RISK ASSESSMENT AND FEASIBILITY STUDY ON ALTERNATIVE FORMS OF VOTING IN POST-WAR ELECTIONS IN UKRAINE WITH A FOCUS ON INTERNET VOTING

Ardita Driza Maurer, Véronique Cortier, Oksana Kulyk,
Armin Rabitsch, Volodymyr Venher, Olivier Pereira

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

RISK ASSESSMENT AND FEASIBILITY STUDY ON ALTERNATIVE FORMS OF VOTING IN POST-WAR ELECTIONS IN UKRAINE WITH A FOCUS ON INTERNET VOTING

Authors
Ardita Driza Maurer (lead author), Véronique Cortier, Oksana Kulyk, Armin Rabitsch and Volodymyr Venher

Contributor
Olivier Pereira

Council of Europe

Ukrainian version:
«Оцінка ризиків та можливості використання альтернативних форм голосування на післявоєнних виборах в Україні з фокусом на інтернет-голосуванні»

The study was developed within the framework and with the support of the Council of Europe project "Supporting democratic post-war elections in Ukraine" within the framework of the Council of Europe Action Plan for Ukraine "Resilience, Recovery and Reconstruction" 2023 – 2026.

Cover design, design and layout:
Hanna Voina
Photo: ©shutterstock

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

About the authors

Ardita Driza Maurer is a jurist based in Switzerland, focusing on electoral law and digital technologies used in elections. She led the experts' groups that drafted the Council of Europe guidelines on the use of information and communication technology in electoral processes in Council of Europe member states (2022) and Recommendation CM/Rec(2017)5 on standards for e-voting. She works as an independent expert for international organisations, national EMBs and other institutions on issues of legal regulation of e-voting and of other e-backed solutions.

Véronique Cortier is an academic (CNRS) researcher at the LORIA laboratory (Nancy, France). Her research interests include formal definitions, proofs and design of security protocols, in particular e-voting protocols. She is co-designer of the Belenios voting protocol and voting platform and she is involved in several research collaborations with voting companies and state organisations. For example, she acted as third party for verifying the French legislative elections in 2022 and 2023.

Oksana Kulyk is an associate professor at the IT University of Copenhagen. Her research focuses on the human and social factors of cybersecurity and privacy, investigating the effects of human behaviour and human errors on security-critical systems, and issues of trust and transparency of cybersecurity assurances in such systems. Her particular focus is on the security of election technologies, in particular internet voting.

Armin Rabitsch is an election expert and chairperson of Election-Watch.EU, a non-partisan election observer organisation. Election-Watch.EU conducted election assessment missions of the European Parliament elections in 2019 and 2024 covering all the 27 EU member states. He works as an adviser for the European institutions and is the author of several reference documents on elections, human rights and artificial intelligence.

Volodymyr Venher is an associate professor at the Department of Jurisprudence and Public Law at the National University of Kyiv-Mohyla Academy. He conducts comprehensive research on implementing the rule of law and human rights standards in Ukrainian legal practice. He acts as a national expert for a number of Council of Europe projects and is currently working on legal issues for the Organisation and on holding free and fair elections in post-war Ukraine.

Olivier Pereira is a professor at UCLouvain in Belgium. His research explores the design and analysis of cryptographic protocols that offer advanced verifiability and privacy features. He contributed to the design of several free and verifiable voting systems that have been deployed in private and public elections, including Helios, STAR-Vote and ElectionGuard, and to the analysis of several other systems, including the Swiss and Estonian internet voting systems. He has provided consultation on election technologies for government institutions of various countries, including Belgium, France, Switzerland and the USA, and for other public international organisations.

Contents

Abbreviations

CEC	Central Election Commission
EMB	Election management body
E2EV	End-to-end verifiability/verification
IDPs	Internally displaced persons
OCV	Out-of-country voting
OCVs	Out-of-country voters
SVR	State Voter Register

Summary

The study focuses on the questions of the feasibility and risks of internet voting for OCV during the first post-war elections from a legal and technical perspective.

Legally, the design of a system for voting abroad depends on the particular circumstances of a country, including its administrative infrastructure, budget constraints, in-country election arrangements and level of public confidence. Each country should find a balance between secure and universal suffrage, knowing that elections abroad should generally meet the same standards for democratic elections as in-country procedures. Experience from countries like Estonia and Switzerland shows that detailed regulation on internet voting introduced by government agencies has grown complex. Several legal questions subsist, including those related to threats to anonymity and secrecy and to addressing coercion, the faith put in the experts versus the public, control over the election and the difficulty of obtaining evidence. Other questions relate to the level of i-voting regulation (whether contained in the constitution, law or lesser forms of regulation), the level of detail of the regulation required to ensure compliance and public confidence and the appropriate checks to ensure constitutional conformity of the regulation. These and other reasons are also given by legal and scientific investigations or court decisions in several countries, both with and without previous experience of i-voting, which have concluded that internet voting is not an option for the time being for larger-scale political elections.

If online voting is to be considered in terms of a long-term perspective, in addition to technical aspects, focus should be placed on legal challenges such as that of introducing constitutional changes to allow for early voting, voting other than on paper, voting from an unsupervised environment (addressing secrecy, coercion, etc.); drawing up detailed, clear (to make implementation possible) and constitutionally compliant regulation of i-voting which integrates end-to-end verifiability mechanisms; updating criminal law as well as election dispute resolution mechanisms to account for i-voting-related violations and claims; discussing trust assumptions of internet voting, on which security relies, with decision makers; reflecting on the fact that internet voting so far has been developed to encompass voting from a personal computer and not from a mobile phone; building human capacities and knowledge at all levels, including at the Election Management Body (EMB) level and the electorate; and discussing the specific risks of introducing i-voting in Ukraine.

Technically, post-war elections in Ukraine must be defended from a large variety of risks, the sum of which seems to be much higher than that faced in most other countries. Ukraine needs a strongly verifiable system, with cast-as-intended, recorded-as-cast, tallied-as-recorded and eligibility verifiability, that also provides vote-buying resistance. Unfortunately, no deployed system satisfies all these constraints together at the moment. Furthermore, the specific situation in Ukraine may prevent countries or companies from allowing their systems be used in such a hostile context. Conducting online voting elections within a short time frame would thus be unfeasible, given the security requirements and present threats outlined in Part II of this study.

If online voting is to be considered in terms of a long-term perspective, in addition to legal aspects, focus should be placed on technical challenges such as that of developing a reliable public digital infrastructure; conducting a thorough security analysis of the electoral processes; investing in independent servers and independent tallying authorities (requiring independent machines and independent software) as well as in creating reliable channels between voters and the authorities (such as physical postal addresses, e-mail addresses, phone numbers); promoting transparency and involving independent experts; establishing processes for voter support, including the transparent handling of complaints; introducing processes such as digital access to the voting register or use of technology to secure postal voting and a general digital identity infrastructure, to improve paper-based election processes and help voters familiarise themselves with the use of technology in elections. Technology could also be used (first) to improve the security of voting by postal mail by supporting the recorded-as-cast and the tallied-as-recorded verifiability properties or to deploy super-

vised mobile voting kiosks, which would offer strong guarantees about the identity of voters and would support the free expression of the vote in a voting booth. Such uses of technology could be arguably simpler than internet voting. However, more research and piloting is needed.

Mandate and methodology

A. Context

The full-scale armed Russian aggression against Ukraine in 2022 led to tremendous and unprecedented consequences for the lives, economy and infrastructure of Ukrainian people, including challenges in terms of the democratic processes that will be needed in a post-war period, to a degree not seen in decades on the continent.

Following the opinion on Ukraine's application for membership of the European Union and the candidate status granted to Ukraine on 23 June 2022, as well as the decision of the European Council on the opening of the European Union accession negotiations with Ukraine in December 2023, further progress and fulfilment of the commitments related to functioning of democratic institutions will be necessary for Ukraine to become a member of the EU.

Within the framework of the Council of Europe Action Plan for Ukraine – Resilience, Recovery and Reconstruction 2023-2026 – the Council of Europe, among others, provides its support to the Ukrainian authorities and civil society for post-war elections to be held in line with European electoral standards, with the electoral rights of Ukrainian citizens being duly ensured. For this purpose, a democratic environment should be in place in order for everyone to enjoy their electoral rights fully and freely. As specified in the needs assessment report "Organisation and holding of elections in post-war Ukraine – Prerequisites for and challenges", commissioned by the Council of Europe in May 2022 and updated in 2023[1], large-scale displacement of Ukrainians within and beyond the country, massive destruction of civilian infrastructure, post-war security threats and the need for the development and implementation of a transitional justice policy will pose significant challenges for organising and conducting the first post-war democratic elections.

Ukrainian population

The last census in Ukraine was conducted in 2001. Therefore, even official data on the number of people who lived in Ukraine before the full-scale invasion on 24 February 2022 may vary. According to government estimates, 37.3 million people lived in Ukraine (excluding the temporarily occupied territories) as of 1 December 2019.[2] As of 1 February 2022, the State Statistics Service of Ukraine estimated the existing population (without taking into account the temporarily occupied Autonomous Republic of Crimea) to be 41 130 432.[3] According to World Bank data,[4] the population of Ukraine has continued to decrease since 2014: from 45.2 million people to 43.8 million in 2021 and to 38 million in 2022.

Ukrainian nationals residing abroad

The Ministry of Foreign Affairs of Ukraine reported that there were 8 177 000 Ukrainians abroad as of 21 June 2023.[5] Almost 63% of Ukrainians abroad are adults and 22% are children under 18. The age of the other 15% of people is not specified. It should be mentioned that only one out of 16 Ukrainians abroad is

1. See the Needs assessment report "Organisation and holding of elections in post-war Ukraine – Prerequisites for and challenges" in Ukrainian: https://rm.coe.int/ua-2023-elections-needs-assessment-2777-2271-8729-1/1680ae9b59, in English: https://rm.coe.int/en-organisation-and-holding-of-elections-in-post-war-ukraine/1680aedbaf
2. https://www.pravda.com.ua/news/2020/01/23/7238191/
3. http://db.ukrcensus.gov.ua/PXWEB2007/eng/news/op_popul_e.asp
4. https://data.worldbank.org/indicator/SP.POP.TOTL?end=2022&locations=UA&start=2014
5. Reported by the Civil Network OPORA: https://www.oporaua.org/en/viyna/24791-kilkist-ukrayintsiv-ta-yikh-migratsiia-za-kordon-cherez-viinu-doslidzhennia-gromadianskoyi-merezhi-opora-24791

registered with a Ukrainian consulate abroad: as of 21 June 2023, there were slightly more than 493 000 such citizens, 88% of which were adults. According to the last UNHCR update, 6 196 600 Ukrainian refugees were recorded globally as of 23 August 2023, of which 5 829 600 Ukrainian refugees were recorded in Europe and 367 000 outside Europe.[6] Most Ukrainians have registered for temporary protection or similar national protection schemes in Europe. Around one fifth of Ukrainian nationals are thus living abroad, the majority of them being refugees who fled after the full-scale armed Russian aggression in February 2022, most of them having registered for temporary protection or a similar status in European countries.

Internally displaced persons in Ukraine

According to information from the Ministry of Social Policy of Ukraine,[7] some 5 million Ukrainians have been registered as internally displaced persons (IDPs) since 24 February 2022. It should be noted that not all IDPs are registered and therefore official statistics may not fully reflect the real situation. According to Iryna Vereshchuk, Deputy Prime Minister of Ukraine and Minister for the Reintegration of Temporarily Occupied Territories of Ukraine (holding the post from November 2021 to September 2024), there are approximately 2 million unregistered IDPs. More than a million people have been internally displaced twice since 2014:[8] first after the occupation of the Autonomous Republic of Crimea and certain parts of the Luhansk and Donetsk regions in 2014, and then after the full-scale invasion on 24 February 2022.

First post-war elections[9]

In this context, the Ukrainian authorities, namely the Parliamentary Committee on state building, local governance, regional and urban development (the Parliamentary Committee) and the Central Election Commission (CEC), are now considering different options to ensure the electoral rights of a huge number of displaced Ukrainian voters, both abroad and inside Ukraine, after the end of the war. The constitution prohibits the holding of elections under martial law and the Ukrainian authorities have clarified that no elections can be organised under martial law.

In March 2023, the CEC created three working groups to deal with three sets of questions, namely on holding elections abroad, on updating the national electoral register and on organisational challenges. Their findings and recommendations are expected to be presented to parliament. The EU Parliament, together with IDEA International, organised a meeting (30-31 May 2023)[10] on out-of-country voting and on specific international support for Ukraine for its first post-war elections once martial law is lifted. It recommended that countries continue to support Ukraine with expertise and assistance and that the Ukrainian authorities hold inclusive Parliamentary Committee hearings and adopt the necessary legal framework to allow for adequate preparation for post-war elections, thus avoiding the need to take hasty decisions that may undermine security and trust in the results and ensuring that candidates and voters are well aware of changes to the rules and procedures.

B. Mandate

The Parliamentary Committee requested the Council of Europe to prepare a risk assessment and feasibility study on the possible introduction of "institutes of e-democracy", particularly e-voting and e-counting, as well as other alternative forms of voting for post-war elections in Ukraine.[11] The focus should be on the risk and feasibility of internet voting in the context of post-war elections in Ukraine and the implications for the repartition of responsibilities between different institutions potentially involved in organising and conducting internet voting and counting.

