

Thus, while initial cost calculations may seem to favor internet voting in short-term horizons, factoring in medium- and long-terms costs that are not immediately intuitive can lead to a very different cost calculation. It is imperative that this takes place at the start of discussions so that stakeholders fully understand the criteria upon which they are basing their decisions of whether or not to implement such a technology.

Lessons from Norway

Norway piloted a limited internet voting system for municipal elections in 2011 and 2013, but canceled the project in 2014, citing security concerns and the government's conclusion that, contrary to expectations, the new system had not improved turnout. Norway's Institute of Social Research said that there was "*no evidence that the trial led to a rise in the overall number of people voting nor that it mobilized new groups, such as young people, to vote." Even just a "low-effort" review of the system by computer experts from the Norwegian Computing Center and the Norwegian University of Science and Technology found "significant problems" with security, among other things, to the extent that the experts said the software did "not have acceptable quality for use in an e-voting system.*" It is useful to note that the Norwegian authorities did not mention security as a primary concern, contrary to most other evaluations and case studies. It is however reported that voters have very limited knowledge about the security mechanisms in the system, affecting the premise of free and fair elections.

[4] Robert Krimmer, David Duenas-Cid and Iuliia Krivonosova (2020) *New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper?*, Public Money & Management: https://www.tandfonline.com/doi/full/10.1080/09540962.2020.1732027

[5] Review of the official publication and response following the ROCA bug identified in the Estonian ID card; https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf and https://e-estonia.com/wp-content/uploads/faq-a4-v02-id-card-1.pdf)

[6] Presentation of the audit from the international team; https://estoniaevoting.org/ and https://nordicinnovationlabs.com/wp-content/uploads/2018/07/ivoting-ccs14.pdf; response from the Estonian Election Commission; https://estoniaevoting.org/press- release/response-national-election-committees-statement/

[7] Recommendations from OSCE/ODIHR Estonia Parliamentary Elections Final Reports, 2005-2019.

Impact on 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 voting channels 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, the type or level of elections, trust in parties and candidates, intensity of the campaign and the media's interest in the election.

The COVID-19 pandemic presents an unprecedented situation for the modern world, with citizens in multiple countries unable to travel or leave their homes. An online, remote-based voting system could resolve some of the obstacles to participation if, for example, large swaths of the electorate were unable to physically travel to a polling station due to a sudden national (or, in this case, global) emergency. However, a system that utilizes remote, online voting takes a long period to establish effectively. If it is already in place and tested prior to the emergency, this might be a positive in terms of turnout during a crisis such as COVID-19. However, due to the high levels of planning, preparation and testing needed, it is unlikely that countries that do not already have systems in place would be able – or should even attempt – to launch internet voting as an immediate response to a crisis.

Being the only country that implements nationwide internet voting, Estonia can again provide some quantitative data and insights.[8] In Estonia, there was no significant change in voter participation after the introduction of internet voting; it has been observed to be a substitute voting mechanism for voters already engaged in the electoral process.[9] The main takeaway in terms of voter experience is that it makes voting more "convenient" for existing voters, rather than increasing the participation of those who had not voted previously.[10] The trend indicates that more and more people vote online, and that voters who have voted online once will continue doing so.

The Norwegian example also adds an interesting finding regarding youth voters, who are very often used as an argument in favor of online voting. Young voters participating in the pilot election in Norway

[8] Tove Wigartz (University of Gothenburg), *Does Internet voting in Estonia affect voter turnout?, 2017*; https://core.ac.uk/download/pdf/95665595.pdf

[9] Kitsing Meelis, *Online participation in Estonia: Active voting, low engagement*, *2011*; https://www.researchgate.net/publication/221547555_Online_participation_in_Estonia_Active_voting_low_engagement

[10] Other references to the impact of internet voting on voter turnout in Estonia; http://www.democraticaudit.com/2013/10/03/the-estonian-experience-shows-that-while-online-voting-is-faster-and-cheaper-it-hasnt-increased-turn-out/; a review of the statistics of internet voting maintained by the government of Estonia; https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia

seemed to prefer to vote in their polling station on Election Day as a political statement. Based on findings by the commission analyzing the results of the pilot, young people reported being more concerned about the question of why young people should vote than how they will vote.[11] While internet voting should not be excluded in terms of its potential for increasing voter participation, this must be accompanied by wider civic and voter education and public information that will encourage voters to participate in the political process.

