Policy paper
Internet Voting: Challenges and Solutions

Introduction

Digital technologies provide the public with the multitude of more accessible, connecting, and instant e-activism opportunities. Albeit, this comes with a price. Internet access to e-participation portals makes them more vulnerable to internal corruption and external hacking while online media make the public opinion more susceptible to manipulation. These issues are especially pertinent for electronic voting as a principal method of decision making in internet politics, electronic governance, and digital democracy. Nevertheless, due to a set of solutions in architecture, legislature, procedures, and awareness, e-voting risks can be mitigated.

Thereby, the aim of this paper is to identify, structure, and remit the risks of electronic voting by offering practical solutions for countering them. In the context of a wider electoral reform, after a cost-benefit analysis has been performed and the introduction of internet voting has been decided upon, this policy paper can help foresee presumable challenges and refute ungrounded objections. In contrast to most publications that either focus on particular risks or describe proper i-voting, this paper inspects multiple challenges and addresses them. It is intended as a reference for politicians, public officials, civic activists, and citizens overall for preventing, detecting, and mitigating i-voting misuse, safeguarding e-democracy against distortions, and strengthening good governance.

For the purposes of this inquiry, of all varieties of electronic voting (e-voting), such as voting via an electronic voting machine inside a polling station or remote electronic voting using a 'kiosk' outside a polling station, specifically remote internet voting is taken into account. Here, internet voting (i-voting) is defined as voting using internet and computer technologies at least for casting and counting votes. In this sense, it is synonymous to online voting and mobile voting.

As a universal e-participation tool, i-voting is viewed in relation to a wide spectrum of e-democracy formats, including but not limited to non-binding online opinion polls, binding e-voting for policies, participatory budgeting projects, e-plebiscites, e-referenda, and e-elections (i-elections, online elections). Thereby, i-voting can serve representative, direct, participatory, liquid, and other forms of democracy.

This study is based on a desk review of existing academic and policy research and the analysis of the available secondary data on i-voting statistics. The conclusions are drawn from national and local cases, and therefore are potentially applicable to a range of remote i-voting designs in diverse political contexts.

The paper presents the temporal sequence of major i-voting challenges, offers recommended solutions, analyses each typical i-voting issue in greater detail, and concludes with final reflections. Also, it includes a succinct overview of countries that practised and abandoned, abandoned and considered, currently practise, and consider i-elections.

Author: Dmytro Khutkyy, Policy and Advocacy Advisor, European Digital Development Alliance.

Reviewers: Daniel Innerarity, Professor, School of Transnational Governance, European University Institute, Italy; Robert Krimmer, Professor of e-Governance, TalTech Tallinn University of Technology, Estonia.

Acknowledgement: This work has been prepared within the framework of the Policy Leader Fellowship at the School of Transnational Governance, European University Institute.

Disclaimer: *The position and opinion expressed are those of the author and do not necessarily represent the position and opinion of the European University Institute (EUI) or the School of Transnational Governance (STG).*

Publisher: European Digital Development Alliance, Brussels, Belgium, August 2020.

Principal points

	Risks	Solutions
1.	**Issue framing:** Manipulating the ballot for i-voting in a poll, survey, plebiscite, referendum or an election; also – framing a voting issue in mass media discourse	**Balanced formulation:** Ensured by a commission review, advance publication, discussion, and correction of the ballot; free access to the Internet
2.	**Biased polarisation:** Preselection effect and confirmation bias lead to group polarisation and create filter bubbles and a distorted social reality	**Deliberative connection:** Facilitation of a setting supportive of the diversity of views, a critical perception of information, and intelligent discussion
3.	**Public opinion manipulation:** Using big data, bots, and paid writers for opaque micro-targeting individual voters with personalised messages	**Online media regulation:** A systemic legislative, enforcement, and civic action to impose limits, ensure disclosure, and implementation
4.	**Technical system malfunctioning:** Hardware or software technical issues with the voting system, as well as human errors in using them	**Reliable system functioning:** Performing system tests, training i-voting administrators, planning technical and organisational contingency measures
5.	**Malicious hacking:** Cyber security concerns related to hacking an i-voting system by in-country or out-country governmental or non-governmental agents	**Cyber security and integrity:** System evaluation and certification, cyber security strategy, system test, bug contest, staff training, and educational campaign
6.	**Exclusion:** Concerns about the legal eligibility of certain groups and the accessibility issues imposed by the digital divide	**Inclusion:** Guaranteeing the right to vote to all eligible citizens, adding i-voting as an additional option to the traditional offline voting
7.	**Inaccurate voter registers:** Corrupt voter registers may be misused to prevent certain people from voting and exploit fake records for hacked voting	**Accurate voter registers:** Standard technical and organisational measures combined with distributed ledger technologies, such as blockchain
8.	**Misidentification:** The risk that some eligible voters will not be allowed to vote while some fake voters will vote without having the right to do so	**Identification reliability:** Introduce several stages of reliable identification that combined will minimise misidentification risks
9.	**Vote disclosure, pressure, and buying:** The challenges of voluntary or forced vote disclosure, group pressure, vote coercion, and vote buying	**Voting secrecy, freedom, and integrity:** Technical and organisational mechanisms, vote changes, awareness raising, reporting, and enforcement
10.	**Routine voting and absenteeism:** The decreased symbolic value of the vote casting act leading to a less massive and unifying voting campaign	**Value-based deliberate voting:** Digital technologies facilitate civic action and new rituals; civic education and awareness-raising motivate for voting
11.	**Corrupt vote storage and counting:** I-voting results may be distorted at the stages of vote recording, storage, and counting	**Verifiability and accountability:** End-to-end verifiability, distributed ledger technologies, *Prêt à Voter* system, voting trials, audits, and accountability
12.	**Voting campaign discreditation:** Manipulated voting can decrease the trust towards democratic institutions and harm the legitimacy of voting results	**Legitimacy and trust:** Early and balanced expert discussion about i-voting design combined with the transparency-based communication for the public

1. Issue framing *versus* balanced formulation

Already at the earliest stages of preparing i-voting the formulation of its subject might be problematic. Primarily this refers to non-binding opinion polls or surveys and to binding plebiscites or referendums, but can also relate to elections. The Council of Europe guidelines on e-voting clearly state: "All official voting information shall be presented in an equal way, within and across voting channels… The electronic ballot used for e-voting should be free from any information about voting options, other than that required by law… If information about voting options is accessible from the e-voting site, it shall be presented in an equitable manner."[1]

In a worst-case scenario, a corrupt ballot for i-elections would (i) violate the law-defined (random) order by positioning the preferred individual candidate for a public office or a party at the top of the list or (ii) positioning adversaries to the preferred candidate at the bottom of the list, (iii) disguise adversaries among alike-sounding 'technical' candidates, or even (iv) include verbal or visual advertising in favour of a preferred candidate. This can be prevented by previewing the ballot by a commission formed by a balanced set of representatives – either by a random selection of citizens (applying the randomocracy / sortive democracy design) or from a diverse pool of civil society organisations and political parties. An extra preventive mechanism is the advance publishing of the ballot allowing sufficient time to correct any discrepancies.

A manipulated ballot for i-voting in a poll, survey, plebiscite or referendum could (i) contain an ambivalent or a twofold question confusing or misleading a voter or (ii) consist of a set-up sequence of questions with an implicit opinion or emotion – thereby channelling a voter's choice towards a desired option. This can also be mitigated by an advance publication, discussion, and correction of the ballot. In sum, public transparency and civic oversight mechanisms can prevent i-voting abuse at the early stages of ballot approval.

A more subtle manipulation can be performed by framing a voting issue in mass media discourse. This is especially dangerous when most popular media in the country or a community are dominated by a single individual or a group of tycoons. In this case, free access to the Internet is a solution, as the Internet can provide access to online media, low-cost in creation and diverse in content.