6. The source is the collation of statistics made available to the UNHCR by national authorities of different countries. See the UNHCR operational data portal: https://data.unhcr.org/en/situations/ukraine
7. https://www.msp.gov.ua/timeline/Vnutrishno-peremishcheni-osobi.html; https://www.msp.gov.ua/news/23014.html
8. https://zn.ua/ukr/ECONOMICS/dopomoha-vpo-chomu-pereselentsi-ne-otrimali-viplati-na-pochatku-misjatsja.html
9. The regular elections for the Verkhovna Rada were scheduled for 29 October 2023; regular elections for the President of Ukraine were scheduled on the last Sunday of March 2024; and regular local elections for the last Sunday of October 2025.
10. https://www.idea.int/news/european-parliamentary-dialogue-ukraine-calls-support-voting-rights-countrys-war-displaced
11. A letter of request, No. 04-23/13-2023/57821 of 21 March 2023, was sent to the Council of Europe project "Supporting democratic post-war elections in Ukraine", implemented within the framework of the Council of Europe Action Plan for Ukraine "Resilience, Recovery and Reconstruction" 2023-2026.

The Parliamentary Committee identified the following objectives for the study: to conduct a feasibility study and risk assessment via inclusive consultations with all electoral stakeholders concerned; to gauge public perception of the different types of alternative forms of voting for post-war elections in Ukraine; to facilitate further inclusive and transparent dialogue among national electoral stakeholders on the possible application of alternative forms of voting in post-war elections in Ukraine; to provide consultancy and expert support on the matter as needed and requested by the relevant Ukrainian authorities.

C. Organisation and structure

Based on the mandate and discussions with Ukrainian counterparts, the present study focuses on the assessment of risks, desirability and feasibility of piloting i-voting in post-war elections. The study focuses primarily on nationals residing abroad, also referred to as out-of-country voters (OCVs), and on the national elections to take place immediately after the war. In the long term, it may also concern voters within Ukraine. The general conclusions and recommendations should assist the Parliamentary Committee when considering the piloting of i-voting in general, not only for OCVs or the first post-war elections.

The study investigates the feasibility and risks of introducing i-voting in post-war elections in Ukraine from two viewpoints, namely the legal and organisational perspective (Part I) and the technical perspective (Part II), including an assessment of the risks and security. The study involved deskwork and online interviews and exchanges with the deputy Chair, chair of the profile sub-committee on elections, referendums and other forms of direct democracy of the Ukrainian Parliamentary Committee on state building, local governance, regional and urban development; with the chair of the sub-committee on e-democracy of the Ukrainian Parliamentary Committee on digital transformation; with CEC members and the CEC Secretariat; and with representatives of the International Foundation for Electoral Systems in Ukraine (IFES Ukraine) and the Civil Network OPORA, as well as online discussions among experts. Its conclusions and recommendations are based on the legal and factual situation in Ukraine, on legal recommendations from the Council of Europe, the European Commission for Democracy through Law (Venice Commission) and the OSCE/ODIHR, on state-of-the-art academic technical expertise and on lessons learned from similar experiences in other countries. Conclusions rely on consensus among all the experts involved.

D. Terminology

A few concepts related to internet voting are explained below. For further definitions one can refer to the glossaries that accompany the two relevant Council of Europe instruments, namely Appendix II of Recommendation CM/Rec(2017)5 on standards for e-voting and the glossary in the Committee of Ministers Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member states.

E-voting

The mandate uses the term "e-voting" (electronic voting) to refer to internet voting, or "i-voting", including the process of e-counting of internet votes. Recommendation CM/Rec(2017)5 contains a more detailed definition of "e-voting", which is the use of electronic means to cast and/or count the vote. In this definition, "e-voting" covers voting machines in polling stations, use of scanners to count paper ballots and the use of the internet to vote from a remote location, outside the control of electoral authorities (from home) or the use of the internet to vote from a remote location under the control of electoral authorities (kiosk voting). In this study, e-voting and i-voting are used as synonyms.

E2EV

End-to-end verifiability involves all the following verifiability steps: cast-as-intended, recorded-as-cast, tallied-as-recorded and eligibility verifiability. These verifications develop the concept of a chain of trust in e-enabled elections. They do not prevent potential manipulation of the vote but may allow verification that the vote and the overall result have not been tempered with.

- **Cast-as-intended:** the voter shall be able to verify that his or her intention is accurately represented in the vote.

- **Recorded-as-cast:** the voter shall be able to verify that the sealed vote has entered the electronic ballot box without being altered; any undue influence that has modified the vote shall be detectable by the voter.
- **Tallied-as-recorded:** the system should provide sound evidence that each authentic vote is accurately included in the respective election results and such evidence should be verifiable by means that are independent from the e-voting system.
- **Eligibility verifiability:** the system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system.

Individual verifiability: cast-as-intended and recorded-as-cast are also known as individual verifiability.

Universal verifiability: tallied-as-recorded and eligibility verifiability are also known as universal verifiability.

Part I

LEGAL PERSPECTIVE

This part answers the main research question about the legal feasibility of internet voting for non-resident Ukrainian nationals, or OCVs, in the first post-war elections. It also looks at the feasibility of other alternative voting methods for OCVs.

First, some of the main characteristics of the Ukrainian electoral legal framework will be considered. Second, the focus will be on voters' rights and more specifically on the rights of OCVs. International standards and good practice on effective OCVs registration and on effective voting channels for OCVs will be discussed and compared to the existing regulation and practice in Ukraine. Third, and the main theme of this part, the legal feasibility of introducing a new voting channel – an internet voting channel – will be discussed. This part will present international legal standards and some examples of advanced national regulation for internet voting, namely the Estonian and Swiss models. Drawing from international legal standards, it will introduce the main legal requirements that should apply to internet voting and will consider their impact, namely how Ukrainian legislation needs to adapt before experiments with internet voting can begin (the modification of existing laws/regulations and/or the introduction of new ones). Such international legal requirements are the minimum requirements and apply to all instances of internet voting with binding results for political elections, including small-scale pilot schemes. This part will finish by presenting some conclusions. It should be noted that general conclusions on the legal feasibility of internet voting are not limited to OCV or to the first post-war elections but apply to the use of internet voting for political elections in general.

A. Ukrainian electoral framework

The regulation of elections in Ukraine has a long and varied history. Parliamentary and local elections have frequently been governed by legislation which has been modified shortly before the election. At times, such changes were minor; however, in some cases the electoral system underwent a virtually complete transformation. The adoption of the Electoral Code of Ukraine in 2019 aimed not only to systematise national electoral legislation but also to prevent frequent and chaotic alterations. However, substantial changes were again introduced just before the regular local elections in 2020. Changes in electoral legislation cause a lack of stability if they are relatively frequent and introduced shortly before each election. International good practice recommends that electoral reforms should be carried out and completed sufficiently in advance of elections. Fundamental aspects should not be changed within one year of elections.[12] Adjustments to election procedures introduced shortly before elections, even if construed as a remedy for severe or extraordinary situations, must not generate other problems that might detract from, rather than contribute to, the integrity of an election.[13] Understanding this is critically important when envisaging future regulatory developments and implementation of new electoral institutions, such as remote voting in general and internet voting in particular.

1. National and local elections

The Electoral Code of Ukraine lays down provisions for presidential, parliamentary and local elections. The President of Ukraine is elected through a first-past-the-post absolute majority-based system: if none of the candidates secures a majority of votes, a second round is scheduled (Articles 127 and 128 of the Electoral

12. Section II.2.b of the Venice Commission Code of Good Practice in Electoral Matters stipulates that "the fundamental elements of electoral law, in particular the electoral system proper, membership of electoral commissions and the drawing of constituency boundaries, should not be open to amendment less than one year before an election". Paragraph 110 of the Venice Commission's Reflections on the Respect for Democracy, Human Rights and the Rule of Law during States of Emergency notes that "Making a change [to] the election code as regards voting modalities less than one year before elections may possibly be in accordance with the Code of Good Practice in Electoral Matters if it is necessary for, or contributes to, fair elections".

13. OSCE/ODIHR, Alternative voting methods and arrangements, Warsaw, 12 October 2020, p. 8.

Code). Elections to the Verkhovna Rada of Ukraine (Parliament of Ukraine) are carried out based on the principles of a proportional system under single electoral lists of candidates for MPs in a nationwide constituency, which are used to form regional electoral lists of candidates (hereinafter referred to as "nationwide electoral lists" and "regional electoral lists") from political parties (Article 133.1 of the Electoral Code). Local elections are addressed in Article 192 of the Electoral Code. The detailed rules for the nomination of candidates and territorial constituencies are to be found in Appendix A.

2. Voting procedure

Ukrainian legislation provides only for the possibility of personal voting by the voter through the completion of a paper ballot. Counting is also conducted manually at polling stations.

Voting shall be held on the voting day from 8 a.m. until 8 p.m. without any breaks. Voting at foreign election precincts shall be held according to the local time of the country where such precincts are established. The voting procedure at the polling station and in the voters' place of residence is regulated in detail by the Electoral Code of Ukraine (Articles 113-119, 168-174, 240-249). Certain aspects are detailed further in CEC resolutions. For example, the requirements for polling station premises and their equipment with the necessary inventory are regulated separately by the CEC. Any voter who for health reasons (disability, a temporary health disorder or age) cannot complete the voting ballot personally shall have the right, after notifying the chairperson or another member of the precinct election commission, to be assisted by another voter and not by any members of the election commission, candidates or their proxies and official observers.

Detailed rules for voting and counting as well as the distribution of mandates are in Appendix B.

B. Rights and obligations of different groups of voters

1. Resident voters

Ukraine's electoral legislation regulates electoral rights in a manner largely in keeping with countries with a continental legal system, akin to many other nations in eastern Europe.

1.1. Registration

For local elections, the right to vote is determined by the affiliation of a voter with a respective territory, which is determined by their electoral address. Typically, the electoral address aligns with the registered place of official residence. However, the Law of Ukraine on the State Register of Voters was amended in 2019 to ensure the rights of internally displaced persons, allowing voters to freely change their electoral address. Such changes can be made by any voter, at their discretion, without additional justification for such a need, through the submission of a written statement by the voter or even electronically through the official voters portal. Relevant procedures are limited during the state of war.

Unlike IDPs, Ukrainian nationals residing abroad, including those forced to leave after 24 February 2022, have no right to temporarily change their electoral address. Offering them such a right is currently being discussed. If approved, such a change will impact the organisation of registers and other processes. It would be necessary to establish a date up until which such changes are permitted to allow enough time for the administration to complete its work, according to the Civil Network OPORA.

1.2. Right to vote and to elect

Citizens who are aged 18 or older on the day of elections or referendums and who have not been declared legally incapacitated by a court possess the right to vote (Article 70, sections 1 and 2 of the Constitution of Ukraine). A voter exercises their right to vote in elections based on their inclusion on the voter list at an election precinct. Voters' lists are compiled separately for each election. The administration of the State Register of Voters (SRV) is regulated by the Law on the State Register of Voters and the Electoral Code of Ukraine. The SRV serves as the basis for the formation of voter lists.

1.3. Right to stand for election

Candidates are presented by parties or are self-nominated. The voter can only choose from among those candidates presented on a list. The detailed rules are explained in Appendix C.

1.4. Resident voters' obligations

These are relatively few and procedural. Voting is a right not an obligation for the citizens of Ukraine. There are no direct or indirect legal consequences for absenteeism. The general duty is to adhere to legislative regulations and show respect for electoral procedures. The primary obligation for voters is to ensure the secrecy of voting. The voting ballot must be completed by the voter personally in the booth for secret voting (with a few exceptions for health issues or age and under the conditions explained above). During the completion of the voting ballot, the presence of other persons and any form of photo or video recording are prohibited. To fulfil this duty and ensure the proper conduct of electoral procedures, a voter is only allowed to remain in the voting premises for the time necessary to cast their vote. During the vote counting process, only a limited group of individuals may be present. Legislation includes measures to prevent abuse of electoral rights and punish unlawful actions such as voter bribery, illegal influence on members of election commissions, falsification of electoral documents, etc. Legislation establishes administrative (offence) and criminal liability for violations of the secrecy of voting. Their practical application is limited, however.

2. Internally displaced persons (IDPs)

There are no special rights or duties prescribed for IDPs. Until 2019, their active electoral right was restricted, as the inability to change the electoral address (which often was in territories outside the control of the Ukrainian Government) hindered voting. Upon the adoption of the Electoral Code of Ukraine in 2019, corresponding changes were introduced, granting internally displaced persons, as well as labour migrants, students and other people who change their place of residence unofficially (without informing the relevant authorities), the right to change the electoral address (Article 119 of the Electoral Code on procedures for organising voting at voters' places of stay). This provided the full range of voter's rights in the new location.[14]

3. Non-resident nationals

This is the focus group of this study.