Accessibility

The right to vote for elected representatives is a cornerstone of democracy, enshrined in numerous international commitments including the Copenhagen Document and the United Nations Convention on the Rights of Persons with Disabilities. However, for voters with disabilities whose polling stations are not accessible, this right is largely not respected in many countries around the world. Internet voting could provide the opportunity for more people with disabilities to access their right to cast a ballot if no other remote voting options are available. In addition, the ability for a voter with disability to use their own electronic device to vote could provide more ease of access, as many devices include accessibility functions that provide additional audio or large text options, for example. However, even if remote internet voting does provide some ease of access for people with disabilities, it must be coupled with accessible voter registration and identification processes, as well as voter information and education in formats that are accessible and easy to understand for all voters, including voters with disabilities.

Efficiency

Internet voting can potentially make the voting process significantly faster for voters who are able to use it, saving the time and perhaps physical barriers 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; particular care should be exercised to understand the level of technological literacy in a country. Attention should also be paid to infrastructure, both in terms of levels of publicly available internet as well as personal infrastructure – whether or not people have mobile phones with sufficient data plans, whether they have computers with connection to sufficient bandwidth, etc.

While results and voting itself are much faster 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. In terms of timing – and legality – decision-makers must also consider what legal amendments are necessary to introduce remote internet voting as an option.[12] Depending on the context, this

[11] Study of the impact of internet voting in Norway; https://www.regjeringen.no/en/historical-archive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regiona/tema-og-redaksjonelt-innhold/kampanjesider/e-vote-trial/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trials-in-201/summary-of-the-isf-report/id685824/

[12] 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: https://www.regjeringen.no/globalassets/upload/krd/prosjekter/e-valg/evaluering/topic7_assessment.pdf. The 2017 Council of Europe Recommendation is probably the most

amendment process could be extensive and take significant time. Legal considerations should include items such as:

- Secrecy of the vote: One of the most controversial issues is 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 remotely on a personal device.[13]
- 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, recounts, a voter verifiable audit trail and more.
- Effect on transparency requirements, such as the role of observers and party agents
- Impact of internet voting on invalid and blank votes

Eventually, introducing any kind of e-voting requires substantial changes to the national legal framework governing elections.[14] 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.

End-to-End Verifiability

End-to-end (E2E) verifiability is a requirement for any credible e-voting 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. Like all internet-facing systems, E2E does not protect against sophisticated malware that could have been specifically designed to spy on a voter's selections, compromise ballot secrecy or vote fraudulently on a voter's behalf.

Additionally, it is difficult to provide a way for voters to verify how they voted without also making it possible for the voters to prove to a third party how they voted, which introduces the risk of vote buying

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*: https://www.coe.int/en/web/electoral-assistance/-/council-of-europe-adopts-new-recommendation-on-standards-for-e-voting. There is also an emerging body of other electronic voting standards by IFES, OSCE/ODIHR, the Carter Center and others, particularly regarding electoral observation but also applicable as guidelines for EMBs.

[13] This discussion also pertains to postal voting and the possibility for voters to vote multiple times. Estonia, discussed later, mitigates this and potential coercion by only counting the last online ballot cast by a voter. In Estonia, it is also possible for anyone who has voted through the internet to cast their vote in person at a polling station on Election Day, which nullifies his or her internet vote.

[14] The Venice Commission Code of Good Practice in Electoral Matters states that major changes to electoral legislation should not take place within the year before an election event; https://rm.coe.int/090000168092af01

or coercion. Over the years, Estonia has improved the techniques to allow voters to check their vote before it is permanently recorded. After casting a ballot at a computer, each voter receives a QR code that is valid only for 30 minutes and allows the voter to check the vote from a different device: e.g., a smartphone.[15] This, of course, relies on a voter having multiple devices with an internet connection. Note that the verifiability property of E2E in internet voting also makes it vulnerable to vote buying, and there is currently no technology that can efficiently mitigate this.

Limited Ability to Audit Results

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. Unlike some modern e-voting machines, there is no paper audit trail. This makes it more difficult for EMBs to audit results should there be a dispute. 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.[16] A ballot comparison audit 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.[17] Their benefits have been lauded by political scientists, statisticians and election security experts.[18]

Trust and Transparency

Electoral systems 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. A number of factors contribute to this trust, including public perception of the EMB itself, the political environment, the history of fraud or malpractice in a specific country and trust in the system itself and the tools used in the election process. EMBs 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.