2. Biased polarisation *versus* deliberative connection

The realm of public opinion is populated by numerous challenges: the existence of filter bubbles, preselection effect, confirmation bias, group polarisation, fake news, and distorted social reality. The initial challenge is that "the world of social media tends to create small, deeply polarised groups of individuals who will tend to believe everything they hear, no matter how divorced from reality."[2] People living inside a filter bubble do not receive news challenging their own and their social groups' rigid views. Furthermore, people affected by confirmation bias seek out only information they agree with, not an independent verification of that information. Fake news exploit preselection and confirmation bias as the characteristic features of filter bubbles that tend to polarises social groups.[3] As people have inherent cognitive biases and tend to unite into social groups with shared beliefs, these phenomena are part of traditional politics and therefore not a problem *per se*. However, when these processes are amplified by online spaces, this becomes problematic indeed.

Under such circumstances, the principal solution is purposeful facilitation of a supportive setting for the diversity of views, a critical approach to presented information, and an intelligent discussion. First, it is relevant to nurture individual proactivity in searching for alternative information, critically evaluating the source and content of information, and creating the habit of forming a personal independent opinion based on multiple sources and critical reflection. Second, it is reasonable to encourage and support the culture of dispute. Scholars suggest a number of

[1] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[2] Hull, G. 2019. Social Media Is Not Good for Democracy. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 100-104. New York: Greenhaven Publishing.
[3] Hull, G. 2019. Social Media Is Not Good for Democracy. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 100-104. New York: Greenhaven Publishing.

possible corrections for online discussion forums and chats, websites and blogs: moderation, editorial decisions, public scrutiny, signing a user agreement recognising discussion norms, and guidelines toward depolarisation with the penalty of being removed in case of violating the norms of cooperative and non-polarised discourse.[4] To identify potential deviations, they propose to apply cognitive mapping software, automated text analysis, and sentiment analysis to show the direction of deliberation.

Such interventions are based on the assumption that deliberation-oriented norms and practices are able to reverse polarisation trends and promote informed opinion formation, profound deliberation, and more diverse consensus webs. For this aim, possible depolarising measures include: (1) creating a safe space for identity thinning and superordinate identity formation; (2) promoting offline social interactions and structures with de-polarisation rules decreasing online polarisation; (3) introducing cooperative and negotiated frames to decrease negative language and increase conciliatory language; (4) building connections and links among people who share concerns but seek peace rather than violence thus creating and maintaining depolarising norms.[5] Thereby, the normative structure of an online discussion space will nudge towards voicing different opinions, engaging in intelligent disputes, and establishing multiple connections with discussant thus constituting a more complex and interconnected web of individuals with similar viewpoints.

3. Public opinion manipulation *versus* online media regulation

Beyond the emergent imbalances at the stage of forming, public opinion can be deliberately distorted by online media. The big data of user profiles provides sufficient information for micro-targeting individual voters with personalised messages and thereby influencing their behaviour in the way not possible by conventional media. For example, an automated analysis of people's Facebook likes was able to identify their demographic information and basic political beliefs and was used for microtargeting specific voters in the United States.[6]

While traditional mass media advertisement is a standard practice of political campaigning, micro-targeting is equivocal in terms of integrity. The amount of information used to target a person exceeds what is used in traditional media and the readers or viewers are not always aware of what they disclose about themselves. Also, messages about a particular politician tailored to individual voters can be inconsistent or even contradictory with each other, thereby putting a unified political platform in question. While traditional mass media messages can be seen, checked, and questioned by other viewers, micro-targeted ads are difficult to monitor and contrast. Furthermore, the algorithmic opacity of the black box of the newsfeed, search algorithm, and ad segmentation prevents watchdogs or regulators from understanding what ads are being shown to whom and when, who paid for them, how much and when.[7] In addition, a message can be reinforced in social media either by numerous posts by (semi)automated bots from fake accounts or by highly visible posts by secretly paid writers. Although some authors might sincerely support a candidate, the problem arises when such activity is stealthily coordinated or financed. This creates an illusion of a genuine independent support of a politician or a party, while in fact it is not.

These challenges require a systemic legislative, enforcement, and civic action in response. The government can impose limits, ensure disclosure, and perform enforcement on the issue: purchasers such as political parties and vendors like Facebook should be required to proactively disclose full information about a political ad in a machine-

[4] van Dijk, J.A.G.M., Hacker, K.L, & Mollov, B. 2018. Digital Media and Networking: Opportunities and Constraints for Depolarizing Political Discourse. In: van Dijk, J.A.G.M., Hacker, K.L. *Internet and Democracy in the Network Society*. Pp. 108-130. New York: Routledge.

[5] van Dijk, J.A.G.M., Hacker, K.L, & Mollov, B. 2018. Digital Media and Networking: Opportunities and Constraints for Depolarizing Political Discourse. In: van Dijk, J.A.G.M., Hacker, K.L. *Internet and Democracy in the Network Society*. Pp. 108-130. New York: Routledge.

[6] Hull, G. 2019. Social Media Is Not Good for Democracy. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 100-104. New York: Greenhaven Publishing.

[7] Howard, A., & Wonderlich, J. 2019. Social Media Sites Should Have to Disclose Political Advertising Files. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 105-112. New York: Greenhaven Publishing.

readable, open format online to the public and election regulators.[8] Sponsored political support should be explicitly stated by writers, monitored by social media platform vendors, and punished in cases of finding hidden political endorsement. For instance, Facebook is already identifying and deleting accounts displaying signs of coordinated inauthentic behaviour. Moreover, government activity should be accompanied by shareholder activism, media coverage, policy white papers on the issue, and public pressure.[9]

4. Technical system malfunctioning *versus* reliable system functioning

The usual concern associated with voting using digital means relates to possible technical issues with the operation of the voting system, whether of hardware or software character. It might be an incorrect code leading to errors in vote casting or counting, a system overload, or an equipment crash. In the worst case, "small mistakes in the implementation and configuration of web applications can result in total compromise."[10] Indeed, such risk does exist because digital voting systems are centralised. Nevertheless, it can be mitigated by performing tests with maximum workload and against multiple risks.

Another related problem can be credited to the human factor. Whereas "poorly trained administrators can inadvertently create errors that swiftly erode public trust."[11] It should be noted that this challenge is not specifically attributed to electronic voting, but can occur during any voting campaign. To prevent errors in human-computer interaction during e-voting, electoral management must trust and understand the voting technology, that is ensured through rigorous evaluation processes and effective training strategies.[12] The authors also recommend that external service providers, both private and public, must comply with laws and requirements, that is assured by the risk assessment of external service providers' potential associations and dependencies.

Furthermore, the Council of Europe's guidelines on e-voting are extremely relevant in this respect. In particular, they emphasise technical and organisational measures for preserving data even in the case of a breakdown, regular checks of system functioning and availability for users, storing e-voting equipment in a secure area, having backup arrangements, a disaster recovery plan, and a contingency procedure, the procedure for installing updates and corrections in the system, and handling cryptographic material securely.[13]

5. Malicious hacking *versus* cyber security and integrity

Probably, most often concerns with i-voting are associated with cyber security risks. Hacking threats can emerge within the society where i-voting takes place, within the authorities administering i-voting, come from cybercriminals of another country, or a hostile foreign government. Regarding attacks from within the society, it should be noted that remote offline voting has similar risks – for example, with absentee voting, mail voting, vote count etc. Due to using servers accessible from the Internet to allow vote casting online, i-voting is indeed more exposed to foreign attacks, be they private or state-orchestrated. Thus, "governments willing to invest high level of resources into attacking any internet platform could aim these resources at internet voting, with the goal of either actually changing the outcome of an election or undermining public confidence in the outcome of the election."[14] Similar to

---

[8] Howard, A., & Wonderlich, J. 2019. Social Media Sites Should Have to Disclose Political Advertising Files. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 105-112. New York: Greenhaven Publishing.

[9] Howard, A., & Wonderlich, J. 2019. Social Media Sites Should Have to Disclose Political Advertising Files. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 105-112. New York: Greenhaven Publishing.