3.1. Right to vote and to elect

International standards and practice

Whether non-resident nationals should be given voting rights – and if they are, to what extent – is unregulated in international law.[15] While the Universal Declaration of Human Rights emphasises the right to take part in government, including through voting, as a fundamental human right, the legal framework surrounding the rights of non-resident nationals and the organisation of elections abroad for non-resident nationals varies among countries and is shaped by national laws. The European Court of Human Rights (the "Court") found in a comparative analysis of domestic law conducted in 2012 that the majority of the countries concerned authorise and have implemented procedures to allow their nationals resident abroad to vote in parliamentary elections. However, the situation varies greatly and the different scenarios do not lend themselves to classification into neat categories. Thirty-seven member states of the Council of Europe provide either for voting in polling stations abroad or postal voting, or both. Among those, 17 countries allow voting in embassies or

14. This practice is aligned with UN recommendations to allow internally displaced persons to vote in their location of displacement for their constituency of origin or their constituency of displacement. See Report of the UN Special Rapporteur on the human rights of internally displaced persons, Cecilia Jimenez-Damary, 13 April 2022, A/HRC/50/24.

15. There is one exception: Article 41 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, which enshrines voting rights of migrant workers, says "Migrant workers and members of their families shall have the right to participate in public affairs of their State of origin and to vote and to be elected at elections of that State, in accordance with its legislation". Ukraine, however, is not a signatory to this convention.

consulates or in polling stations set up elsewhere; eight allow their citizens living abroad to vote by post only, either through an embassy or consulate or by writing directly to the competent national authority; a few (at that time in 2012, the Netherlands – which has stopped doing so since – Estonia and Switzerland) allowed internet voting. In five member states of the Council of Europe only persons temporarily resident outside the country have the right to vote from abroad. In some countries, expatriates lose the right to vote after a certain period of time. Certain countries, including Ukraine, allow external voting only with the permission of the host country. In four countries expatriates may elect their own representatives to the national parliament in constituencies set up outside the country. Eight member states of the Council of Europe do not allow voting from abroad in parliamentary elections.[16]

After also considering international law and practice, in addition to national laws, the Court has reached several relevant conclusions. Restrictions on expatriate voting rights based on the criterion of residence might be justified by several factors.[17] Hence, there is no obligation to offer expatriates voting rights, although this is considered good practice.[18]

When expatriates are given the right to vote, none of the legal instruments examined by the European Court of Human Rights form a basis for concluding that, as the law currently stands, states are under an obligation to enable citizens living abroad to exercise the right to vote. In other words, Article 3 of Protocol No. 1 to the European Convention on Human Rights[19] does not impose a positive obligation on national authorities to guarantee voters abroad the right to vote from their place of residence in parliamentary elections. Each country has to balance the principle of universal suffrage on the one hand against the need for security of the ballot and considerations of a practical nature on the other.[20]

Ukrainian legal framework and practice

As discussed above (see section A., Context), around one fifth of the total population of Ukraine is reported to be living abroad, which is an important challenge to election organisation. While the Venice Commission recognises three categories of citizens abroad (those abroad on election day for personal or business reasons; those temporarily abroad, like students; and those settled abroad for a much longer duration or in a permanent manner and likely to have double nationality, also considered as voluntary migrants), Ukraine also contains a fourth important group: refugees that fled the war in 2022 or forced migrants and whose status is unclear (whether they are temporarily abroad or settled abroad for a longer duration or permanently).

With respect to their rights, according to existing legislation, OCVs can only vote for nationwide parties' lists but not for candidates on regional lists and they have no rights to vote in local elections either. An option to offer forced migrants that left after 24 February 2022 some additional rights, namely the right to vote for candidates on regional lists is not considered for the time being. The right to be elected and the right to register

16. Sitaropoulos and Giakoumopoulos v. Greece (Application no. 42202/07 [GC]), Judgment, 15 March 2012, §§ 32 ff.

17. Ibid. § 69.

18. Although the introduction of the right to vote for citizens who live abroad is not required by the principles of the European electoral heritage, the Venice Commission suggests that states, in view of citizens' European mobility, and in accordance with the particular situation of certain states, adopt a positive approach to the right to vote of citizens living abroad, since this right fosters the development of national and European citizenship. Further, the Parliamentary Assembly of the Council of Europe encourages member states to allow their citizens living abroad to participate to the fullest extent possible in the electoral process, without making it an obligation.

See the following documents.

- Council of Europe's European Commission for Democracy through Law (Venice Commission) 2002 Code of Good Practice in Electoral Matters. The code provides that "the right to vote and to be elected may be accorded to citizens residing abroad", without making it a requirement to grant such a right.
- The Venice Commission's report on out-of-country voting adopted by the Council for Democratic Elections at its 37th meeting (Venice, 16 June 2011) and by the Venice Commission at its 87th Plenary Session (Venice, 17-18 June 2011) (CDL-AD(2011)022-e).
- Parliamentary Assembly of the Council of Europe's Resolution No. 1459 (2005) and Recommendation No. 1714 (2005) on the abolition of restrictions on the right to vote; see also Recommendation No. 1410 (1999) on links between Europeans living abroad and their countries of origin.

19. Article 3 of Protocol No. 1 to the European Convention on Human Rights reads: "The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature".

20. Sitaropoulos and Giakoumopoulos v. Greece (Application no. 42202/07 [GC]), Judgment, 15 March 2012, §§ 71 ff.

a temporary voting address are discussed.[21] If respective proposals are approved upon the results of the discussions, there will likely be different categories of OCVs. It is important to clearly define the different groups of OCVs and their respective rights (for example, the right to vote for regional candidates, be assigned to local precincts, have their vote counted at the regional level, etc.).

3.2. Right to stand for election

International standards and practice

The situation is the same as for active voting rights (see above, 3.1. "Right to vote and to elect").

Ukrainian legal framework and practice

According to existing legislation, a Ukrainian citizen loses the right to stand in elections after staying abroad for more than 90 days or for more than 183 days in total for each annual period before the voting day. In the current circumstances of forced migration and war, there are proposals to offer passive voting rights to forced migrants that left after 24 February 2022 and live abroad in connection with martial law.[22] If this is accepted, there will be at least two different groups of OCVs to be distinguished. Hence, the importance of clearly defining the different groups of OCVs and their respective rights.

3.3. Registration

International standards and practice

According to the Venice Commission, one of the major problems with citizens residing abroad is that they generally stay on electoral rolls in-country. This is the case, in particular, in countries with passive voter registration. The risk is not double voting but impersonation (which is also possible in countries which do not provide for out-of-country voting). Strict identity checks are therefore carried out to avoid impersonation.

Active registration is a precondition to voting for OCVs in most cases in the Council of Europe region.[23] To avoid multiple registration, the use of a central voter register and clear separation of the OCV register are required. It might be advisable that voters are not registered in both registers, but if they opt actively for OCV registration their entry in the central voter register is crossed out but not deleted. This way, election authorities could provide information about the status of the entry in cases where a voter's name in-country cannot be found on the voter list. It would be advisable for citizens abroad whose names are not in the civil status register to either list their last residential address in-country or provide references to a certain municipality in-country. This would enable the authorities to establish a "home" municipality for such citizens abroad.

It is recommendable to provide the possibility for citizens abroad to register as an OCV for a certain limited time period (like 5 to 10 years) without having to register for each election again. Voter information should be updated any time the voter's address abroad changes.

Despite the requirement of a residential address abroad, there needs to be a clear standard applied and communicated coherently about who is entitled to be included in the OCV register in respect of time periods applied for out-of-country voter status or for being only temporarily abroad.

21. See Civil Network OPORA/ IFES Ukraine Road map, 18 October 2023. The IFES Ukraine report (2023b) argues that one specific reason for keeping forced Ukrainian migrants engaged in political processes is to increase the likelihood of eventual return to the country and that debates about what methods to use, how much to spend, etc. to enfranchise forced Ukrainian migrants are more urgent than those on enfranchising other expat voters.
22. Ibid.
23. The Court has reviewed the variety of existing administrative procedures for registration of expatriates on the electoral roll in 22 member states that allow voting from abroad. See Sitaropoulos and Giakoumopoulos v. Greece (Application no. 42202/07 [GC]), Judgment, 15 March 2012, §§ 39 ff.

The display and consultation of the voter register should be conducted in compliance with the General Data Protection Regulation (GDPR) of the European Union[24] and Council of Europe Convention 108.[25] Stricter conditions apply to qualified sensitive electoral data. Such conditions should be introduced to the regulatory electoral instruments (the Electoral Code and similar). Citizens abroad (like those in-country) would gain from being able to check their voter registration records online using a website, app or SMS service.

Ukrainian legal framework and practice

Registration with an embassy is currently a precondition for being allowed to vote as an OCV. Voters abroad are included in voter lists at special polling stations abroad. The voter lists at each election precinct are compiled based on information from the State Voter Register (SVR), which is maintained in electronic form and has a unified centralised database containing the personal data of all Ukrainian voters, including those living or temporarily staying abroad. SVR maintenance bodies update the register database once a month based on information submitted by other officials; information on OCVs is submitted to the SVR by the heads of Ukraine's foreign diplomatic institutions. The challenges in particular for OCVs that left after 24 February 2022 are numerous.[26] For the purpose of this study, it should be noted that one difficulty is the Ukrainian authorities' ability to verify the accuracy of the addresses abroad of OCVs. The possible requirement of verification of address could complicate and delay registration and disenfranchise voters. Having the correct address is important for sending voting material for both postal voting and i-voting, where a second communication channel – in addition to an internet channel – is needed to send verification information to the voter (this could be a postal channel).

According to some interlocutors,[27] as of 24 February 2022, only about 450 000 of the approximately 3 million citizens abroad were entered onto the voter list. In June 2023, around 490 000 were registered out of more than 8 million people abroad, of which more than 5 million were adults. The likely reasons for Ukrainians' reluctance to be placed on the consular register include the feeling there is no need to do so, lack of awareness of the procedure, the need to pay for consular services and unfounded fears that being placed on the consular register may lead to deportation or to the necessity to pay additional taxes in Ukraine, etc.[28] IFES suggests that registration with a consulate should not be a precondition to participation in elections.[29] The Civil Network OPORA proposes offering OCVs the possibility of temporarily changing their voting address using electronic services without the need to visit authorised bodies. Which OCVs may benefit from this remains to be seen. Again, this may lead to having different groups of OCVs which points again to the importance of clearly defining the different groups of OCVs and their respective rights.

Finding adequate solutions for updating the SVR in view of the first post-war election is an important challenge in the current situation. It is not known yet how this challenge will be addressed. Yet, the solution to be found will be important in terms of identifying voting methods for OCVs.

3.4. Is there an obligation to offer an effective voting channel?

International standards and practice

See the above Section 3.1 on the right to vote and to elect. The conclusion of the Court is that Article 3 of Protocol No. 1 to the European Convention on Human Rights does not provide for the implementation by Contracting States of measures to allow expatriates to exercise their right to vote from their place of resi-

24. The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the EU or not. See: https://gdpr.eu/companies-outside-of-europe/

25. Convention for the Protection of Individuals with regard to the Processing of Personal Data (1981), ratified by Ukraine on 6 July 2010.

26. See IFES Ukraine (2023b).

27. Interviews with representatives of Civil Network OPORA and IFES Ukraine held on 1 December 2023 and 11 December 2023 respectively.

28. See IFES Ukraine (2023a) regarding the problems with consular registration that were noted by OCVs.

29. During the interview, IFES experts proposed developing a mechanism for registering OCVs so that the un-alternative registration at the consulate would not be an obstacle for participation in the elections.

dence. This implies that non-resident citizens who are given voting rights can return to vote in the country.[30] Countries considering arrangements for external voting will have to balance universal suffrage against transparency and security during elections. The extent to which large groups can be accommodated is also a matter of cost.[31] No precise international standards exist but elections abroad should generally meet the same standards for democratic elections as in-country procedures. The design of a system for voting abroad depends on the particular circumstances of a country, including its administrative, infrastructure, budget constraints, in-country election arrangements and level of public confidence.[32]

The most common voting options for voters abroad are in-person voting and postal voting. Other methods are internet voting and voting by proxy. An overview of out-of-country voting in EU member states is provided in Appendix D.

Before drafting regulations for procedures, a thorough process of mapping the individual steps and possible scenarios of the various processes is advisable. It is also advisable to test OCV options and processes on a smaller scale, for example for a state opinion poll.[33]

Ukrainian legal framework and practice

Legislation only foresees in-person voting at premises of foreign diplomatic institutions of Ukraine. Any alternative method requires legislative changes.

Introducing other voting options for OCVs should furthermore consider several factors specific to Ukraine, including the following.

- The introduction of different modalities of voting in Ukraine and abroad may be considered by some as a violation of the principle of equality of voters. This concerns not only the legal dimension of this principle but also the organisational and societal aspects. Granting different voting conditions to those who have left Ukraine may trigger unfavourable social reactions.
- Implementing alternative voting modalities for voting abroad will require maximum support from the respective foreign governments. Currently, Ukraine cannot obtain relevant verified information about the number of Ukrainians residing in specific countries. Establishing co-operation for such a complex process as an election might be extremely challenging.
- Changing the voting model abroad requires important financial resources, which are currently unavailable in Ukraine. Even finding the necessary funds for conducting elections within Ukraine under the old model will be exceptionally challenging.