[15] A QR code is a type of three-dimensional barcode, most of the time used to encode information (URL or contact details) and decoded with the help of a dedicated app on a mobile phone; https://en.wikipedia.org/wiki/QR_code

[16] Mark Lindeman and Philip B. Stark, *A gentle introduction to Risk Limiting Audits*, *2012*; https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

[17] The Belfer Center, *State and Local Election Cybersecurity Playbook, 2016*; https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

[18] The Brennan Center, *America's Voting Machines at Risk, 2015*; https://www.brennancenter.org/sites default/files/publications/Americas_Voting_Machines_At_Risk.pdf

The introduction of any new technology to an electoral process needs to be carefully planned[19]. A negative first experience – or a poorly handled vulnerability exposure – can turn electoral stakeholders against technology, and trust then becomes difficult to regain. This has happened in a number of instances: The Barcelona referendum in Spain[20] was contentious in many ways, including the voting process itself, with impersonation cases reported and sent to court; and the public expressed security concerns in Norway[21] and in France.[22] Beyond voters, electoral managers and their staff must also trust and understand the technology they use in their work. This can only be achieved through rigorous evaluation processes and by effective training strategies. External service providers involved in an election must also comply with laws and requirements; if service providers appear to be in breach of the law, stakeholder trust plummets. EMBs should undertake a special risk assessment regarding external service providers' potential associations and dependencies, as these connections could undermine the new system's credibility. This is not limited to private sector vendors, but also the dependencies of other state institutions.

Lessons from Switzerland

Cantons in Switzerland have been experimenting with internet voting, but the number of eligible and participating voters has remained marginal due to ongoing tests and audits, cost and public trust. Two systems have been trialed in parallel. The sVote system from Swiss Post is proprietary, disclosed software developed by Scytl. It provides the option for Swiss resident voters and those abroad to vote via a mobile app and a website. The voter authentication method is substantially different than Estonia's. It does not rely on a sophisticated ID card, but rather on a unique security code sent to them by post; pre-registration is required by voters in order to receive the security codes. Voters then have to enter their voter numbers, unique security codes, birth dates and municipality of origin. Swiss internet voting was the subject of a heated debate when the authorities organized a "bug bounty," during which critical vulnerabilities were identified and publicly disclosed. This system has now been abandoned by the Swiss authorities. A second system – the Geneva System – has also been recently discontinued. The future of internet voting in Switzerland is, thus, currently unclear.

Beyond possibilities for fraud, which are examined further in the "Security Concerns" section below, poorly trained administrators can inadvertently create errors that swiftly erode public trust. Voters who do not understand how to properly use the system could make mistakes themselves, and later attribute this to purposeful malfeasance on the part of the EMB. Piloting and introducing internet voting projects should only be done in a political and social context where a high level of trust in the electoral system

[19] ACE Project, *Guiding principles for election technology – trust and transparency*; http://aceproject.org/main/english/et/et20.htm

[20] *Datasheet regarding Barcelona's referendum*, p. 124; https://www.regjeringen.no/globalassets/upload/krd/prosjekter/e-valg/evaluering/topic6_assessment.pdf

[21] https://www.bbc.com/news/technology-28055678

[22] https://www.reuters.com/article/us-france-election-cyber/france-drops-electronic-voting-for-citizens-abroad-over-cybersecurity-fears-idUSKBN16D233

already exists. Internet voting itself will not necessarily increase trust, and might actually decrease it,[23] or be used as a partisan or political tool. Similarly, a lack of public trust in the impartiality of the election staff will not be regained by introducing more technology into the process; rather, this trust is built by actively fighting against corrupt practices and increasing transparency. These issues of trust need to be dealt with comprehensively before technology is introduced to an election process.

Security Concerns

Over the past decade, there have been numerous high-profile cases of attacks on internet portals, viruses that have shut down the websites of government agencies and major corporations and ransomware that has crippled organizations by encrypting their data. 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 or malware designed to manipulate the vote.

A virus, if not detected by an anti-virus program on a voter's computer, could manipulate the victim's vote in favor of the specific attacker's party. It is 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 preventing a voter from casting his or her 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.

Election officials usually have higher-level permissions to add eligible voters to the voter registration database, remove ineligible voters, configure ballot styles, define the time and date to cast ballots, set up the tallying rules for the election contests, and generate election reports. These stakeholders may maliciously and intentionally compromise the system or unintentionally participate in an attack via an infected machine. The automation and computerization of election officials' tasks needs to be accompanied with a set of protocols that would prevent hidden attacks against the system, appropriate levels of login profiles, passwords and auditing, and trainings and awareness programs on cybersecurity risks.