[10] Halderman, J.A. 2017. Practical Attacks on Real-World E-Voting. In: Hao, F., & Ryan, P.Y.A. (eds.) *Real-world Electronic Voting: Design Analysis and Deployment*. Pp. 143-170. London: CRC Press.

[11] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.

[12] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.

[13] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.

[14] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.

counteracting corrupt voting in remote offline voting the solution to mitigating cyber security risks of online voting is developing better security mechanisms. Prior to launching i-voting, the technical system should undergo evaluation and certification. Council of Europe recommends that "an independent and competent body shall evaluate the compliance of the e-voting system and of any information and communication technology (ICT) component with the technical requirements" in the form of formal certification or other appropriate control.[15]

There are multiple ways in which an i-voting system can be hacked. For example, "anyone may attempt to tamper (*malicious code*) or officials may inadvertently enable others to tamper with the voting process (*Trojan horse* attacks)."[16] In one case study "researchers showed that a man-in-the-middle attacker could exploit the vulnerabilities in the Australian iVote system to inject vote-stealing code… including compromising insecure Wi-Fi access points, poisoning ISP DNS caches, attacking vulnerable routers, and hijacking BGP prefixes."[17] They also reported that the electoral commission modified the iVote server configuration the next day. In another vivid example "during i-election trials to Washington DC the testing team performed a number of attacks and demonstrated that criminals could steal secrets, change past votes, change future votes, compromise the secret ballot, introduce a postponed stealth effect."[18] These vulnerabilities are reportedly simple to fix in retrospect. Thereby, some system issues are technical and can be repaired. For this purpose, 'white hat' ethical hackers (who identify security weaknesses aiming to fix them and prevent to be abused by villains) can be hired (in a 'bug bounty') to challenge the system, identify its vulnerabilities, and help improve its cyber security.

At the level of system architecture, several solutions can also be introduced. In this respect, the National Institute of Standards and Technology (NIST) Cybersecurity Framework provides several recommendations to mitigate hacking risks: perform thorough threat modelling, develop risk management plan and cyber security strategy, use cryptographic protections (for data transfer and data at rest), advance cryptographic voting techniques, use dedicated and trusted hardware (such as an e-ID card), employ end-point security scanning (to verify that a piece of e-voting software has not been altered), pre-configurable booting environment or virtualisation technology (to thwart malicious software) and secondary communication channels (such as the Estonian QR code that allows voters to verify their vote with an alternate device).[19] A good model of cyber security is the Estonian i-voting system using the protected ID card and the possibility to verify one's own vote. Reportedly, "there is no evidence that Estonian internet voting has been compromised."[20] Also, a coordinated but decentralised i-voting system is a good solution for damage control in case of partial system malfunction or attack.[21]

Alternatively, an attacker may decode and publish sensitive information, such as voter data, posing electoral commissions the dilemma of cancelling an election or announcing it valid but facing the disclosure of sensitive data online. Still, even this risk can be mitigated. In particular: (1) the result can be reported for subsets of voters such that the number of votes for each candidate is large enough to hide encoded information in statistical noise provided by the votes of honest voters; (2) statistics about invalid votes should be kept to a minimum and reported in aggregate form and not per voting district or other small regions; (3) further detailed statistics and information should be considered secret.[22]

---

[15] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.

[16] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[17] Halderman, J.A. 2017. Practical Attacks on Real-World E-Voting. In: Hao, F., & Ryan, P.Y.A. (eds.) *Real-world Electronic Voting: Design Analysis and Deployment*. Pp. 143-170. London: CRC Press.

[18] Halderman, J.A. 2017. Practical Attacks on Real-World E-Voting. In: Hao, F., & Ryan, P.Y.A. (eds.) *Real-world Electronic Voting: Design Analysis and Deployment*. Pp. 143-170. London: CRC Press.

[19] The National Institute of Standards and Technology. 2011. *The Security Considerations for Remote Electronic UOCAVA Voting*.

[20] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.

[21] Trechsel, A., Kucherenko, V., & Silva, Federico. 2016. *Potential and challenges of e-voting in the European Union*. EUDO Report 2016/11. Firenze: European University Institute.

[22] Wikström, D., Barrat, J., Heiberg, S., & Krimmer, R. 2017. How Could Snowden Attack an Election? In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017.* Pp. 280-291. Cham, Switzerland: Springer.

Besides technical vulnerabilities, there are human errors that can compromise the i-voting system. First of all, system administrators who have access to servers and voting software may intentionally or accidentally contribute to an attack by using infected USB flash drives or by lowering the protection of the systems.[23] To prevent such incidents, a rigorous training of election staff is advised.

Even if maximum cyber security is ensured at the level of central i-voting system, there remains the challenge of the cyber security of personal devices used for i-voting. It is estimated that "many personal computers or mobile devices used to vote online are poorly defended."[24] Technically speaking, attackers could launch denial-of-service attacks aimed at disrupting the election, try to redirect voters to fake voting sites, and conduct widespread attacks on voters' client machines, perhaps using pre-existing botnet infections.[25] And these threats are considered to be one of the most difficult and the least resolved problems in internet security. Nevertheless, a thorough system testing with maximum load and diverse cyberattacks can mitigate these risks.

Alternatively, an attacker can apply reverse Bayesian poisoning to distort voters' software. This can be performed by a denial-of-service attack on a voter's spam filters – stealthily training the voter's spam filter by sending spam mails crafted to include keywords from genuine mails from the voting system and in this way silently suppressing mails from the voting system.[26] Yet, the authors suggest that the users can mitigate the effects of reverse Bayesian poisoning by whitelisting the election email address and thus preventing the emails from being suppressed, while election officials can mitigate this attack by using alternative channels (e.g. SMS messages) to notify the users that credentials have been mailed.

Individual voters might be subject to other hacker attacks. By means of a injecting a computer virus, stealing credentials, phishing or social engineering attackers could prevent a voter from casting his or her ballot, alter a voter's choices, monitor how a voter votes, use the voter's credentials to gain access, and expand that access to damage the voting system, change election results or harm the credibility of the election results.[27] Presumably, such manipulations would not affect a large number of voters. In any case, these risks should be taken into account. One reason that voters are highly vulnerable is because "although they may be likely to notice if something goes wrong with their online banking because of money lost, the anonymity of the voting process means that it is almost impossible for them to notice if their vote has been changed."[28] However, this concern relates only to i-voting designs where voters are not able to check their votes at any time. In some IT solutions, they do possess such a possibility. Overall, considering the wide spectrum of voter-targeted manipulations, it is reasonable to launch civic education campaigns drawing attention to i-voting risks and explaining how to vote securely, advising to use advanced anti-virus software, ignore phishing requests, check their votes etc.

6. Exclusion *versus* inclusion

One concern about i-voting relates to the issue of inclusion. Taking into account the complexity of policies and the diversity of societies, it is essential to guarantee effectiveness, pluralism and fairness by mechanisms of indirect or representative democracy.[29] One consideration is that i-voting presents challenges to the eligibility requirements for

[23] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[24] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.
[25] Halderman, J.A. 2017. Practical Attacks on Real-World E-Voting. In: Hao, F., & Ryan, P.Y.A. (eds.) *Real-world Electronic Voting: Design Analysis and Deployment*. Pp. 143-170. London: CRC Press.
[26] Jonker, H., Mauw, S., & Schmitz, T. 2017. Reverse Bayesian Poisoning: How to Use Spam Filters to Manipulate Online Elections. In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017*. Pp. 183-197. Cham, Switzerland: Springer.
[27] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[28] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.
[29] Innerarity, D. 2019. *Politics in the Times of Indignation: The Crisis of Representative Democracy*. London: Bloomsbury Academic.

voting in general elections and evokes debates as to who should be entitled to vote, because many countries restrict voting in general elections to citizens who are residing in the country (either for principled considerations or for practical matters of administering the votes of citizens residing outside the country).[30] Yet, in such cases, i-voting has the emancipatory and empowering potential. First, the principle of universal suffrage guarantees the right to vote to all eligible citizens. Second, remote internet voting as an additional option to the traditional offline voting at polling stations is capable of expanding the voter base. Thereby, the introduction of i-voting can generate the debate about eligible voters, entail legislative change, and provide access to general voting for some excluded social groups, such as expatriates thus potentially making polls, consultations, referenda, and elections more inclusive.