3.5. In-person voting

International standards and practice

The Venice Commission distinguishes two kinds of practical difficulties in organising out-of-country voting: organisational difficulties (for example, drawing up electoral rolls, providing election equipment or counting votes) and difficulties in guaranteeing that the election process is conducted in the proper way when methods of remote voting are used (postal vote, proxy voting or internet voting). They can be avoided by restricting the voting procedure to embassies or consulates (or possibly to a number of specially designated polling stations). However, if this is the case, universal suffrage may not be fully guaranteed because fewer voters will be able

30. In Sitaropoulos and Giakoumopoulos v. Greece [GC], 2012, the applicants complained that, in the absence of regulation on that point, they could not exercise their voting right in the country where they lived as expatriates (France) even though the constitution of their country of origin (Greece) provided for that possibility. The Court found that there had been no violation of Article 3 of Protocol No. 1 as the disruption to the applicants' financial, family and professional lives that would have been caused had they had to travel to Greece would not have been disproportionate to the point of impairing the very essence of their voting rights.
31. Venice Commission CDL-AD(2011)022, Report on out-of-country voting.
32. Venice Commission CDL-AD(2007)012, Joint opinion on the draft working text amending the election code of "The Former Yugoslav Republic of Macedonia".
33. OSCE/ODIHR, Alternative voting methods and arrangements, Warsaw, 12 October 2020, p. 8: "Changes in voting practices need to be subject to and preceded by significant research and testing to ensure their proper implementation."

to vote in practice.[34] Hence, as already mentioned, finding a balance between secure and universal suffrage is necessary.

In-person voting is the most used voting method for non-resident nationals voting abroad worldwide. It is used in 109 out of 216 countries.[35] Many countries that organise in-person voting abroad offer this option not only to those permanently abroad but also to those temporarily abroad. In most cases, voting takes place at the respective consulate or embassy, but some countries organise polling stations in other locations so as to ensure proximity to the voters and/or to accommodate a high number of voters. Alternative places include churches, schools, special post offices and, where the expatriate community is large, convention and exhibition centres or sports centres. Special polling stations can also be set up on ships and at military facilities.

Providing the right to vote in person abroad has advantages as voting can take place in a controlled environment where the electoral authorities can ensure that the secrecy of the vote is respected. It is important nevertheless to be aware of the limitations and to be prepared to control this process since it takes place abroad. Issues include addressing the number and quality of polling stations and issues of jurisdiction in resolving disputes. While regulations and operationalisation should leave no gaps, mishaps are nevertheless inevitable. This requires anticipating and mitigating risks and managing them actively.

To uphold the secrecy of the vote, it would be advisable to connect the counting of the ballots at a diplomatic representation to a certain minimum threshold (for example 100 votes cast). If the number of votes is below that threshold, the ballots would need to be transferred in a secure manner in tamper-evident envelopes and counted at central level by the CEC.

It should be noted as well that not all countries allow others to organise elections on their territory.[36] In all cases, setting up alternative voting places abroad requires specific agreements with host countries. An overview of host country agreements is included in Appendix E.

34. Venice Commission CDL-AD(2011)022, Report on out-of-country voting.

35. International IDEA: https://www.idea.int/data-tools/world-view/52

36. European Commission, DG JUSTICE (2018), Lupiáñez-Villanueva, F. and Devaux, A. Study on the Benefits and Drawbacks of Remote Voting, Brussels, 2018, p. 61.

In-person voting abroad: benefits and drawbacks[37]

Benefits for the CEC	Drawbacks for the CEC
— Voting takes place in a controlled environment, following the standard process. Secrecy is ensured because voters themselves place the vote in the ballot box. — The identity of the voter can be verified in person. — Polling booths or specific spaces to vote in private ensure the secrecy of the vote. — It can be used by people who live abroad and make the effort to travel to the diplomatic representation. — It can be observed (although this could be more complicated and resource-intensive than in-country voting observation). — There is no dependency on the postal services.	— Countries with not many diplomatic representations might face additional challenges to create OCV polling stations. — Establishing polling stations outside of diplomatic representations is logistically difficult and expensive. — It may be difficult to use for people with a disability. — If votes are counted at the polling station abroad and there are very few voters, secrecy can be at risk. — There may be problems of dual inscription, with voters being registered in the electoral lists abroad and within the country. — There may be problems in countries permitting postal voting and on-site voting with ensuring no double voting takes place. — If votes are sent to the country for counting, there is some risk that they get lost or damaged during transportation. — An advance application is often needed to use this option. — It implies some costs for the public administration, as well as organisational efforts. — Voters may not be able to use constituency-specific ballots (or may require additional organisation to deliver such ballots to the voters' location abroad).
Benefits for the voter	**Drawbacks for the voter**
— It can be used by people who live abroad and want to vote. — Voting takes place in a controlled environment, following the standard process. Secrecy is ensured because voters can vote in a polling booth and place the vote themselves in the ballot box. — There is no dependency on the postal service. — Familiar polling procedures.	— It may entail a lot of travelling for those who live abroad but without a nearby consulate. — It may be difficult to use for people with a disability. — If votes are counted at the polling station abroad and there are very few voters, secrecy can be at risk. — An advance application is often needed to use this option. — If there are very few polling stations, there may be long queues for voters. — Voters may not be able to use constituency-specific ballots (or may require additional organisation to deliver such ballots to the voters' location abroad).

37. Ibid, p.67, table adapted.

Ukrainian legal framework and practice

In-person voting at diplomatic representations

According to the existing legislation, non-resident citizens can only vote in person at Ukrainian diplomatic representations abroad. Election precincts are established by the Central Election Commission at Ukraine's diplomatic institutions abroad and military units deployed outside Ukraine. The key problem is the very limited number of such diplomatic institutions, which could not even meet the needs of past elections.[38] This will be a key obstacle in the first post-war elections. Furthermore, the practice of several recent elections shows that the burden is extremely challenging for diplomats. For voters too, voting at diplomatic institutions entails logistical difficulties. The very limited number of polling stations means that voters may have to travel quite a long distance to cast their vote.

Another key challenge here is the need to ensure a high level of security for all participants in the electoral procedures, primarily for voters. Voters should not be afraid to cast their votes in a consulate or embassy. Securing voting stations abroad requires co-operation with host countries. In some not entirely "friendly" countries, this will be particularly challenging. The alternative, selective conduct of voting only in some countries, can significantly impact the principles of equality and societal perception of the election results.

To ensure universal suffrage, interlocutors in Ukraine have recommended diversifying the voting methods for OCVs. However, to prevent multiple voting, they also suggest that OCVs should choose one preferred method among those offered and preclude the use of others. The main difficulty here is that in cases involving i-voting, a second channel should always remain available to the voter, to be used in case the voter faces issues in accessing internet voting or in case verification shows that the internet vote was compromised.

In-person voting extended beyond diplomatic representations

It is clear that election precincts established at diplomatic institutions will not provide sufficient opportunity to vote for all Ukrainian voters abroad who are willing to register and cast their vote in the first post-war elections.[39]

Hence, stakeholders like Civil Network OPORA recommend opening new precincts abroad to allow for an extension of in-person voting and creating more polling stations beyond diplomatic representations. This option faces several challenges though, currently being discussed in Ukraine. It does not require changes in the constitution but requires prior arrangements with local authorities in foreign countries, in addition to introducing specific regulation for this new option. Another challenge relates to sufficient funding for this costly activity. According to the electoral legislation, the organisation and conduct of elections must be funded only from the state budget of Ukraine. Therefore, even if funds are received from foreign partners, such funds must be contributed to the state budget. It is also being discussed if and how the administrative and criminal law of Ukraine can apply to these out-of-country voting premises outside consulates to address potential violations of voting rights that might occur and how this aspect can be covered by the necessary agreements with hosting countries.[40] One difficulty is the fact that most municipalities where such new precincts could be established, unlike big cities, are not experienced in handling requests of foreign EMBs to hold out-of-country voting. In addition, some countries are wary of the possibility of opening extra-territorial election precincts in their territory, especially if they themselves do not accord voting rights to their own expats.[41]

The staffing of the election commissions, that is, the necessity of involving a large number of Ukrainian citizens in the work of the election commissions and their information and training, is an additional challenge.

38. IFES Ukraine (2023b) states that until February 2022, Ukrainian diplomatic institutions were deployed in 119 countries worldwide. Out of those, 102 were approved as precincts allowed to organise out-of-country voting.

39. See conclusions in IFES Ukraine (2023a). Also, see a recent study by researchers at Lviv University which found that 82% of those OCVs currently living in Poland said they would like to participate in the first post-war elections. The study also calculated that the existing polling stations can cater for a maximum of 250 000 OCVs, provided they open from 8 a.m. to 8 p.m. on election day. The situation was already difficult in the past. See, for example, the IFES Ukraine (2023b): p.55 and CEC Regulation of 27 September 2022 No. 102 "On proposals to improve the legislation of Ukraine, aimed at ensuring the preparation and holding of elections after the termination or abolition of martial law in Ukraine". Although participation of OCVs before the war was very low (some 15% of 3 million out-of-country Ukrainians registered to vote and only between 7% and 12% of them effectively voted in the 2019 elections), there were still long queues outside Ukrainian embassies in Prague, Warsaw, London, Brussels and Tbilisi, and even overcrowding in Chisinau.

40. Information from OPORA's blogpost "Experts discuss how to face the challenges of mass migration of Ukrainian citizens for the organization of the first post-war elections", 25 October 2023, and references therein.

41. IFES Ukraine (2023b): p. 63-64.

According to the Electoral Code of Ukraine, political parties and candidates participating in elections should nominate candidates for the election commissions. Their ability to find and propose a large number of candidates abroad is questionable. The Electoral Code allows for the possibility of forming election commissions abroad with greater involvement of the Ministry of Foreign Affairs; however, an excessively large number of candidates submitted by this ministry may exert undue influence of the executive branch on the work of the commissions. Preventing administrative resource abuse and maintaining trust in election results is a serious concern in Ukraine. In their interim report on OCVs, the Civil Network OPORA notes that sufficient resources should be dedicated to the electoral commissions abroad and other election management bodies, to guarantee professional work.

3.6. Voting by postal ballot

International standards and practice

Postal voting is the most used voting method for non-resident nationals among EU member states.[42] One key element of the administration of postal voting is the procedure by which voters apply to use the method, and how the identity of the person casting the vote is confirmed to be the same as the original applicant. Since postal voting takes place in the voter's home or other remote location without the presence of election authorities, the process may be vulnerable to fraud or to family voting.[43]

In some countries like Slovenia, Italy, France or Portugal, postal voting is automatically activated for voters registered at the relevant embassy/consulate as permanently resident abroad. In Slovenia, for example, all citizens registered abroad automatically receive a postal ballot by priority mail. Where registration and/or an application process is required, this is done either in person or online (for example in Austria, Slovenia, Poland, Bulgaria and Spain).

Countries employ different methods of verifying the identity of the postal voter and some use multiple methods.[44] These include the following: verification at the point at which the voter registers for the voting mechanism, for example by submitting a copy of their ID along with the application form, as in North Macedonia; verification at the time of receipt of the voting materials by the voter, for example presenting ID in order to receive the ballot in Spain; verification at the point at which the vote is cast, for example by mandating the completion of a self-declaration of identity, as in Austria, a copy of the voters' identification documents to be submitted together with the vote, as in Bosnia and Herzegovina or requiring the presence (Sweden) or signatures (Finland) of two witnesses.

For postal voting, the delivery of postal ballots depends on the performance of local or international postal services and the conditions during transit. Austrian and Slovenian expats have reported at times late delivery of postal ballots in previous elections. In most countries[45] voting material is sent out about a month in advance by normal letter via state (or partly privatised) postal services. Other countries like Austria, Slovenia, Bosnia and Herzegovina, Estonia, Lithuania and Romania send the postal ballots by registered mail while in the Netherlands the possibility exists to receive the postal ballot by e-mail.[46]

In some exceptional cases, countries with an extensive use of direct democracy instruments and hence of frequent votes have introduced universal postal voting, making remote voting the rule, rather than the exception, not only for OCVs but for all resident nationals.[47] This is the case in Switzerland and in a handful of US states. Election management bodies mail postal ballots to every voter included on the voter register,

42. Nineteen out of 28 in 2017; see European Commission, DG JUSTICE (2018), p. 48; European Parliament, European Parliamentary Research Service Briefing on European elections 2024, Voting from abroad in European Parliament elections, March 2024, p. 13.
43. European Commission, DG JUSTICE (2018), p. 48.
44. Ibid.
45. Like in Belgium, Estonia, France, Ireland, Latvia, Lithuania, Sweden and the UK.
46. European Commission, DG JUSTICE (2018), p. 50.
47. IFES (2020), Wally M., Vote by mail: international practice during COVID-19, October 2020, p. 10, available at https://www.ifes.org/publications/vote-mail-international-practice-during-covid-19. "Switzerland and the U.S. states of Oregon, Colorado, Washington, Utah and Hawaii permanently operate universal postal voting – making distance voting the rule, rather than the exception. New Zealand has universalised postal voting for referendums and local elections for more than 20 years – without opening any polling stations."

including to out-of-country voters, without the need for voters to apply for it. Such experience needs to be evaluated on a case-by-case basis and in line with the Venice Commission's position that highlights the risk of remote voting from an unsupervised environment.

Certain measures to promote personal and secret suffrage in postal voting are mentioned in the Code of good practice in electoral matters. The legislator (parliament) must take measures to ensure that the principle of secret suffrage is protected. In practice, certain systems require the elector to complete the ballot paper individually, ensuring that he/she is not being watched, place it in the electoral envelope and make a solemn statement to the effect that the ballot paper was personally completed. This is so in the German regulation of postal voting. Such legal prerequisites are of crucial importance for the compatibility of postal voting with the principles of electoral law as enshrined in the German Fundamental Law.[48] However, they remain lex imperfecta to the extent that it is impossible to control their respect in practice.