[23] Presentation of the bug bounty in Switzerland; https://www.theverge.com/2019/2/12/18221570/swiss-e-electronic-voting-public-intrusion-test-hacking-white-hack-bug-bounties

System administrators have the highest level of permissions in administering a server and other election information systems. Most of the time, they have physical access to the equipment and are allowed to install, configure and monitor different components of the voting system to ensure it functions properly. They may intentionally or accidentally contribute to an attack by using infected USB flash drives, for example, or by intentionally or unintentionally lowering the protection of the systems. In certain environments, personal threats against key information and communication technology staff should be considered, as they could provide information that could be exploited by adversaries.

The National Institute of Standards and Technology (NIST)[24] Cybersecurity Framework provides several recommendations to mitigate these risks against these actors. These should be taken with caution – they do not release an organization from performing a thorough threat modeling and risk management plan, as no cybersecurity strategy is ever completely effective. Among its recommendations, NIST advises using cryptographic protections (for data transfer and data at rest), advance cryptographic voting techniques, the use of dedicated and trusted hardware (such as an e-ID card), end-point security scanning (to verify that a piece of software used for voting has not been altered), pre-configurable booting environment or virtualization technology (difficult to apply for each voter's devices, but which can potentially thwart malicious software) and secondary communication channels (such as the Estonian QR code that allows voters to verify their vote with an alternate device).

Lessons from Washington, D.C.

In 2010, the District of Columbia Board of Elections issued an open invitation for hackers to find vulnerabilities in an internet voting pilot program to allow out-of-country voters and military personnel to cast ballots online. A team led by researchers from the University of Michigan was able to get into the system in less than 36 hours and gained access to all the identification and passwords of the eligible voters. They modified all the votes to an imaginary candidate without the administrators of the program even noticing it, even gaining access to the video surveillance system of the election commission. Through numerous articles and interviews online, this case generated wide public discussion and became an example of how much damage can be done to the credibility of an election commission when exposing an insecure information system. In the U.S., internet voting is used in more than 30 states, mostly for out-of-country voters and military personnel, despite warnings and recommendations from experts and various committees.

Online Blockchain Voting

In the last three years, there has been an increased effort to market online voting. With this surge, commercial companies have started to promote the use of blockchain as a "platform" by which ballots

[24] The National Institute of Standards and Technology at the request of the U.S. Election Assistance Commission, *The Security Considerations for Remote Electronic UOCAVA Voting*, *2011;* https://www.nist.gov/sites/default/files/documents/itl/vote/NISTIR-7700-feb2011.pdf

can be transmitted from voters' private devices to a centralized tabulation facility, alleging to provide E2E properties.

A blockchain is a type of distributed database. It is usually owned and operated by several independent entities acting as peers. Each peer records new transactions, which are cryptographically encrypted with a signature of the previous transaction. By design, a blockchain is resistant to data modification by one peer, a property called immutability. In a blockchain-based election, the blockchain serves as a distributed ballot box holding the cast ballots, although it is sometimes used to hold other information as well.

One fundamental point for blockchain is that it relies on having multiple peers. With only one peer – the EMB – there is no data immutability and the benefit of using blockchain is lost.

Lessons from Germany

The German Constitutional Court 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.

Unfortunately, most serious vulnerabilities threatening the integrity and secrecy of voting happen before ballots ever reach the blockchain.[25] Most of these solutions do not resolve the voter ID issue, for example. This is crucial to the credibility of an election. Estonia, for instance, has resolved this issue without blockchain by using e-ID cards. Additionally, the security of the device from which voters cast the online ballot is largely outside the scope of these blockchain systems. Blockchain technology also does not protect against distributed-denial-of-service attacks that make servers unable to operate, does not protect information as it travels on the internet and does not make servers and infrastructure more resistant to advanced persistent threats.

[25] David Jefferson (Verified Voting), *The Myth of "Secure" Blockchain Voting*; https://www.verifiedvoting.org/wp-content/uploads/2018/10/The-Myth-of-_Secure_-Blockchain-Voting-1002.pdf

Conclusion

The introduction of new technology, such as internet voting, needs to answer a specific problem. Before considering remote internet voting, or any other technology solution, it is critical that an EMB first identify issues in the election process that it is trying to mitigate or address. If remote internet voting is deemed to address this problem, it must then be carefully considered before being implemented. While new technology certainly presents opportunities, lack of preparation or due diligence could cause extensive damage to public trust and the integrity of an election itself. There are different ways of integrating remote voting technology, from targeting a limited voting population for which casting a ballot is a challenge, to ambitiously trying to improve national turnout and reduce cost of polling. Remote internet voting is one option; numerous other avenues for electronic solutions exist. Those considering internet voting as a global solution should carefully evaluate potential impacts on cost, participation, efficiency, trust and security.