A more contested point is the merit-based right to vote. There is an opinion that for efficient and fair democratic decisions it is not necessarily desirable to increase voters' participation in elections if doing so blurs the distinction between the voters with intense (more stable and cooperation-based) preferences and other voters (e.g., effortless voting from home via i-voting may not ultimately be desirable).[31] But such attitude contradicts the principle of equal rights and equal votes and tends to discriminate against people willing to vote online – therefore, it should be rejected for normative reasons. The cited argument is also flawed because online deliberation and collaboration are not 'effortless', but sometimes are as much or even more energy and time consuming as offline ones. Besides, an instant change of opinion can be reasonable if it is based on some new information about a prospective policy, a candidate for a public office, or a party. Even if an opinion change is not rational, but emotional, it is the right of a voter to do so. It is the responsibility of policy makers and politicians to communicate the most relevant, accurate, and persuasive information about themselves to their constituents.

Another related concern refers to the problem of digital divide. The worry is that "internet voting can enfranchise the 'haves' and make it easier for them to vote but not help the 'have nots'."[32] But the combination of online and offline options as alternatives actually bridges the divide because a voter can freely choose the most convenient and preferable voting format. In addition, there is a list of measures that can facilitate the use of i-voting. In particular, the Council of Europe recommends that: (1) the voter interface of an e-voting system is easy to understand and use by all voters; (2) the voting options on any used device are optimised for the average voter without have specialised computer knowledge; (3) voters are involved in the design of e-voting systems; (4) new IT-products are compatible with the former ones; (5) e-voting system is accessible to persons with disabilities and special needs; (6) upon request voters are supplied with special interfaces or other equivalent resources; (7) i-voting interfaces comply as much as possible with the guidelines set out in the Web Accessibility Initiative.[33] Also, for example in European countries, the digital divide is diminishing in the promising trend of an increasing digital literacy and the diffusing the use of internet-based technologies.[34]

7. Inaccurate *versus* accurate voter registers

Voter registers might be subject to manipulation. The concern is that election officials who 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 may maliciously and intentionally compromise the system or unintentionally participate in an attack via an infected machine.[35] Then corrupt voter registers may be misused to prevent certain people from voting (for example,

[30] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[31] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[32] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.
[33] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[34] Trechsel, A., Kucherenko, V., & Silva, Federico. 2016. *Potential and challenges of e-voting in the European Union*. EUDO Report 2016/11. Firenze: European University Institute.
[35] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.

identifying their political preferences according to personal statements in social media) and to exploit records of fake or dead persons (to unlawfully vote for a preferred policy, politician or a party).

These risks should be taken into account and prevented. According to the Council of Europe guidelines, "The authenticity, availability and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected."[36] There are standard technical and organisational solutions for this. In particular, "the automation and computerisation 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."[37]

At the level of system architecture, it is also possible to employ distributed ledger technologies (for instance, blockchain). Due to their peculiar design they establish a peer-to-peer network and a set of consensus algorithms for a consistent set of replicated, shared, and synchronised digital data. A voter register utilising such technology will be much more difficult to modify, although this will require to decentralise access to the register among several entities (public agencies) and familiarise system administrations with this elaborate technology. Besides, such system might be overloaded by a large number of records and requests, so it requires rigorous testing with maximum load.

8. Misidentification *versus* identification reliability

In an uncontrolled environment of a remote internet voting there is a risk that some eligible voters will not be allowed to vote while some fake voters (semi- or fully automated bots or real persons misusing stolen or fake credentials) will vote although they have no right to do so. The concern is that in internet voting "it would be difficult, if not impossible, to ascertain that a particular vote was cast by the person entitled to do so and not by an interloper."[38] In the worst-case scenario a critical number of thereby misidentified voters may artificially 'boost' a particular policy option at an e-consultation poll, binding e-referendum, or elect to a public office a preferred candidate at an e-election.

This can be safeguarded by introducing several stages of reliable identification that combined will minimise misidentification risks. For example, Estonian residents possess digital identities and the "combination of a 'hard' token (the identity card) and a 'soft' token (the PIN number) provides security that verifies that the person logging into the system is, in fact, the correct person."[39] Hypothetically, a person may waive his or her digital identity for money. But that would be similar to giving away one's passport that can be used to take a bank loan or register a business. Such risks are too high for a person to commit. Yet, there are preventive measures even for such cases of digital identity abuse. A voter would be required to take a digital photo in front of camera immediately before casting a ballot – the photo would be compared to a benchmark voter's photo taken for a government-issued ID. Such arguments in favour of a stricter identification "are often framed as a trade-off between the accessibility of the voting process to voters and the need for greater security against fraud in the voting process."[40]

[36] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[37] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[38] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[39] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.
[40] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.

9. Voting disclosure, pressure, and buying *versus* voting secrecy, freedom, and integrity

Remote i-voting raises the challenge of ensuring the secrecy of a vote. Supposedly, "i-voting potentially compromises ballot secrecy."[41] However, multiple technological and organisational mechanisms are designed to ensure the secrecy of an i-vote. According to the Council of Europe guidelines e-voting (1) shall ensure that the secrecy of the vote is respected at all stages of the voting procedure; (2) voter register data should be clearly separated from voting components; (3) an e-voting system and any authorised party shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify or otherwise gain knowledge of this data; (4) an e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties; (5) the voter should be informed of possible risks to remote e-voting secrecy and recommended means to reduce them ahead of voting; (6) the voter should be informed on how to delete, where it is possible, traces of the vote from the device used to cast the vote remotely; (7) the e-voting process shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter; (8) voter information should be separated from the voter's decision at a pre-defined stage of the counting process; (9) any decoding required for the counting of the votes should be carried out as soon as practicable after the closure of the voting period.[42] Despite such measures, voters may intentionally violate voting secrecy and take photos of the cast ballots. But this can occur in offline and online voting alike. As noted, "countries should also be wary of enabling voters to send selfies from within the polling booth."[43] Thereby, legal restrictions respectively enforced in practice and demonstrated by showcases should stop such practice.

The complexity of technical solutions faces certain critique. For example, the consideration is that enabling the voter ahead of time to define a code known only to the voter that will signify the meaning of the vote (e.g. when voting 'A' means 'B') would fail in complex voting systems and, at the most simplistic level, a voter may not remember the code when voting.[44] Still, a voter may also forget a list number or confuse the name of a candidate or a policy if there are similar to the genuine 'disguising' options on the ballot list. Cognitive risks seem similar in online and offline voting and should be treated and mitigated in any case. Thus, offline elections may have technical failures too, yet they are conducted despite these concerns for normative reasons of maintaining democracy.

The challenge of e-voting secrecy bears extra risks. As it is impossible to guarantee that nobody is watching voters casting their ballots, this opens the door to voter coercion.[45] Yet, this problem does have a solution. To meet the challenge that a coercer may stand next to the voter during casting a vote, the United States allow the voter to cast multiple votes with only the last one counted.[46] Indeed, the right to unlimited changes of a ballot until the end of election period safeguards against an immediate threat to a voter as it is possible to vote as instructed and change the vote later. The objection is that "this does not solve the problem since the pressure to change a vote may influence the voter at the last minute before the ballot closes."[47] However, the intention to abuse i-voting massively would require too many 'controllers' to stand near voters at the end of an i-voting period, which would make this pressure technique not feasible at a large scale.