To preserve the secrecy of the vote, most countries use a system of either two or three envelopes to enable identifying details to be checked without revealing the content of the ballot. At the moment of counting, the electoral authorities open the outer envelope to identify the voter and place the inner envelope, which contains the ballot paper(s), into the ballot box, thus ensuring that no link can be made between a voter's identity and his/her vote.[49] The two envelopes principle diminishes the risk that a link is made between a voter and their vote but malicious electoral authorities can still open both envelopes.

In most cases, voters abroad return the postal ballot envelope either directly to the EMB of their country or to their country's embassy or consulate, which sends it to the EMB. Several countries have provisions in place to facilitate and accelerate the process for voters. In Austria, voters have the option to drop off their envelope in person or by post at an embassy to have it delivered through diplomatic mail.[50] In other countries, voters abroad can return their postal ballot by registered mail and then get reimbursed, like in Spain, or else they need to cover the costs of returning the postal ballot themselves, as is the case in Slovenia.[51]

The counting procedures of postal ballots vary too. In some countries the capital city's constituency EMB is in charge of counting votes from abroad.[52] In some cases the counting of postal votes takes place several days after election day, as in Austria and Slovenia. In Austria the postal ballots are counted by special district electoral commissions starting the day after election day. In Slovenia, postal votes from within the country are counted one day after election day, and those from abroad thereafter, as they can be accepted until the eighth day after the election day.

The costs of postal voting vary according to which postal services are used. One postal voter in Austria costs more than €7 to the EMB. Costs could go up if an EMB uses private courier services like DHL to send out and have a postal ballot returned immediately following delivery.[53] In the 2020 US presidential elections, postal ballot fees were as little as 22 US cents each to send out, and 55 US cents each to get them returned. Slovenia pays its state-owned postal service €45 000 for sending out postal ballots by priority to 90 000 voters abroad, resulting in a cost of 50 cents per postal voter.

Postal ballot logistics is an industry of its own, where most services – including the printing of voters' addresses on envelopes, QR/barcode tracking, sorting and posting – can be outsourced to private companies

48. Venice Commission/Grabenwarter 2004: § 64 referring to the Federal Constitutional Court of Germany, BVerfGE 21, 200 [205]).

49. European Commission, DG JUSTICE (2018), p. 51. In the two-envelope system (Austria, Belgium, Estonia, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Romania, Spain and the UK), the inner envelope contains the vote and the outer the voter's identification. In France and Sweden there are three envelopes: in France, a second inner envelope is used to enclose the identification details, and in Sweden the ballot is enclosed within two envelopes before being placed in a third for shipping.

50. Ibid. In Spain, people can send the ballot at no cost through certified and urgent mail in person at the post office. A similar system is in place in France. In Germany, the Federal Government has a contract with one postal service provider who is responsible for the special postal ballot service.

51. In Spain, for voters who use postal voting from abroad, the press has reported that those trying to get their related costs reimbursed have encountered problems.

52. See European Commission, DG JUSTICE (2018), p. 51. French consulates transmit postal ballots to Paris and votes are counted on the day of the election in a special polling station in the city. Likewise, in the Netherlands, The Hague municipality appoints a post-only polling station that counts votes cast by post from abroad. In Estonia, ballot papers of voters permanently abroad are counted by the Tallinn City Vote Counting Committee. In Romania, votes are counted by the special Electoral Board for postal voting at the same time as normal votes.

53. The Italian EMB reportedly paid €300 million to DHL for the OCV postal services in the 2018 general election. Interview with Manuel Wally, 15 November 2020.

(for example Cetis in Slovenia).[54] Regarding QR/barcode tracking, it is important to differentiate between two different QR/barcodes: the one used by the postal service provider to track the postal delivery of the postal ballot; and the QR/barcode used by the EMB to identify the voter and ensure that each postal voter voted only once, thereby preventing multiple voting, for example by post and in-country. The code tracking would also provide the option to the EMB to inform the voter that his/her ballot arrived on time and has been included into the count. This could help to detect mistakes, like missing signatures of voters, and reduce the number of invalid postal ballot papers.

With respect to the drafting of the tender documents as well as for the tendering of printing, logistics and postal services, a high level of transparency and inclusion of international expertise could enhance trust in the processes and strengthen the selection procedures.

Postal voting: benefits and drawbacks[55]

Benefits for the CEC	Drawbacks for the CEC
— Once established it could be expanded in-country for people with disabilities or in hospital, home-bound voters, people who live in remote areas and prisoners. — The CEC could reach more voters abroad to participate in elections. — For countries with few diplomatic representations abroad but a large diaspora, it is less of a logistical burden than establishing polling stations abroad. — It is considered to be more cost-efficient than in-person OCV.	— Voting takes place in an uncontrolled environment. It is difficult to ensure that the person votes freely and without coercion. — There is the risk that another person votes on behalf of the voter (it is difficult to identify the voter). — The vote may be intercepted and manipulated. — It is difficult to observe the whole voting process. — Postal services may not work well in certain countries or their service may be disrupted. — Voters may not receive the voting material on time. — The procedures for requesting the vote and for sending the ballot are sometimes criticised for being too bureaucratic. — It implies some costs for the public administration, as well as organisational efforts.
Benefits for the voter	**Drawbacks for the voter**
— It can be used by all people who live abroad, including those with no diplomatic representation in-country or nearby. — It may entail less travelling for voters. — It may be easier to use for people who are sick or have a disability. — It may be used by people in hospital, long-term care facilities or similar institutions.	— Sometimes voters need to pay for the postage of the return envelope. — The postal ballot might not arrive on time. — A voter might be exposed to coercion, attempts to buy votes or other psychological pressure. — Ballots may get lost or damaged, or they may arrive late at the place of counting. — It may be difficult to verify that the vote has arrived. — Votes usually need to be cast in advance. From this moment until election day the voter may change their electoral decision if new information becomes available.

International good practices on setting up postal voting for OCVs are included in Appendix F.

54. https://www.cetis.si/en. There are numerous other companies, like BallotTrax in the US: https://ballottrax.com/

55. Adapted table, see European Commission, DG JUSTICE (2018), p. 54.

Ukrainian legal framework and practice

Ukrainian national legislation does not provide for postal voting, but changes to the legislation may lead to such a voting modality being introduced. However, gaining trust in it will be extremely challenging. Currently, the functioning of postal services in Ukraine raises concerns about the quality and reliability necessary for election-related purposes. Even important legal documents (for example, summonses) cannot be delivered in a timely and correct manner. The use of postal voting may significantly undermine trust in the election results. The negative perception of voters towards the postal service in Ukraine will cast doubt on the results of postal voting abroad, even if it is properly organised by reputable postal operators in other countries. Hence, CSOs like Civil Network OPORA recommend improvement of the existing system, for example by creating more polling stations abroad as the main option.

One important challenge is that postal voting extends the time frame of the electoral process, namely for registration of the candidates, as ballots and other informational material need to be sent to the OCVs sufficiently early to allow them to vote and send back their ballot in time. It requires amending the constitution to allow for early voting. Another major challenge is to prevent vote selling/buying, which is considered an important issue in Ukraine. Supervising the printing process, improving the postal service's reliability and the public's confidence in it, and giving the electorate time to get acquainted with the new voting method are among some of the other challenges. Another issue is the replacement of the current ballot with a smaller and cheaper alternative to facilitate shipping abroad.[56]

3.7. Proxy voting

International standards and practice

Proxy voting[57] is a system where a voter grants authorisation to another individual, known as a proxy, to vote on their behalf. This typically occurs when the voter faces difficulty or is unable to cast their vote in person. The voter communicates their voting preference to the proxy, who pledges to cast the vote according to these instructions. Depending on the established voting procedures, the authorised proxy may cast votes either during early or advanced voting, through postal services, at diplomatic missions abroad, or at regular polling stations on the election day. The eligibility criteria for proxy voting vary, ranging from general availability to all voters to specific and narrowly defined circumstances. Some instances may necessitate proof of the voter's incapacity to attend a polling station. In Belgium,[58] individuals facing obstacles such as illness, work commitments, studies, military service, imprisonment or adhering to religious beliefs as well as those residing abroad may designate a proxy to vote on their behalf. Written authorisation is required. In contrast, both France and the Netherlands have more lenient requirements, as no proof or justification is necessary for proxy vote requests in France, where proxy voting is the sole form of absentee voting, and each proxy in the Netherlands can represent up to two individuals. In France and the Netherlands, proxy voting is the only form of voting available for prisoners and voters in pretrial detention.[59] According to the Venice Commission's Code of good practice in electoral matters though, very strict rules must apply to voting by proxy and the number of proxies a single voter may hold must be limited. According to the OSCE/ODIHR, it can be argued that proxy voting can support the requirements of universality and equality as it facilitates voting for groups at greater risk of exclusion, such as the elderly, people with disabilities, voters abroad, citizens in pretrial detention and penal institutions and others.[60] Other countries, notably Finland, explicitly prohibit proxy voting. Even in those countries where proxy voting is a legitimate voting tool, many women have been effectively disenfranchised through proxy voting by men relatives. Proxy voting is particularly problematic in countries where vote buying is a prevalent concern and thus is not to be recommended.

Although used in some countries, generalised use of proxy voting for voters abroad is not in line with upholding the secrecy and equality of the vote as enshrined in international standards and regional

56. Some MPs disagree, saying that this would confuse voters.
57. OSCE/ODIHR, Alternative voting methods and arrangements, Warsaw, 12 October 2020.
58. Venice Commission, Report on Electoral Law and Electoral Administration in Europe, 8 October 2020, Study No. 965/2019a, p. 36.
59. Ibid.
60. OSCE/ODIHR, Alternative voting methods and arrangements, Warsaw, 12 October 2020, p. 20.

commitments.[61] It should be underlined that the same concerns related to proxy voting are also valid for postal voting and for internet voting from home.

3.8. Other voting methods for non-resident citizens

International standards and practice

Returning to vote in the country

Members of the Slovenian diaspora may freely choose to vote at a polling station in a diplomatic or consular representative office (diplomatic representations) if available, by post or in-country at a special polling station at the headquarters of a local electoral commission (OMNIA polling station) and need to notify the EMB no later than 30 days before the election day about the chosen method. Croatia provides for in-person OCV. If the voter wishes to vote in the area of another diplomatic representation or within Croatia, the voter has to state in the request the diplomatic representation and the address of temporary residence in Croatia on election day. Several other countries allow expatriate citizens to vote in the country on election day, but no international guidelines of good practice exist. In Singapore voters abroad are also assigned a polling station in Singapore, where they can vote in person if they happen to be in Singapore on election day. No EU member state covers the costs of voters abroad to travel to an embassy/consulate to vote in person. However, in Malta eligible voters have been offered the opportunity to book subsidised tickets (in 2022, costing €90 with Air Malta) to vote in person in-country as no OCV exists.

Mobile voting stations abroad

While recent IDEA research[62] indicates that there are two countries offering mobile ballot boxes for OCV, there is no indication as to which two. It could be an option for mobile voting units to visit military bases or other locations to facilitate voting, but this might be prone to possible misconduct.

Ukrainian legal framework and practice

Returning to vote in Ukraine

This matter entails a dual aspect that warrants careful consideration. Ukrainian citizens currently registered with consular authorities and possessing their electoral address abroad for the purpose of returning to Ukraine to participate in elections will be required to modify their electoral address within a constrained time frame. The likelihood of all individuals effecting this change within the allotted time frame is not substantial. It will undoubtedly require additional regulation. Individuals residing abroad who have not undergone registration with consular bodies (retaining their registered address within Ukraine) will retain the freedom to return and exercise their voting rights within their home constituency or opt for an alternative polling location. This option is extremely complex and largely depends on the security situation in Ukraine. Furthermore, of great importance is the engagement of voters in the overall electoral campaign (nomination of candidates, formulation of their programmes, public discussion of electoral programmes, political competition, etc.). Ensuring these aspects will not be so straightforward for a large number of voters.

Mobile voting stations abroad

National legislation does not provide for such a possibility abroad. Mobile voting stations are possible within Ukraine (voting at home). An election precinct may be regular (the system of permanent precincts approved by the Central Election Commission), special (established in hospitals and other specialized institutions) or abroad. Extracts from the regular voter list are created at each ordinary polling station for home voting, providing the opportunity to vote at home to individuals who, because of health issues, cannot come to the polling station and are included in these extracts from the voter lists. There is a relatively low level of confidence in voting outside regular polling stations in Ukraine. For example, remarks about the honesty and freedom of elections occur much more frequently during home voting or voting at special polling stations than at regular polling stations.

61. ICCPR, Article 25, paragraph 20, of the 1996 CCPR General Comment No. 25; European Convention on Human Rights Protocol No. 1 (Article 3); paragraphs 7.3 and 7.4 of the 1990 CSCE Copenhagen Document require participating states to "guarantee universal and equal suffrage to adult citizens" and to "ensure that votes are cast by secret ballot or by equivalent free voting procedure."