This paper presents an overview of key considerations from existing literature and highlighted in different case studies. This overview is intended to encourage further study of this topic before decisions are made and present a broad range of issues and perspectives for consideration. These global experiences also bring with them an amount of caution:

- Political and social contexts vary from one country to another. A successful experience in Estonia does not mean that this model is good for another country. A failed pilot in one country can also drive its own stakeholders away from technology for the longer term.
- Cost is an important factor. All costs need to be properly calculated at the start of discussions to ensure that stakeholders fully understand the criteria upon which they are basing their decisions.
- There is not a single instance to date in which internet voting has increased voter participation.
- The legal framework will require adjustments to allow the use of new technology during the vote casting. This might impact the time necessary to fully deploy the technology in legally binding elections.
- Introducing technology does not automatically increase trust. Trust can be only earned by establishing proper procedures and audits and providing stakeholders with transparency and enough access and information to fully understand the sequence and the mechanisms of the voting process. Trust is built from the outset – EMBs must ensure that the piloting and design phases include consultation with external stakeholders.
- Remote voting can impact the secrecy of the vote. Without in-person oversight of the voting process by polling station workers, for example, EMBs must be aware of possibilities for external pressure, vote buying or abuse and take measures to counteract this.
- Security and, importantly, the perception of security, is a key factor that should drive the conversation around internet voting.

While there are benefits that countries could gain from piloting internet voting, particularly for specific groups of voters such as persons with disabilities, internally displaced persons, voters in occupied territories or the diaspora, the risks have to be carefully assessed. Many countries have moved away from internet voting – and electronic voting more widely – due to security concerns and issues of public trust.

Successful deployments of this technology have shown that it needs to be built on a strong existing infrastructure that citizens are familiar with and rely upon for other services, such as in Estonia, rather than a new platform created specifically for internet voting.

Any and all efforts to digitalize a country's electoral process – including internet voting – should be carefully considered through a feasibility study that incorporates international research and national context. This is in line with European good practice and should precede potential piloting and subsequent rollout.

Annex 1 – Additional Resources and Documentation

Essential Resources

1. Securing the Vote, Protecting American Democracy by the National Academies of Sciences, Engineering, and Medicine, 2018: https://www.carnegie.org/media/filer_public/34/9d/349d3207-d994-4838-8b79-5f8d88e0e412/nas_report.pdf
2. Bruce Schneier essay on Voting Security, 2004: https://www.schneier.com/essays/archives/2004/07/voting_security.html
3. International Foundation for Electoral Systems and National Democratic Institute 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

Other Important Resources and Documentation

1. Online Voting: Rewards and Risks, Report from The Atlantic Council and McAfee, 2014: https://www.verifiedvoting.org/wp-content/uploads/2014/10/Online_Voting_Rewards_and_Risks.pdf
2. “Internet Voting: Past, Present and Future,” International Foundation for Electoral Systems, 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/public-policy/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-FS-and-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-offer-online-voting-but-experts-warn-it-isnt-secure/, https://www.youtube.com/watch?v=tHJlRkwOd4U and https://www.youtube.com/watch?v=G4myYkbtkuk
8. Organization for Security and Co-operation in Europe 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-of-Local-Government-and-Regiona/tema-og-redaksjonelt-innhold/kampanjesider/e-vote-trial/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trials-in-201/summary-of-the-isf-report/id685824/
10. International Foundation for Electoral Systems, “International Experience with E-Voting, Norwegian E-Vote Project” by Jordi Barrat i Esteve, Ben Goldsmith and John Turner, 2012: https://www.regjeringen.no/en/historical-archive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regiona/tema-og-redaksjonelt-innhold/kampanjesider/e-vote-trial/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trials-in-201/id684642/

Annex 2 – Countries that Use Internet Voting (Use of Internet Voting Outside of Polling Stations in Politically Binding Elections)