Moreover, election bodies can keep the backup option of an offline voting at a polling station. Thereby, a person will be able to vote offline even after the online voting period. A counterargument to this measure is that allowing the

[41] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.
[42] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[43] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[44] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[45] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.
[46] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[47] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

voter to change the vote in a controlled environment such as the polling station is not a solution to this vulnerability in the integrity of the process, because "the coerced person may be too frightened to go to the polling station."[48] Albeit, a person can be frightened and take a photo of the vote even at offline elections. Reportedly, "Historical studies of incidents in which ballots were cast in the open in the United States reveal that voters were often subject to harassment and even abduction or murder if they did not cast their votes according to the desires of coercers. Even absent explicit coercion, voters might have abstained from the vote altogether to avoid harassment for expressing their opinions."[49] To shield voters from this, there should be a hotline for reporting such instances and a professional law enforcement system capable of handling such cases. In terms of strategy, one simulation demonstrated that it is in the interest of a society not to adapt to the expected strategy of the coercer, but to announce its anti-coercion policy openly as a rational coercer will be forced to refrain from coercion.[50]

Even if a person casting a ballot is the one entitled to vote and there is no immediate threat, the person might not have a genuine intention to do so. Voters may feel the pressure to conform to peers' expectations, may be willing to do so because a single vote does not usually determine election results, they may be subject to family and tribal pressures – these pressures would not be effective in the setting of a secret vote at a polling station.[51] But, as long as people discuss their preferences before the voting period, peer, family, and tribal pressures may exist in offline elections too. These risks exist regardless of voting technology applied and can be mitigated by encouraging an open and intelligent public discussion. Actually, with a mobile i-voting technology it would be difficult to exert constant pressure, since a person is able to find time and place when and where nobody is around and i-vote in privacy.

Even if there is no external pressure, vote buying can happen. Reportedly, "The loss of secrecy may lead to bribery and a market for votes. We have evidence from both the United States and Britain that buying votes became unattractive only when there was no external mechanism to guarantee that a vote was indeed cast the way the voter declared it was."[52] This relates to previously mentioned solutions of the possibility of altering vote and voting offline after casting a vote online. The most critical perspective assumes that currently no technology can efficiently mitigate vote buying.[53] This is a complex socio-political problem that may occur at offline and online elections alike and should be addressed by awareness raising combined with law enforcement measures.

10. Routine voting and absenteeism *versus* value-based deliberate voting

Further critique of i-voting challenges its value for civic action. Presumably, internet voting may "affect the way a ballot is cast by making the act more akin to a 'Like' than a deliberative act of public engagement," may "increase the weight voters place on private interests as distinguished from communal objectives," eliminate the value and motivation to "being 'seen' by their neighbours, friends, peers and family as active and engaged citizens," and even "lead to a decrease in the rate of voting, despite the advantages of ease and low cost."[54] However, before voting online people may invest considerable amount of time, attention, and energy in studying policies in question or political candidates on the ballot. Then the act of casting a vote on the Internet will have a lot of value. Furthermore, people can post photos near voting devices or with notifications "vote casted," keeping the vote secret. Actually, digital technologies

[48] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[49] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[50] Jamroga, W., & Tabatabaei, M. 2016. Preventing Coercion in E-Voting: Be Open and Commit. In: Krimmer, R. et al (eds.) *Electronic Voting: First International Joint Conference, E-Vote-ID 2016*. Pp. 1-17. Cham, Switzerland: Springer.
[51] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[52] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[53] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[54] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

make it easier to demonstrate civic action. While the emphasis on private or common interests and the inclination to vote or abstain is a generic motivation and supposedly should not depend on the voting technology.

Another concern relates to the symbolic value of the vote casting act. The contemplations are that "making the act of voting as casual as channel-surfing on the sofa eliminates the ceremonial nature of elections," "voting becomes as mundane as pressing the button of a remote control device, not a defining communal moment in the life of a nation," voters no longer "enact their citizenship through the ritual of gathering with their fellow citizens at the polling booth" lacking the transformation of "the collective of individual people into the sovereign people body."[55] On the contrary, i-voting may give birth to new rituals, such as posting in social media with common hashtags and thereby connecting with fellow citizens. Further, the importance of voting depends not on distance, but on values. They can be enhanced by civic education and awareness-raising.

11. Corrupt vote storage and counting *versus* verifiability and accountability

I-voting results may be distorted at the vote recording and counting stage. Thereby, the Council of Europe has set up a list of guidelines ensuring valid e-voting results. The recommendations state that measures should be taken to ensure that (1) only the appropriate number of votes per voter is cast, stored in the electronic ballot box and included in the election result; (2) if a voter is allowed to cast an electronic vote multiple times, then only one vote is counted; (3) if a voter is allowed to cast a vote by more than one voting channel, then only one vote is counted; (4) in all other cases – a voter does not cast more than one vote; (5) in all cases – the voter is clearly informed about the voting possibilities that are offered and about the rules for the counting of votes.[56]

To ensure valid results, i-voting systems aim to introduce possibilities of verifiability. In particular, end-to-end (E2E) verifiability means that "voters and possibly external auditors should be able to check whether the published election result is correct, i.e., corresponds to the votes cast by the voters, even if voting devices and servers have programming errors or are outright malicious."[57] The authors further specify that an individual verifiability is achieved when a sender can verify if the message has reached its destination, but cannot determine if this is true for the other voters, while universal verifiability guarantees that it is possible to publicly verify that the tallying of the ballots is correct. The prospective is that "an end-to-end verifiable voting (E2EVV) system would eliminate electoral fraud by enabling voters to verify not only that their vote is cast as intended, but also correctly recorded and counted."[58]

For example, even Estonian secure i-voting system can be susceptible to an attack targeting election results. To illustrate this, one proof-of-concept malware demonstrated the possibility to either change or block a vote without the voter noticing it. In response, two advanced verification mechanism have been developed: (1) an independent mobile computing device that downloads the vote cryptogram from the storage server and brute forces it using the encryption random seed, obtained from the voter's computer via a QR code; (2) a server-hosted software that generates the verification code for the voter.[59] The protocol introduces stronger security, requiring at least two parties to collaborate maliciously to break the verification or privacy properties.

To ensure secure storage of voting data and secure vote counting, it may be useful to employ advanced e-voting technologies. One of them, blockchain, is an open distributed ledger resistant to data modification due to a cryptographic data recording requiring a peer-to-peer network consensus to alter data. Another voting system is *Prêt*

[55] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[56] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[57] Küsters, R., & Müller, J. 2017. Cryptographic Security Analysis of E-voting Systems: Achievements, Misconceptions, and Limitations. In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017*. Pp. 21-41. Cham, Switzerland: Springer.
[58] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.
[59] Kubjas, I., Pikma, T., & Willemson, J. 2017. Estonian Voting Verification Mechanism Revisited Again. In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017*. Pp. 306-317. Cham, Switzerland: Springer.

à Voter that uses randomised and cryptographically encoded candidate list. It simultaneously enables an automatic instant calculation of election results, allows a voter to check an individual vote, and protects vote secrecy. Both blockchain and *Prêt à Voter* solutions "ensure that no single party is able to control, delete, or modify all data and thereby distort voting results."[60] Yet, there remains the risk that blockchain technology "does not protect information as it travels on the Internet and does not make servers and infrastructure more resistant to advanced persistent threats."[61] Taking this into account, an i-voting system trial on smaller scale or for non-binding voting would be a reasonable solution.