62. IDEA 2023, "Unravelling out-of-country voting – A deeper look into OCV practices, the use of technology and turnout": https://www.idea.int/data-tools/data/ocv-technology-turnout

3.9. Observation

International standards and practice

Election observation provides greater transparency. The perception that out-of-country voting is a "black box" contains a significant risk that perceptions of fraud through diaspora voting, whether valid or not, can seriously undermine the integrity and acceptability of the overall electoral process.[63] An absence of the normal checks and balances provided by observation could create a situation with little scope for independent rebuttal and verification by the EMB. Legal safeguards on the observation, monitoring and access to the CEC during the administration of out-of-country ballots and on the testing, verification and safety of election material or information technology systems which are used for OCV shall not be to a lesser extent than those in in-country voting.

Ukrainian legal framework and practice

The establishment of election administration bodies abroad should occur on a party political basis. Political parties must have at the very least the ability to effectively control the work of election commissions or other bodies. The majority of parties lack such organisational and financial capacity and this capacity is unlikely to develop in most parties even after the conclusion of the war.

3.10. Out-of-country-voter obligations

International standards and practice

The situation is the same as for active and passive voting rights (see above, Section 3.1 and 3.2 "Right to vote and to elect" and "Right to stand for election").

Ukrainian legal framework and practice

The duties of voters at foreign polling stations are analogous to the duties of voters within the territory of Ukraine. One significant obstacle to the exercise of electoral rights abroad is the very limited number of polling stations. Voters may have to travel long distances to cast their vote.

C. Internet-voting channel

1. International legal standards

This study focuses on standards that apply in the Council of Europe region. The core mission of the Council of Europe is to safeguard and realise the principles that are the common heritage[64] of its member states, among which are the principles for democratic elections enshrined in Article 3 of Protocol No. 1, the right to free elections, to the European Convention on Human Rights (the "Convention") as interpreted by the European Court of Human Rights (the "Court"). These principles are included and further developed in national constitutions and electoral laws. All solutions, tools or procedures used in elections, including i-voting, should respect all applicable principles.

The application of electoral principles to i-voting is not straightforward, given the technical complexity of this channel. Following demands from member states, the Council of Europe has created soft-law instruments that offer guidance to countries on how to regulate such technologies with a focus on compliance with electoral principles. Soft-law instruments include the Committee of Ministers Recommendation CM/Rec(2017)5 to member States on standards for e-voting and the related explanatory report and implementation guidelines,

63. IFES (2012), Erben P., Goldsmith B. and Shujaat A., Out-of-country voting: a brief overview, April 2012, p. 4

64. The Venice Commission Code of Good Practice in Electoral Matters sets out the fundamental principles of the European electoral heritage.

as well as the 2022 Committee of Ministers Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States. The recommendation on e-voting addresses the use of electronic means for voting and/or counting purposes, in both supervised (polling station) and unsupervised (from home) environments, covering e-voting machines in polling stations, the use of optical scanners to register and/or count paper ballots and internet voting. The guidelines on the use of ICT in elections aim to provide minimum requirements for any other ICT used in elections. The guidelines are aligned with and complementary to the recommendation on e-voting. Both instruments are relevant for this study. Furthermore, the Council of Europe organises biennial meetings to discuss the implementation of the recommendation and guidelines with member states. The last meeting (June 2023) concluded that:

> *there is a rising concern over an increased risk of cyberattacks, foreign interference and manipulation particularly in national elections where the stakes are likely to be the highest. As the mere allegation of interference in elections might in itself undermine trust in democratic processes and its outcomes, states seem to be reluctant to consider or introduce internet voting solutions, especially as it is extremely difficult to ensure full security of online systems.*[65]

Other relevant documents have been drawn up by the Venice Commission and OSCE/ODIHR. The Venice Commission reviewed in 2004 the compatibility of remote voting and electronic voting with the standards of the Council of Europe and the Court's case law. The report concluded that electronic voting (including internet voting) should be accepted only if it is secure and reliable and if electors are able to obtain confirmation of their vote and correct it, if necessary, while respecting secret suffrage. A system's transparency should be guaranteed and at the same time any violation (including of secret suffrage) should be sanctioned.[66] The OSCE/ODIHR has developed guidelines for observing the use of internet voting.[67]

2. Countries' regulations

2.1. Switzerland

I-voting development

Switzerland has several specificities. It is a federal state whose 26 cantons (states) assume the responsibility for organising and financing their voting systems. Each canton decides which system to use. All have generalised postal and polling station voting, the two main voting systems in Switzerland. Almost half of the cantons have at some point in the past 20 years experimented with internet voting, either building their own system (Geneva, Neuchâtel, Zürich) or co-operating with those three cantons who had systems or with the fourth and more recent system of the Swiss Post. Several did so for longer, other for very short periods. Since 2019, there has been only one system: the Swiss Post system. Three cantons resumed i-voting trials in 2023 (Basel-Stadt, St. Gallen and Thurgau); a fourth one (Graubünden) received federal authorisation to do so in 2024. Federal authorisation is required for any use of i-voting during federal votes. A fourth voting method exists, namely public voting in assembly by raising of hands (total lack of secrecy), also known as Landsgemeinde and practised once a year in the smaller cantons of Appenzell Inner Rhoden and Glarus for cantonal votes. Assembly voting is practised in a majority of municipalities for local votes only.[68] A typical feature is mutual trust between voters and the election administration.

Another typical feature is that Switzerland is a semi-direct democracy whose electorate not only elects representatives but also votes on issues (initiatives and referendums) at the three tiers of government. This means

65. See the outcome document of the Council of Europe conference on "E-voting and use of ICT in elections – Taking stock and moving forward", held in Strasbourg, France, on 16 June 2023 at https://rm.coe.int/conference-on-e-voting-and-use-of-ict-in-elections-taking-stock-and-mo/1680abedd9

66. Venice Commission (2004), Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2004)012-e; see also: Council of Europe (2017), Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726c0b

67. OSCE/ODIHR, Handbook for the observation of information and communication technologies (ICT) in elections, Warsaw, 26 February 2024.

68. Switzerland has entered a reservation to Article 25 of the ICCPR to safeguard such methods despite the violation of vote secrecy. The federal court has referred to the historical aspect of the Landsgemeinde as well as to practical aspects (namely financial), concluding that advantages prevail. The legal literature is more critical.

that voters go to the polls on average four times a year. Expatriates have extensive voting rights too, including all active and passive rights at the federal level: they can vote to elect the federal parliament and on federal initiatives and referendums, they can sign such requests and also be themselves candidates for the federal parliament. They are assigned to their commune of origin or last residence and do not elect their own representatives. Several cantons have given their expatriates rights at the cantonal level and a couple of them do so also at the local level, allowing expatriates to participate in local decision making. Such extended rights are criticised by several authors who argue that expatriates do not pay taxes in Switzerland. Others contrast such extensive rights for expatriates to the absence of rights for regularly established foreigners who, despite paying their taxes in Switzerland, have no political rights in a majority of cantons, not even at the local level.

An important Swiss peculiarity is the apparent lack of concern about coercion. Postal voting has been in widespread use since the 1990s and roughly 90% of voters vote by post. Postal voting is considered an important precondition for allowing experiments with i-voting. Switzerland has adopted a cautious approach towards i-voting, reflected in the moto "security before speed". This explains the very long experimental phase which started at the beginning of 2000. After hundreds of trials (a trial is the binding use of i-voting by one canton for one federal vote),[69] i-voting was stopped in 2019 and only resumed in 2023, and is currently limited to four cantons (as of March 2024).

All voters automatically receive all voting material at home via post and can choose to vote by post, at the polling station or, where the possibility exists, by i-voting. Where i-voting is possible, voters receive several codes with their voting material which serve to authenticate the voter, confirm his or her vote and verify it. Codes are valid only for one vote/election and are individual (different for each voter). I-voting lasts four weeks (from Monday to Saturday before election/voting Sunday). This is also the case for postal voting (in some cases, postal votes are accepted until the closing of polling stations on the Sunday). Polling stations open a couple of hours on voting Sunday and in the preceding few days. Voting ends at noon on Sunday. Only after that can the results be published. The table below details the number of voters authorised to use i-voting in the three cantons during the last federal election of October 2023 and their level of participation (note that participation is usually higher in elections than in votes on initiatives and referenda; note also that use of internet voting resumed in 2023 after an interruption of four years). Federal law limits i-voting trials to a maximum of 10% of the federal electorate and 30% of the cantonal electorate (only some cantons do i-voting simultaneously) (Article 27f of the Political Rights Ordinance). These upper limits have never been reached, not even in the best years, where up to 14 cantons used i-voting.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei

Eckdaten zum Einsatz der elektronischen Stimmabgabe am 22. Oktober 2023 (Nationalratswahlen)

Bedingungen / Kantone	Zugelassenes Elektorat Anzahl Stimmberechtigte (A)			Stimmbeteiligung zugelassenes Elektorat alle Kanäle (B)		Anteil elektronischer Stimmkanal (C)		
	Inland	Ausland	Total	Anzahl Stimmende	in %	Anzahl Stimmende	in % am zugelassenen Elektorat (A)	in % an allen eingegangenen Stimmen (B)
Basel-Stadt	18	9'861	**9'879**	2'359	23.88%	1'444	14.62%	61.21%
St.Gallen	39'598	10'889	**50'487**	19'821	39.26%	2'495	4.94%	12.59%
Thurgau	-	4'953	**4'953**	956	19.30%	541	10.92%	56.59%
Total	**39'616**	**25'703**	**65'319**	**23'136**	**35.42%**	**4'480**	**6.86%**	**19.36 %**

Lesebeispiel: Im Kanton St. Gallen waren 39'598 im Inland wohnhafte und 10'889 im Ausland wohnhafte Stimmberechtigte und damit insgesamt 50'487 Stimmberechtigte zum Versuch mit der elektronischen Stimmabgabe zugelassen. Davon haben 19'821 an der Abstimmung teilgenommen, dies entspricht einer Stimmbeteiligung von 39.26 %. 2'495 dieser 19'821 abstimmenden Stimmbürgerinnen und Stimmbürger haben für die Stimmabgabe den elektronischen Kanal benutzt, dies entspricht einem Anteil von 12.59 %. Von den 50'487 zugelassenen Stimmberechtigten haben im Kanton St. Gallen 4.94 % elektronisch abgestimmt.

69. Half of Swiss cantons have trialled e-voting and stopped using it.

The table above also details the use of internet voting in the latest federal elections of 22 October 2023. The total number of voters authorised to use i-voting on that occasion was 65 319, of which 25 703 were non-resident citizens. The total number of Swiss electors for that election was 5 583 221, of which 222 889 were non-residents. The overall participation rate (through all voting channels available, including at a polling station, including anticipated voting, postal voting and i-voting in the three cantons) was 46.7%.[70] Only 6.86% of those authorised to use i-voting in the three cantons made use of this option, which represents 19.36% of those who actually voted. Participation was higher in the cantons of Basel-Stadt and Thurgau compared to St. Gallen. The difference may stem from the fact that in the first two, non-residents were (almost) the only group authorised to use i-voting, whereas in St. Gallen, the majority of those authorised were resident voters (over 39 000 as opposed to over 10 000 OCVs). This confirms that non-residents are the most interested in i-voting. Their lobby is the main group pushing for the greater use of i-voting in Switzerland.

I-voting regulation

Federal regulation of internet voting includes a dedicated article (Article 8a) in the Political Rights Act (PRA). This article authorises the federal government to experiment with i-voting. A dedicated chapter (Articles 27a ff.) was introduced in 2002 to the Political Rights Ordinance (PRO) offering mainly organisational details about i-voting. I-voting trials started in 2003 (only in cantonal votes). Since 2004, i-voting has been authorised for federal votes as well.

There have been three evaluation reports of the trials by the federal government. They served as a basis for further changes to the PRO. The PRA has not changed, and i-voting is still experimental. In its third evaluation (2013), the federal government decided that "black box" first-generation systems used until then should be gradually replaced with "end-to-end verifiable" systems that offer individual and universal verifiability. The PRO was modified at the end of 2013 and a new instrument, the very detailed Ordinance of the Federal Chancellery on e-voting (OEV) was introduced on 15 January 2014 to regulate in detail verifiability and other aspects. Individual verifiability requires a second channel for the transmission of verification codes: in Switzerland, this second channel is the postal channel. An important provision was introduced on 1 July 2018 making the publication of the source code for the software for complete verifiability and related documents mandatory. The federal regulation requires that e-voting systems and their security are state of the art. Use of internet voting for federal votes continues to be subject to authorisation by the federal government and to the agreement of the Federal Chancellery. Risks must be constantly evaluated and kept at an acceptable level by the cantons. Political risks may prompt federal authorities to suspend or not issue the federal authorisation or agreement.

Consultations between the Federal Chancellery and academics took place from the beginning of the experiment. However, joint work with IT academics intensified after 2019 following the results of a transparency exercise (public intrusion tests and disclosure of source code), during which researchers discovered major flaws in the Swiss Post system. The attempt by the government to put an end to experiments and to normalise the use of i-voting failed. After consultations, a new PRO and OEV entered into force in July 2022. These new regulations aim to organise stable trials with i-voting, prolonging the experimentation. According to the Federal Chancellery, the system and its operation have improved to such an extent that it is possible to use it within the limited scope of the approved trials.[71]

Several legal questions subsist. Unlike Germany or Austria, there has been no evaluation of the constitutional compliance of the i-voting federal regulation by a federal judge, or any other validation of this order. The indefinite continuation of the experimentation may be questioned. Scholars have criticised the fact that the Swiss regulation and practice do not respect the requirement of public control over the election and that the lower-level regulation (unlawfully) delegates important responsibilities to experts.[72] The renewed extension of the experiment shows, among other things, that, as stated by the Federal Chancellery, the system is not mature for larger deployment (to more than 10% of the federal electorate). This is despite the 20 years' experience and continued improvements, and the money put into the quest for state-of-the-art solutions.