Used Nationwide	Used in Some Parts of the Country or for Some Type of Voters	Planned to be Piloted or Piloted but Discontinued or Never Used
Estonia is the only country to allow all citizens the option of online voting in local, national and European elections.	**Armenia**: Diplomatic staff and their families can vote online.	**France**: Voting was used for out-of-country voters in the 2012 parliamentary elections but discontinued in 2017 due to security concerns; the government plans to bring it back in 2022. Out-of-country residents also voted online in the 2016 Republican party primaries.
	Australia: Online voting was trialed for out-of-country military personnel in 2017 but has been discontinued. New South Wales allows some groups – voters with disabilities, living in remote areas, out of state – to vote online, but there are no plans to extend this option to other states.	**India**: In 2010, internet voting was trialed in the local elections in the state of Gujarat.
	Canada: Online voting is possible for municipal elections in some districts of Ontario and Nova Scotia. Canada has considered introducing internet voting in federal elections.	**Norway**: Online voting for 2011 local and 2013 national elections was made available in some districts. In 2014, internet voting was discontinued for security reasons.
	Mexico: Some states have allowed online voting for out-of-country voters.	In 2004, the **Netherlands** used internet voting for an election to the *Rijnland* water board and in 2006 for out-of-country voters for national elections. Internet voting was discontinued in 2017 due to security concerns.
	New Zealand: Out-of-country voters can vote online.	**Spain**: In 2010, Barcelona held an online referendum on an urban

		development project. The voting was a one-off, online-only pilot and was highly controversial.[26]
	Panama: Out-of-country voters can vote online.	**United Kingdom**: Online voting was trialed in local council elections between 2002 and 2007.
	Switzerland: Some cantons offer online voting to out-of-country voters – also in a few cases, to resident voters – in elections and referendums. The stated goal is to roll out internet voting to the entire country.	**Russia** is set to introduce its first online voting system. The system will be tested in a Moscow neighborhood that will elect a single member to the capital's city council in September 2019. One of the first experiments to introduce internet voting was conducted by the Electoral Commission of the Volgograd Region during voting in Uryupinsk in 2009, and in the Odintsovo district in 2010.
	United States: Despite the security concerns raised after a District of Columbia trial of internet voting was hacked, more than 30 U.S. states allow military personnel and out-of-country residents to vote online. Voters using online or mail-in ballots waive their secrecy rights.	**Finland** has appointed a working group to study the technical feasibility of an online voting system. It determined that the technology does not yet sufficiently meet all the requirements, citing problems with reconciliation of verifiability and election secrecy.

Source: http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI(2018)625178_EN.pdf

[26] The Spanish city of Barcelona encountered problems in relation to voter identification and identity theft, with a prominent voter finding that someone had already logged on with his authentication details and cast a ballot for him; https://www.regjeringen.no/globalassets/upload/krd/prosjekter/e-valg/evaluering/topic6_assessment.pdf

About the Authors

Meredith Applegate, IFES Program Adviser, Ukraine

Meredith Applegate is the program adviser for IFES in Ukraine. She brings over 10 years of experience developing, managing and implementing election and democracy programs in headquarters and the field. She is particularly focused on gender equality, civil society advocacy and development, voter and civic education, and disability rights. Applegate has held long-term posts in Indonesia, Myanmar and Ukraine. She has also worked on short-term to midterm assignments on election operations, civic and voter education, and ending violence against women in elections, including for the United Nations Entity for Gender Equality and the Empowerment of Women in Sierra Leone, United Nations Development Programme in Moldova and IFES programs in Cambodia, the Dominican Republic, Nepal and Timor-Leste.

Vladlen Basysty, IFES Technology and Cybersecurity Manager, Ukraine

Vladlen Basysty is the technology and cybersecurity manager for IFES in Ukraine. Basysty has 16 years of experience managing information technology projects with organizations including the International Organization for Migration, CGI Federal, the United States Embassy in Ukraine, the Office of the United States Department of Homeland Security, Federal Law Enforcement Training Center, John Snow Institute/United States Agency for International Development project, "AIDS Foundation East-West," and United States Peace Corps in Ukraine.

Thomas Chanussot, Senior Election Technology and Cybersecurity Expert

Thomas Chanussot has been working in the field of elections since 2004. With a background in information technology, he has been involved in more than 12 electoral operations around the world, particularly in voter list and result management technology, during which he has held diverse roles including system development, security audits and team management. He has worked extensively on mission-critical electoral infrastructure, designing and securing biometric and nonbiometric voter list databases, as well as result management systems. He now manages several critical electoral cybersecurity initiatives in Asia and Eastern Europe and leads cybersecurity assessments for IFES.

INTERNATIONAL FOUNDATION FOR ELECTORAL SYSTEMS

IFES

· 30 Years ·

Global Expertise. Local Solutions.
Sustainable Democracy.

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