In addition to establishing a cyber-secure i-voting system and enabling the function of end-to-end verifiability, it is reasonable to perform electoral management bodies-led and civil society-led audit by default. The rationale is that complex i-voting manipulations may be able to disguise the fact of distorting voting data. Thus, the simulation of Australian i-elections showed that using the MOV-based manipulation and minimising first preference changes an attacker can avoid an automatic recount and successfully change the winner of elections with high confidence.[62] Therefore, the authors warrant rigorous risk limiting audits of elections. Ideally, such audits should cover the full dataset of votes. Specifically, "a ballot comparison audit requires independently counting all computer ballots, not just the sample, to check whether election computers added up the totals correctly."[63]

Comprehensive standards are set up by the Council of Europe. In particular, they require that (1) the e-voting system shall be auditable; (2) the audit system shall be open and comprehensive, and actively report on potential issues and threats; (3) the audit system should record times, events and actions; (4) automated tools and system procedures should enable the data to be analysed and reported on in a fast and accurate manner, thus enabling rapid corrective action; (5) the audit system should provide verifiable reports on cross-checks of data, system or network attacks, intrusion detection and reporting, data manipulation, fraud and fraud attempts; (6) the e-voting system should maintain reliable synchronised time sources; (7) the accuracy of the time source should be sufficient to maintain time marks for audit trails and observation data, as well as for maintaining the time limits for registration, nomination, voting or counting; (8) the conclusions drawn from the audit process should be considered in future e-elections.[64]

Besides verifiability, i-voting system should possess accountability. Accountability not only allows one to verify whether a desired property is guaranteed, for example, that the election outcome is correct, but also ensures that misbehaving parties can be identified if this is not the case.[65] The authors explain that accountability strengthens the incentive of all parties to follow their roles because they can be singled out in case they misbehave and then might face, for example, severe financial or legal penalties, or lose their reputation.

12. Voting campaign discreditation *versus* legitimacy and trust

Regardless whether an i-voting hacking attempts occurred or not, it is essential that a community or a society agrees that an i-voting was performed properly thereby affirming its legitimacy. It is not enough that the elections meet the requirements of universal, equal, free and secret suffrage *de facto*, but for democracy to exist, voters must believe that these requirements have been met and there must be no question of the propriety of the voting processes

[60] Khutkyy, D. 2020. E-voting in Ukraine: Advancements, Challenges and Perspectives. *Brussels Ukraïna Review, April*, 11-13.
[61] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[62] Blom, M., Stuckey, P.J., & Teague, V.J. 2019. Election Manipulation with Partial Information. In: Krimmer, R. et al (eds.) *Electronic Voting: Fourth International Joint Conference, E-Vote-ID 2019*. Pp. 32-49. Cham, Switzerland: Springer.
[63] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[64] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[65] Küsters, R., & Müller, J. 2017. Cryptographic Security Analysis of E-voting Systems: Achievements, Misconceptions, and Limitations. In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017*. Pp 21-41. Cham, Switzerland: Springer.

among voters.[66] This is especially critical for the initial i-voting. Whereas "a negative first experience – or a poorly handled vulnerability exposure – can turn electoral stakeholders against technology, and trust then becomes difficult to regain."[67] Manipulated voting can harm not only attitudes towards a particular voting technology, but towards democracy itself. Thus, large-scale electoral fraud has the potential to undermine trust in democracy.[68]

In this respect, regular transparency-based communication activities are vital for maintaining trusting attitude of the public. When in 2017 a critical vulnerability was identified in Estonian ID card system, national authorities adopted a policy of maximum transparency about the impact of the vulnerability and the actions that were taken to mitigate it – this policy was successful due to public trust in the authorities and relatively small population.[69]

Recommendations on this matter are as follows: (1) states shall be transparent in all aspects of e-voting; (2) the competent electoral authorities should publish an official list of the software used in an e-election; (3) public access to the components of the e-voting system and information thereon, in particular documentation, source code and non-disclosure agreements, should be disclosed to the stakeholders and the public at large, well in advance of the election period; (4) deployment of electronic voting technologies should include the development of comprehensive, detailed, step-by-step guidelines including a procedural manual; (5) the components of the e-voting system shall be disclosed for verification and certification purposes; (6) e-voting systems should generate reliable and sufficiently detailed observation data so that election observation can be carried out; (7) it should be possible to reliably determine the time at which an event generated observation data; (8) the authenticity, availability and integrity of the data should be maintained; (9) domestic and international observers should have access to all relevant documentation on e-voting processes, to the testing of the software and hardware, and to the evaluation and certification process.[70]

Public opinion of the general public is sensitive with regard to framing the discussion about the voting format. For instance, it was discovered that in the United States priming voters with voting fraud considerations causes them to become more supportive of paper-based alternatives to touchscreen voting machines; and, conversely, priming them with convenience considerations causes them to display higher preference for e-voting relative to paper-based alternatives; the exposure to fraud/convenience considerations causes significant deviations from voters' tendency to prefer systems they are already familiar with.[71] Therefore, the discussion about paper, on-site electronic, or remote internet voting should be well-balanced and objective.

The attitudes of politicians and professionals knowledgeable about the technology and policy of i-voting are also important for establishing credibility of internet voting. In particular, it is reasonable to involve scholars, civic activists, and policy makers at the early stages of developing an i-voting policy, empower the experts with decision-making capabilities, and clearly communicate how their input was taken into account. During the voting period, publishing an open code of an i-voting software, providing instant results, and being open for civic audit can increase trust too. Besides, it is important to explain technical, political, and social aspects of i-voting to journalists and opinion leaders and to illustrate this information with concise infographics and video showcases. The support of political elites in the setting of political neutrality will also facilitate the transition to i-voting.[72]

---

[66] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[67] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.

[68] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.

[69] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.

[70] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.

[71] Alvarez, R.M., Levin, I., & Li, Y. 2018. Fraud, Convenience, and E-voting: How Voting Experience Shapes Opinions about Voting Technology. *Journal of Information Technology & Politics, 15, 1*, 94-105, DOI: 10.1080/19331681.2018.1460288

[72] Trechsel, A., Kucherenko, V., & Silva, Federico. 2016. *Potential and challenges of e-voting in the European Union*. EUDO Report 2016/11. Firenze: European University Institute.

Conclusions

As this analysis has proved, i-voting does bear multiple risks, but they can be remitted. For each particular issue revealed by scholars and practitioners one or several corresponding solutions have been developed. Therefore, if the introduction of i-voting has been decided, it is a matter of performing diligent risk mitigation.

Numerous challenges are associated with the technical side of the voting system hardware and software – malfunctioning, hacking, compromising voter registers, voter misidentification, vote disclosure, corrupt ballot storage and counting. Yet, advanced cyber security solutions and organisational measures should be sufficient to safeguard i-voting system. Given the complexity of internet voting system, efforts to protect and to hack it might look like an everlasting 'arms race.' Nevertheless, attracting 'white hat' ethical hackers to challenge and improve the system should give voting management bodies an extra advantage. In any case, some countries have demonstrated a high level of system reliability in real-life i-voting.

Further potential abuses relate to particular 'political' techniques of influencing voting design, voting administrators, and voters. These include issue framing, online media discourse bias, voter exclusion, voter pressure, and vote buying. They require systematic preventive measures along the lines of legislative action, public transparency, civic oversight, law enforcement, and public accountability. Since governments possess ultimate authority reinforced with an active civil society, together they have the powers necessary to implement the required counter-abuse measures.

And, finally, some biases and manipulations affect individual voters in particular and the public in general thus being of 'social' character. These refer to group polarisation, social reality distortion, group pressure, voting routine, absenteeism, and campaign discreditation. These challenges require deliberate advance activities aiming to create a connecting discussion space, launch civic education, awareness raising, and mobilisation campaigns, supplemented by expert discussions and transparency-based communication with the public. This is probably the most difficult action area, because it depends on changing individual attitudes and transforming the overall public opinion. Nevertheless, societal shifts do happen, although usually gradually.

The scope of i-voting proliferation can be illustrated by its specific application for i-elections of public officials. As official i-elections for public offices are binding, authorise winners with power, and pave the way to direct influencing politics and policy, they are 'high-stake' endeavours. Since the early binding i-elections back in 2003, some countries have tried and already abandoned i-elections, mainly for cyber security concerns. And although these cases have been widely discussed mostly in the light of encountered problem, some of these countries actually consider re-introducing i-elections. Moreover, the number of countries practising i-elections, despite being modest in absolute numbers, is definitely bigger than the number of countries that have abandoned them. Even more countries consider introducing i-elections in the future and their numbers are growing. Their governments learn from predecessors, perform feasibility studies, adopt evidence-based policies, test advanced blockchain and *Prêt à Voter* systems, perform pilots, and launch discussions with experts and the public. And although it takes years, considering the long-term inclusive, temporal, financial, and reputational benefits, i-voting is a worthy undertaking.