70. https://www.fedlex.admin.ch/eli/fga/2023/2613/fr/annexes

71. Media release, "Federal Council approves resumption of e-voting trials", of 3 March 2023, available at: https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-93455.html

72. Markic L., "Die elektronische Stimmabgabe im Lichte des Prinzips der Öffentlichkeit: E-Voting im Spannungsverhältnis zwischen dem Ruf nach mehr digitaler Demokratie und der Wahl- und Abstimmungsfreiheit", in: Dal Molin-Kränzlin/ Schneuwly/Stojanovic (Hrsg.). Digitalisierung - Gesellschaft - Recht. Zürich, Dike Verlag, 2019, pp. 125-143.

Swiss i-voting presents several good practices, including a high level of transparency (publication of source codes, system documentation, audit reports and other expert evaluations), co-operation with IT experts worldwide mandated by the authorities and Swiss Post to work on implementing state-of-the-art solutions,[73] periodical intrusion tests and continuous bug bounty programmes. Switzerland also has the most detailed and comprehensive i-voting regulation.

2.2. Estonia

I-voting development

Estonia is the only country where internet voting is available to all voters as an alternative to in-person voting in polling stations, advance in-person voting in polling stations and postal voting. Postal voting is allowed in Estonia.[74] Countrywide remote i-voting with binding results in all elections and referendums has been allowed since 2005. Internet voting takes place during the early voting period – a six-day period starting 10 days prior to election day.

Estonia's other specificity is that it is one of the most digitally advanced societies. A foundational element is the national identification system where each Estonian (from birth) and resident gets a unique identifier. Personal data are stored in the Digital Population Register. A feature of the legal framework is a prohibition on duplication of information – if a new public service requires, for example, a person's age, this can be retrieved from the Population Register, but not stored in the new system.[75] Another feature is that all adult inhabitants are obliged to possess electronic identity. The e-ID solution is used throughout the private and governmental sector to identify a person and for digital signing. With i-voting, the e-ID serves both to authenticate the voter and to confirm their vote. The compulsory e-ID as a universal access key to public and private e-services is a critical success factor for i-voting, advanced e-health solutions, digital signatures, electronic tax boards, etc.[76]

I-voting regulation

The legal framework for i-voting is provided by electoral law. The provisions are almost the same in all legal acts regulating voting procedures (Riigikogu Election Act, Municipal Council Election Act, European Parliament Election Act, Referendum Act), whereas the most detailed provision is stipulated in the Riigikogu Election Act.[77] This act provides for the establishment of an Electronic Voting Committee whose members are appointed by the National Electoral Committee (NEC). The NEC also provides administrative and operational support and has adopted a decree on the detailed provisions concerning the organisation of i-voting.[78] The Electronic Voting Committee may propose to the NEC "not to start or to suspend or terminate electronic voting if the security or reliability of the electronic voting system cannot be ensured in such way that electronic voting could be conducted pursuant to the requirements of this Act". Furthermore, different Council of Europe guidelines and the OSCE/ODIHR observation and assessment reports on e-voting (including i-voting) have served as examples and sources of best practice in developing Estonian solutions and regulations.

Council of Europe Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting has been referred to by the Supreme Court of Estonia.[79]

73. Federal Chancellery, Summary of the expert dialogue. Redesign of internet voting trials in Switzerland, November 2020, available at https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/berichte-und-studien.html
74. https://www.valimised.ee/en/estonian-elections-nutshell/advance-voting/voting-foreign-states
75. Public Information Act, Chapter 5^1, § 43^1 to 43^9, Databases. See, for example, § 43^3, Establishment of databases: (1) A database is established by an act or legislation issued on the basis thereof; (2) establishment of separate databases for the collection of the same data is prohibited. https://www.riigiteataja.ee/en/eli/522122014002/consolide
76. Madise U. and Vinkel P. (2017), "A judicial approach to internet voting in Estonia", in Driza Maurer A. and Barrat J. (eds), E-voting case law – A comparative analysis, Routledge, Abingdon.
77. See Chapter 7^1 (Articles 482 to 488), Electronic Voting: https://www.riigiteataja.ee/en/eli/ee/510032014001/consolide/current (in force since 11 November 2012).
78. "The procedure for the organisation of electronic voting and the ascertaining of the results of electronic voting" can be found here: https://www.riigiteataja.ee/akt/118032014016 (in Estonian).
79. Madise U. and Vinkel P. (2017), "A judicial approach to internet voting in Estonia", in Driza Maurer A. and Barrat J. (eds), E-voting case law – A comparative analysis, Routledge, Abingdon.

The broader legal framework includes the entire "ecosystem" of e-governance in Estonia, much of which predates the introduction of i-voting and includes the following acts: the Personal Data Protection Act, Public Information Act, Identity Documents Act, Digital Signatures Act, Population Register Act (including Voter Registration and Voter List provisions), Electronic Communications Act, Citizenship Act and Courts Act.

Technical enhancements and improvements have been introduced in response to stakeholder input, including from the OSCE/ODIHR. In 2011, a special working group was established by the parliament to propose solutions for increasing transparency and accountability in internet voting systems. A technical review by the elections management body proposed that voters should be able to verify that their choices had been properly handled by the system (individual verification) and that a separate channel should be used for this verification. Updated legislation in 2012 included provisions for individual verifiability via a separate channel: this second channel is the smartphone. The societal evolution from voters' primary connection to the internet being a personal computer (desktop or laptop) to mobile devices as the primary device has driven a process of re-evaluation of the model. In 2019, a multi-stakeholder working group convened by the Estonian ministry with responsibility for information technology conducted a comprehensive review of the entire system and produced a list of proposals for future improvements and changes – including the necessary responses to the shift to mobile devices as primary devices. Additionally, and recognising the significance of any shift to mobile devices as the primary channel for internet voting, the Estonian State Information System Authority and the State Electoral Office (the EMB) commissioned a separate analysis. A paper presented to the annual eVoteID conference in Bregenz, Austria (held online in 2020) entitled "Planning the next steps for Estonian internet voting" offers a detailed insight into the technical status quo and future for Estonian internet voting.

The country has addressed concerns about voter coercion and lack of secrecy by allowing individuals to modify their online vote multiple times until the day of the election and even allowing them to vote on paper at the polling station during the advanced voting period and, since 2021, during the election Sunday as well, the paper vote overriding the e-vote. The Supreme Court of Estonia explained that to be constitutional, e-voting should offer the possibility to change one's e-vote during the voting process so that the voter could change a coerced vote to one of their own choice at a later time, in private. This is a core pillar of the "virtual voting booth" concept, which strives for delivering to internet voters the same constitutional protections offered to in-person voting on paper, and thus aims at rendering internet voting constitutionally compliant. It follows that internet voting cannot replace paper voting – it must always be offered in parallel with paper voting. The cost implications are clear.

Scholars note that in its decision on multiple voting, the Supreme Court examined only some of the constitutional aspects of i-voting. They emphasise that the constitutionality of the internet as a communication channel, together with possible threats regarding anonymity and secrecy, the faith put in the electoral system and in experts or the difficulty of obtaining evidence, were not analysed during that particular review and indeed have not yet been analysed by the Estonian Supreme Court.[80] The Supreme Court ruled in 2019 that additional technical and procedural provisions related to i-voting should be regulated by law rather than by sub-legal acts from the National Electoral Committee or the State Electoral Office, which was created after the 2015 election (to take over election management tasks, leaving the oversight function to the NEC). The question of the constitutional compliance of i-voting arose again during the 2023 parliamentary election, where more than 50% of voters used i-voting. While the Supreme Court eventually dismissed all complaints filed in connection with the 5 March 2023 Riigikogu election, it also suggested that additional rules for i-voting need to be added to the constitution. The court noted that detailed rules are currently managed by the state electoral office and the NEC, and this can make the process difficult to understand, even by people with good legal knowledge. It also noted that the rules need to be written down in sufficient detail to ensure compliance and public confidence in elections and that the organisation of electronic voting needs continuous attention from the legislator and the executive. The Chief Justice of the Supreme Court, Villu Kõve, suggested that a constitutional review procedure should be initiated to assess the i-voting rules in relation to the constitution. In particular, the 2023 complaints raised the question of whether the essential rules on internet voting should be more specifically contained in the law or at least in a government decree, and whether their establishment should not be delegated to the National Electoral Committee and the State Electoral Office. These arguments recur in appeals from election to election and need a clear position from the Supreme Court to end further disputes, according to the Chief Justice.[81]

80. Ibid. See also Vinkel P., Chapter 3, "Historical developments and legal aspects", in Solvak M. and Vassil K. (2016), E-voting in Estonia: Technological diffusion and other developments over ten years (2005-2015), University of Tartu..

81. https://news.err.ee/1608932273/supreme-court-dismisses-all-election-complaints

The OSCE/ODIHR criticised the process in 2019, since "the system is not software independent, meaning that errors in its components may cause undetected errors in the election results, and it is potentially vulnerable to internal attacks and to allegations of cyberattacks, which may affect public confidence".[82] In 2023, the OSCE/ODIHR noted that there are "notable divisions within the society between those who fully trust and those who fully distrust internet voting" and that "this polarisation was also represented in the political spectrum, with some parties resolutely supporting internet voting and other parties raising doubts before and after the elections, most notably EKRE". It recommended that in order to "further increase and maintain trust in internet voting, the election authorities should proactively address all concerns raised by election stakeholders who distrust the results of internet voting".[83] It furthermore recommended the election authorities to consider methods to achieve end-to-end verifiability, to improve the current verifiability mechanisms, namely remove deficiencies in individual verifiability, to ensure that all the critical steps for determining the results of internet voting are auditable, or to publish complete, precise and up-to-date documentation regarding technologies and processes supporting the internet voting system, among other recommendations.

Estonian i-voting presents several good practices, in particular the openness to observers. According to Estonian electoral laws, all activities related to elections are public. Observers have access to the meetings of all election committees and can follow all electoral activities, including the voting process, counting and tabulation of results. I-voting is no different. Significant documents concerning the i-voting system are public, however there is room for improvement according to the OSCE/ODIHR. In order to enhance the observers' knowledge of the system, political parties are invited to take part in a training course before each election in which i-voting is used. Besides political parties, auditors and other people interested in the i-voting system take part in the training. In addition, observers are invited to follow the test of the whole process and to take part in other preparatory procedures. However, few political parties have so far exercised their opportunity to observe the i-voting procedures.[84] It is important that observers are deployed for a length of time necessary to allow meaningful observation. If some important stages influencing the correctness of final results have not been observed, then conclusions cannot be made about the integrity of the system.[85]

2.3. France

Articles R176-3 ff of the Electoral Code (the Regulation part) provide for distant electronic voting and provide that the automatic treatment of personal data is the responsibility of the Ministry of Interior and the Ministry of European and Foreign Affairs (MEAE). The code also provides that the system should be subjected to controls by independent experts before its implementation and/or after any major modification, to assess the conformity of the system with the required guarantees of secrecy of the vote and sincerity of the election. The detailed regulation is contained in a joint decree from the two ministries, which includes provisions on data, on the means of independent control, on the guarantees that a provider should offer, on the transmission of identifiers and passwords to voters, etc. Based on the results of independent controls or on other considerations related to elections, the MEAE, advised by the National Agency on Security of Information Systems (ANSSI), may decide not to use internet voting.

ANSSI's technical supervision is thus part of the regulation. Furthermore, internet voting is regulated by the CNIL (National Commission on Information Technologies and Freedoms), a French independent agency that defines security recommendations that are legally non-binding with a focus on data protection. The CNIL recommendation on i-voting is general, i.e. covers all kinds of elections. Furthermore, the preamble to the CNIL recommendation mentions that the CNIL maintains reservations about the use of internet voting for political elections.

The constitutional judge has not evaluated the conformity of i-voting provisions with the constitution.[86]

82. OSCE/ODIHR Estonia, Parliamentary elections, 3 March 2019, ODIHR Election Expert Team Final Report, p. 1.
83. OSCE/ODIHR Estonia, Parliamentary elections, 5 March 2023, ODIHR Election Expert Team Final Report.
84. See Maaten E. and Hall T. (2008), "Improving the transparency of remote i-voting: the Estonian experience", in Krimmer R. and Grimm R. (eds), Electronic voting 2008, Gesellschaft für Informatik, Bonn.
85. Madise U. and Vinkel P. (2017), "A judicial approach to internet voting in Estonia", in Driza Maurer A. and Barrat J. (eds), E-voting case law – A comparative analysis, Routledge, Abingdon.
86. Anziani A., Lefevre A., Parliamentary report No. 445 (2013-2104), 9 April 2014 (in French): https://www.senat.fr/rap/r13-445/r13-445.html

2.4. Australia

The state of New South Wales began using internet voting in 2011 but stopped doing so in 2023.[87] The Electoral Legislation Amendment Bill (No. 2) 2022 [NSW] Amendment of Electoral Act 2017 No. 66 introduced a prohibition to use internet voting and, more broadly, any so-called "technology assisted voting" other than telephone voting as a special provision for the 2023 general election and certain by-elections (Part 4, §14 of the bill). Postal voting was maintained.