Appendices

Table 1: Countries that previously used, but have abandoned politically-binding i-voting in elections of public officials (2 as of May 2020)

Source: Unless specified otherwise – IDEA. 2020. ICTS in Elections Database. URL: https://www.idea.int/data-tools/data/icts-elections

Country	Years practised	i-Voting scale	Eligible i-voters	Reasons for official discontinuing
Netherlands	2004 2004 2006[73]	Subnational European Union National	Voters in particular constituencies (Rijnland) Out-of-country voters Out-of-country voters	2008: Cyber security concerns pointed out by civic activists and internalised by the government[74]
Norway	2011 2013	Subnational National	Voters in particular constituencies (10 municipalities) Voters in particular constituencies (12 municipalities)	2014: Government concerns about cyber security and the impact on turnout[75]

Table 2: Countries that previously used, have abandoned, but are considering re-introduction of politically-binding i-voting in elections of public officials (2 as of May 2020)

Source: Unless specified otherwise – IDEA. 2020. ICTS in Elections Database. URL: https://www.idea.int/data-tools/data/icts-elections

Country	Years practised	i-Voting scale	Eligible i-voters	Status
Switzerland (practice)[76]	2003-2018 2008-2018	Subnational National	Voters in particular constituencies (up to 13 cantons) Voters from abroad (from particular constituencies – up to 13 cantons)	2019: Reason for discontinuing – political controversy over cyber security issues[78]
Switzerland (trial)[77]	2019	National	Some voters in particular constituencies, Voters from abroad	2019: Trials of an i-voting system were approved

[73] Caarls, S. 2010. *E-Voting Handbook: Key Steps in the Implementation of E-Enabled Elections*. Strasbourg: Council of Europe.
[74] Loeber, L. 2014. *E-voting in the Netherlands; past, current, future?* Conference Paper. October. URL: https://www.researchgate.net/publication/301547849_E-voting_in_the_Netherlands_past_current_future
[75] Trechsel, A., Kucherenko, V., & Silva, Federico. 2016. *Potential and challenges of e-voting in the European Union*. EUDO Report 2016/11. Firenze: European University Institute.
[76] Germann, M., & Serdült, U. 2014. Internet Voting for Expatriates: The Swiss Case. *JeDEM: eJournal of eDemocracy and Open Government, 6, 2,* 197-215. DOI: https://doi.org/10.29379/jedem.v6i2.302
[77] Geiser, U. 2019. E-voting suffers another setback amid expat Swiss concerns. *SWI: Swissinfo.ch*. 27 June. URL: https://www.swissinfo.ch/eng/digital-democracy_e-voting-suffers-another-setback-amid-expat-swiss-concerns/45059918
[78] Geiser, U. 2019. E-voting suffers another setback amid expat Swiss concerns. *SWI: Swissinfo.ch*. 27 June. URL: https://www.swissinfo.ch/eng/digital-democracy_e-voting-suffers-another-setback-amid-expat-swiss-concerns/45059918

Country	Years practised	i-Voting scale	Eligible i-voters	Status
France (practice)[79]	2012-2016	National	Voters from abroad	2017: Reason for discontinuing – cyber security concerns
France (trial)[80]	2020	Subnational	Voters from abroad	2020: Non-binding tests of an internet voting platform have been performed

Table 3: Countries that currently use politically-binding i-voting in elections of public officials (at least 6 as of May 2020)

Source: Unless specified otherwise – IDEA. 2020. ICTS in Elections Database. URL: https://www.idea.int/data-tools/data/icts-elections

Country	Years practised	i-Voting scale	Eligible i-voters	Features
Armenia[81]	2012, 2013 2017, 2018	National National	Diplomatic staff and their families, voters from abroad Diplomatic staff and their families, voters from abroad, military voters	Election results are stored in log files potentially susceptible to the risk of abuse
Australia	2007[82] 2011–current[83]	National Subnational	Military voters Voters in particular constituencies (New South Wales and Western Australia)	I-elections have demonstrated: reasonable costs; desirability (including the capacity to maintain vote secrecy) and the effect on voter behaviour; confidence in the electoral system[84]
Canada	2003–current[85]	Subnational	Voters in particular constituencies (Ontario and Nova Scotia)	The number and type of credentials (e.g. PIN, date of birth, security question, and advance registration with multiple credentials) vary; reported technical and security issues were

[79] Leigh, T. 2017. France drops electronic voting for citizens abroad over cybersecurity fears. *Reuters*. 6 March. URL: https://www.reuters.com/article/us-france-election-cyber/france-drops-electronic-voting-for-citizens-abroad-over-cybersecurity-fears-idUSKBN16D233

[80] The French Ministry for Europe and Foreign Affairs. 2020. French citizens abroad – Approval of electronic voting for consular elections. 15 January. URL: https://www.diplomatie.gouv.fr/en/the-ministry-and-its-network/news/2020/article/french-citizens-abroad-approval-of-electronic-voting-for-consular-elections-15

[81] Manougian, H. 2020. Did You Know Armenia Allows Internet Voting? (But It's only for Some). *EVN Report*. 13 February. URL: https://www.evnreport.com/politics/did-you-know-armenia-allows-internet-voting-but-it-s-only-for-some

[82] Lundie, R. 2016. Electronic voting at federal elections. *Parliament of Australia.* URL: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook45p/ElectronicVoting

[83] Goodman, N., & Smith, R. 2016. Internet Voting in Sub-national Elections: Policy Learning. In: Krimmer, R. et al (eds.) *Electronic Voting: First International Joint Conference, E-Vote-ID 2016*. Pp. 164-177. Cham, Switzerland: Springer.

[84] Lundie, R. 2016. Electronic voting at federal elections. *Parliament of Australia.* URL: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook45p/ElectronicVoting

[85] Government of Canada. 2017. Online Voting: A Path Forward for Federal Elections. January. URL: https://www.canada.ca/en/democratic-institutions/services/reports/online-voting-path-forward-federal-elections.html#toc21

Country	Years practised	i-Voting scale	Eligible i-voters	Features
				limited; voters report positive experiences[86]
Estonia	2009, 2014, 2019 2006, 2007, 2011, 2015, 2016, 2019 2005, 2009, 2013, 2017[87]	European Union National Subnational	All voters	I-voting is offered for seven days before paper voting on the Election Day; the 'recorded as cast' verification is applied; i-voting is politically neutral and does not bias election results; there is a high degree of confidence (trust) in the system and procedures[88]
Panama	2014, 2018[89]	National, subnational	Voters from abroad	Voters need a valid identity card to vote[90]
United States	2016–current	National, subnational	Voters from abroad, military voters, voters in particular constituencies (over 30 states)[91]	Specific technological solutions vary across states; experts point out cyber security concerns[92]

Table 4: Countries that consider introducing politically-binding i-voting in elections of public officials (at least 17 as of May 2020)

Source: Unless specified otherwise – IDEA. 2020. ICTS in Elections Database. URL: https://www.idea.int/data-tools/data/icts-elections

Country	Years studied, experimented, or developed	i-Voting scale	Eligible i-voters	Status
Austria	2004	National	All voters	A feasibility study has been conducted[93]
Haiti	2017	National	All voters	A feasibility study has been conducted [94]

[86] Goodman, N., & Smith, R. 2016. Internet Voting in Sub-national Elections: Policy Learning. In: Krimmer, R. et al (eds.) *Electronic Voting: First International Joint Conference, E-Vote-ID 2016*. Pp. 164-177. Cham, Switzerland: Springer.
[87] Valisimed. 2020. Toimunud valimiste arhiiv. URL: https://www.valimised.ee/et/toimunud-valimiste-arhiiv
[88] Vinkel, P., & Krimmer, R. 2016. The How and Why to Internet Voting an Attempt to Explain E-Stonia. In: Krimmer, R. et al (eds.) *Electronic Voting: First International Joint Conference, E-Vote-ID 2016*. Pp. 178-191. Cham, Switzerland: Springer.
[89] Tribunal Electoral. 2020. Elecciones Generales 1994-2019. URL: https://www.tribunal-electoral.gob.pa/eventos-electorales/elecciones-generales-1994-2019/
[90] Fierro, C.N. et. al. 2016. *Electoral Studies in Compared International Perspective. Voting from Abroad in 18 Latin American Countries*. México, Mexico: National Electoral Institute. URL: http://www.undp.org/content/dam/undp/library/Democratic%20Governance/Electoral%20Systems%20and%20Processes/Voting%20from%20Abroad%20in%2018%20Latin%20American%20Countries%20web%20version%20ENG.pdf
[91] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[92] Parks, M. 2019. In 2020, Some Americans Will Vote on Their Phones. Is That the Future? *NPR*. 7 November. URL: https://www.npr.org/2019/11/07/776403310/in-2020-some-americans-will-vote-on-their-phones-is-that-the-future?t=1588522064124
[93] Bundesministerium Inneres. 2020. Wahlen. Wahlrecht in Österreich, Überblick. URL: https://www.bmi.gv.at/412/start.aspx
[94] Chéry, P.M. 2017. *Analysis of the Feasibility of Electronic Voting in Haiti. Working paper.* 17 February. Copenhagen Consensus Center. URL: http://www.copenhagenconsensus.com/sites/default/files/electronic_voting_chery.pdf

Country	Years studied, experimented, or developed	i-Voting scale	Eligible i-voters	Status
Iceland	2014	Subnational	Voters in particular constituencies (Reykjavik city)	A feasibility study has been conducted[95]
India[96]	2010-2011	Subnational	Voters in particular constituencies	A trial of binding i-voting has been performed[97]
Finland[98]	2016-2017	National, subnational	All voters	A feasibility study has been conducted
Mexico	2012 2016	Subnational National, subnational	Voters from abroad Voters from abroad	A trial of binding i-voting has been performed[99] Formal guidelines have been developed[100]
Moldova	2016	National	All voters	A feasibility study has been conducted and a roadmap has been developed[101]
New Zealand[102]	2016, 2019	Subnational	Voters in particular constituencies	Trials of binding i-voting have been initiated
Pakistan	2019	National	Voters from abroad	Small-scale trials of an internet voting system have been performed[103]
Portugal	2005	National	Voters from abroad	An experiment of non-binding i-voting has been carried out[104]
Russia[105]	2019	Subnational	Voters in particular constituencies (Moscow city)	A trial of binding i-voting using a private blockchain system has been performed

[95] Island.is. 2020. Overview of the proposed solution. URL: https://vefur.island.is/media/pdf-skjol-a-island.is-2014/RegistersIceland-evoting.pdf

[96] Election Commission of India. 2020. Digital Inclusion for citizens in India for democracy. URL: https://eci.gov.in/divisions-of-eci/ict-apps/

[97] Scytl. 2020. State of Gujarat India. Internet voting for municipal elections. URL: https://www.parliament.uk/documents/speaker/digital-democracy/GUJARATINDIA.pdf

[98] Vaalit Val. 2020. Electronic voting in Finland. URL: https://vaalit.fi/en/electronic-voting1

[99] Munive, E.-Y. 2012. Mexican experience of e-voting. *Diplo Internet Governance Community.* 13 July. URL: http://www.diplointernetgovernance.org/profiles/blogs/mexican-experience-of-e-voting

[100] SEGOB. 2016. Acuerdo. *SEGOB*. 1 December. URL: https://www.dof.gob.mx/nota_detalle.php?codigo=5463327&fecha=01/12/2016

[101] Republica Moldova. Comisa Electorala Centrala. 2016. *Feasibility study on Internet Voting for the Central Electoral Commission of the Republic of Moldova. Report and Preliminary Roadmap*. Chisinau, Moldova: Republica Moldova. Comisa Electorala Centrala. URL: https://www.undp.org/content/dam/moldova/docs/Publications/MD-IVOTE-FS-and-Roadmap_cleanENG.pdf

[102] Molineaux, J. 2019. *Solving and creating problems: Online voting in New Zealand*. January. Auckland, New Zealand: Auckland University of Technology. URL: https://thepolicyobservatory.aut.ac.nz/__data/assets/pdf_file/0003/302538/Solving-and-creating-problems-online-voting-in-New-Zealand.pdf

[103] Haq, H.B., McDermott, R., & Ali, S.T. 2019. *Pakistan's Internet Voting Experiment*. July. URL: https://www.researchgate.net/publication/334558559_Pakistan%27s_Internet_Voting_Experiment

[104] Comissão Nacional de Eleições. 2020. Voto electrónico. URL: http://www.cne.pt/content/voto-electronico

[105] Официальный сайт Мэра Москвы. 2020. Электронные выборы в Московскую городскую Думу. *Официальный сайт Мэра Москвы*. URL: https://www.mos.ru/city/projects/blockchain-vybory/

Country	Years studied, experimented, or developed	i-Voting scale	Eligible i-voters	Status
Sierra Leone	2018	Subnational	Voters in particular constituencies	A full-cycle blockchain-based i-voting system started to be developed[106]
Spain	2018 2003	National Subnational	All voters Voters from abroad from particular constituencies (Catalonia)	A feasibility study has been conducted[107] A pilot of non-binding i-voting has been carried out
Turkey	2011	National	All voters	A *Prêt à Voter* i-voting system has been analysed in a feasibility study[108]
Ukraine	2018 2019	National National	Voters from abroad Voters from abroad	An experiment of non-binding i-voting using a blockchain-based system has been carried out[109] Relevant legislature started to be drafted[110]
United Arab Emirates	2011	National	All voters	Trials of non-binding i-voting system have been performed[111]
United Kingdom	2002, 2003, 2007	Subnational	Voters in particular constituencies (6 councils)[112]	Pilots of binding i-voting have been performed[113]

[106] E&T editorial staff. 2018. Blockchain technology deployed in Sierra Leonean election. *E&T*. 16 March. URL: https://eandt.theiet.org/content/articles/2018/03/blockchain-technology-deployed-in-sierra-leonean-election/
[107] Riera, A. & Cervelló, G. 2013. *Experimentation on Secure Internet Voting in Spain*. URL: https://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-10.pdf
[108] Adalier, O. et. al. 2011. A Case Study for Turkey: A Secure Paper-Based Electronic Voting System. *International Journal of eBusiness and eGovernment Studies, 3, 1*. URL: https://dergipark.org.tr/en/download/article-file/257068
[109] Suberg, W. 2018. Ukraine Electoral Commission Uses NEM Blockchain for Voting Trial. *Cointelegraph*. 8 August. URL: https://cointelegraph.com/news/ukraine-electoral-commission-uses-nem-blockchain-for-voting-trial
[110] Шишацкий, Е. & Юрасов, С. 2019. Большое интервью с Михаилом Федоровым. *Ліга.Tech*. 5 August. URL: https://tech.liga.net/technology/interview/didjital-strateg-zelenskogo-za-kajdym-reestrom-est-smotryaschiy-ot-kriminala
[111] ICA. 2020. E-Voting UAE: A Case Study. URL: https://www.ica.gov.ae/userfiles/EVoting_UAE_%20A%20Case%20Study.pdf
[112] Barry, C. et. at. 2002. *eVolution not revolution. Electronic Voting Status Report 2*. September. URL: https://www.vec.vic.gov.au/files/RP-EvolutionNotRevolution.pdf
[113] Kobie, N. 2015. Why electronic voting isn't secure – but may be safe enough. *The Guardian*. 30 March. URL: https://www.theguardian.com/technology/2015/mar/30/why-electronic-voting-is-not-secure