A review of the feasibility of internet and other forms of technology-assisted voting for New South Wales state and local government elections by the New South Wales Electoral Commission concluded in November 2023 that:

> *(2) To maintain the security and transparency of the New South Wales election system, paper-based voting should continue as the primary voting channel for the foreseeable future …*
>
> *(5) Internet voting is a high-risk channel, facing a worsening cyber and misinformation threat environment involving state and criminal actors seeking to disrupt elections. Moreover, the processes for verifying votes and other assurance steps are not generally understood by electors or political participants.*
>
> *(6) Internet voting appears to be the preferred way for electors who are blind or have low vision to cast their votes independently and in secret – and may be feasible for these electors only from 2027 for NSW state and local government elections. This is contingent on the availability of suitable market solutions, adequate government funding and legislative reform.*

For Australia, the Electoral Council of Australia and New Zealand (ECANZ) "Eleven essential principles for an Australian internet voting service" reflect the objectives of enfranchisement, integrity and privacy when designing and operating internet voting. In drafting these principles, the ECANZ examined the United States Election Assistance Commission's Voluntary Voting System Guidelines (VVSG 2.0) and the Council of Europe's recommendation on standards for e-voting (Recommendation CM/Rec(2017)5).

2.5. Ecuador

Following exchanges with Parliamentary Committee representatives, Ecuador's most recent experience with i-voting in 2023 can also be added to this study. The following information is based on an interview with Régis Dandoy, Political Science Professor at the Universidad San Francisco de Quito, election observer and researcher in electronic voting, in particular in Belgium, France and Ecuador.

Non-resident nationals

Only 200 000 out of an estimated two million Ecuadorian OCVs had registered to vote in the past and participation rates are low, between 20 and 40% in a country where voting is mandatory (however, there is no penalty for non-voting OCVs). OCVs have voting rights only at the national level. Paper voting for OCVs takes place in consulates and in numerous other hired polling places. Paper votes within Ecuador cost US$1 per vote; abroad, at consulates, it costs between US$5 and US$10 per vote, which is considered quite expensive. Additional costs for OCV include sending tonnes of paper abroad (for example, several votes on referendums and elections take place on the same day) and the price of hiring additional voting places (for example in Madrid, the cost of hiring a sports centre and some 30 to 40 polling places in the city for some 40 000 electors). Further costs relate to the fact that each polling place is staffed by five people, some of whom are sent abroad from Ecuador. All staff require training and the travel involves money spent on transportation, hotel, meals, etc. Furthermore, a lot of printed information and publicity related to elections is sent by postal mail abroad.

I-voting

Ecuador initially used internet voting in 2014 in two provinces. The experience was not renewed in the following years, mainly for financial reasons. However, in the 2021 elections, three experimental channels

87. https://elections.nsw.gov.au/about-us/reports/ivote-reports

(pilot schemes) were offered to OCVs: voting machines abroad (for voters in Buenos Aires, Argentina), internet voting (for those in Phoenix, USA) and postal voting (for voters in Ottawa, Canada). The impact of use of voting machines was negligeable. The participation of OCVs in internet voting was evaluated positively against the use of voting machines.[88] It was decided that internet voting should be offered in February 2023 when a lower-stakes election took place. This experience ran smoothly too. Hence, it was decided to use i-voting in the August 2023 snap parliamentary and presidential elections.

Internet voting took place on voting day, Sunday 20 August 2023, from 9 a.m. to 7 p.m. local time, for the election of the President of Ecuador and members of the National Assembly and on two referendum questions. It started smoothly with OCVs voting from Asia. Problems started when expats in Europe and later in the US started to vote. Voters were unable to log in to vote. According to the country's election agency (CNE), cyberattacks in the form of a DDoS (distributed denial of service), with 1 million access demands simultaneously, were generated from seven countries, India, Bangladesh, Pakistan, Russia, Ukraine, Indonesia and China.[89] The attack impacted more particularly the participation of voters in Europe. The problem could be mitigated only hours later. Internet voting can thus be highly vulnerable to effective disruption, as the paralysis of a single hosting infrastructure may be sufficient to disrupt access to the voting system. Such cyberattacks can be particularly challenging to mitigate. The concerns raised by the typical protection mechanisms in the context of elections have been explored by technical research in other contexts, such as during the 2017 state elections in Western Australia.[90]

In Ecuador, the i-vote closed as foreseen without any prolongation, namely for those who were prevented from voting by the attacks. No official documents or studies related to the cyberattacks have been published so far. The votes were counted and the difference of votes between candidates was taken into consideration. The difference of votes between the first two presidential candidates was bigger than the number of registered OCVs. Where the difference was smaller than the number of registered OCVs, the vote was repeated. This was the case for the last two places (13 and 14) on the list for the national parliament. The election of the six representatives of OCV was also repeated. One small party who allegedly won one of these contests and could have appealed against the organisation of a re-run came under public pressure and eventually did not contest the decision to repeat the vote. All parties agreed not to use i-voting for the re-run.

The voting system used is provided by the government and produced by the ESPE University (Armed Forces University; in Spanish: Universidad de las Fuerzas Armadas) in co-operation with the Army. It was administered by the CNE. There are no documents on the system or the procedures available. Regulations on i-voting have not been published. There is also no peer evaluation of the system or of the procedures available.

No i-voting was foreseen for the next two 2024 votes in March and April. However, the idea has not been totally abandoned and discussions on i-voting could resume as early as 2025. Two out of five CNE members are in favour, two are not decided and one (the CNE president) is against.

2.6. Other countries

Constitutional Courts in **Germany**[91] and **Austria**[92] ruled that the detailed regulations governing voting machines and internet voting for student elections breached constitutional principles and abolished them.[93] Supreme Courts in several nations, including India and Namibia, have been inspired by the German Constitutional Court decision and have mandated that the average person must be able to confirm that their vote accurately represents their choice and so VVPAT (voter verified paper audit trails) should be used, and/or that EMBs need to ensure the confidentiality of votes.[94] As for internet voting, no new regulations have been intro-

88. Dandoy R. and Umpierrez de Reguero S. (2021), E-voting and non-resident citizens' voter turnout: a quasi-experiment in Ecuador.
89. https://dig.watch/updates/alleged-cyberattacks-mar-online-voting-in-ecuador
90. Culnane C. et al., "Trust implications of DDoS protection in online elections": https://arxiv.org/abs/1708.00991
91. Germany, Constitutional Court (Bundesverfassungsgericht), Decision 2 BvC 3/07, 2 BvC 4/07, of 3 March 2009.
92. Austria, Constitutional Court (Verfassungsgerichtshof), Decision V 85-96/11-15, 13 December 2011.
93. Oswald M., "E-Voting in Austria: legal determination matters"; Seedorf S., "Germany: the public nature of elections and its consequences for e-voting", both in Driza Maurer A. and Barrat J. (eds) (2017), E-voting case law: a comparative analysis, Routledge, Abingdon.
94. NIRAS: Cost of election procurement, draft, 30 November 2022.

duced in Austria or elsewhere that would satisfy the requirement specified by the respective courts about ensuring the public control over the election by the individual voter or the member of the election commission without help from experts.

A recent (2023) study on internet voting by the German Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) for a dedicated Parliamentary Committee concluded that internet voting is not an option for the time being for elections at the federal or Länder levels in Germany.[95]

Countries like **Norway** (in 2011 and 2013) and **Finland** (in 2008) piloted internet voting but also decided to abandon the idea to introduce it.[96] A review of online voting in Finland in 2017[97] concluded that:

> *"the working group does not recommend the introduction of online voting in Finland, as the risks involved in the project currently outweigh the benefits. However, technological developments and the digitalisation of democracy should be closely monitored also in future".*

While recognising that internet voting contributes to greater inclusion than other channels, a review conducted in 2023 on behalf of the Ministry of Local Government and Regional Development of Norway noted that because it is not possible to guarantee the security of electronic solutions, there is a risk of a loss of trust. The report concludes that one option

> *"to ensure better accessibility for more people, while also limiting the risk of a loss of trust, is to offer electronic voting to only selected voter groups. Not because their vote is less important, but because a security breach will have lower economic and social costs in the form of reduced trust the fewer votes it affects".*[98]

A study in **Belgium** in 2020 and 2021 on the same question[99]concluded that internet voting for political elections is a very complex project. Security is crucial and countries have adopted different compromises between security and usability, however, no solution is convincing or satisfactory on both aspects. Security-related problems, in particular, remain open questions from an academic perspective. Such complexity is reflected at the industrial level as well with a very small number of players in the market for internet voting solutions for political elections. The study also discusses issues such as the electorate's habituation (and respective information efforts required) with advanced voting and distant voting; the important legal and possibly constitutional amendments required ahead of introducing internet voting as well as the important adaptations to the electoral timetable. As an intermediary solution between polling station and internet voting, the study proposes the development of postal voting assisted through the internet, with some elements being offered via the internet, namely access to the ballot, which eliminates the time necessary for sending voting material abroad. The ballot paper should be printed, filled in and sent by the voter via postal mail to the competent polling station. This however also requires adaptation of the legal basis and important communication and explanation efforts (see also section F, Excursus).

A 2018 **US** National Academies of Sciences report[100] concluded that at the present time the internet (or any network connected to the internet) should not be used for the return of marked ballots. Further, internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and are in place, as no known technology guarantees the secrecy, security and verifiability of a marked ballot transmitted over the internet. It further notes that US Election Assistance Commission standards and state laws should be revised to support pilot programmes to explore and validate new election

95. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), Main conclusions of the public discussion that took place on 6 April 2022 at the German Bundestag/Ausschuss für Bildung, Forschung und Technikfolgenabschätzung and Final report (2023): https://www.bundestag.de/dokumente/textarchiv/2022/kw14-pa-fachgespraech-bildung-882928

96. BBC, "E-voting experiments end in Norway amid security fears", 27 June 2014, https://www.bbc.com/news/technology-28055678; Vaalit Val, The electronic voting experiment: "an online voting system is technically feasible, but technology is not yet at a sufficiently high level to meet all the requirements. There are problems for example in the reconciliation of verifiability and election secrecy": https://vaalit.fi/en/electronic-voting1

97. Ministry of Justice, Finland, Online voting in Finland – Feasibility study, 19 December 2017.

98. Oslo Economics, Knowledge acquisition on electronic and internet-based solutions for voting, 27 June 2023.

99. Project Netvoting BE, Étude sur la possibilité d'introduire le vote Internet en Belgique, Part 1 (December 2020) and Part 2 (March 2021): https://elections.fgov.be/informations-generales/etude-sur-la-possibilite-dintroduire-le-vote-internet-en-belgique

100. National Academies of Sciences, Engineering, and Medicine (2018), Securing the vote: protecting American democracy, The National Academies Press, Washington, DC, https://nap.nationalacademies.org/catalog/25120/securing-the-vote-protecting-american-democracy

technologies and practices. Election officials are encouraged to seek expert and public comment on proposed new election technology before it is piloted.

3. Main legal requirements for i-voting and implications for Ukrainian legislation

A few legal requirements that should be included in national regulation of i-voting are described below with reference to international standards and practice.

3.1. Sufficient legal basis

International principles[101]

In some countries the voting method may be foreseen by the constitution (see, for example, Austria where the introduction of postal voting required a change in the constitution) and the question of modifying the constitution to introduce i-voting arises. In others (including Ukraine), the constitution does not cover the voting methods but contains the guarantees of voting rights which need to be upheld by all voting methods, namely the guarantees of free and fair elections. Hence the question of how to ensure that the i-voting regulation, to start with, is constitutionally compliant.

According to the legality principle, any use of i-voting that produces results which are binding for the authorities (as opposed to mock elections with non-binding results) should be legally regulated. Recommendation CM/Rec(2017)5 of the Committee of Ministers on standards for e-voting states:

> *"Member states of the Council of Europe shall develop technical, evaluation and certification requirements and shall ascertain that they fully reflect the relevant legal and democratic principles. Council of Europe member states shall keep the requirements up to date".*

The requirement of a sufficient legal basis has several implications. Lower-level i-voting regulations must respect higher-level electoral (and other) principles. I-voting-related decisions must be based on law. The law must present a certain level of quality and clarity. In the European heritage, clarity is linked to implementation. Regulations should be clear to make implementation possible. Whether they should be clear to the point of being understood by the layperson is an open question: Swiss i-voting regulation is complex and written to be understood by experts (whether this is constitutional or not is another question); the German Constitutional Court required that regulation on e-voting machines be clear to the layperson; whereas the Austrian Constitutional Court required that it be clear to the members of the Electoral Commission (who may face similar difficulties to laypersons). State bodies have a duty to implement the law. A regulation that is of poor quality (in terms of clarity) hinders the effective implementation of the law, hence the interest in evaluating its quality. According to the Venice Commission, the compatibility of postal and of i-voting with the principles depends, first of all, on adequate legal and regulatory provisions. In other words, the legal regulation and its quality (including the level of detail) are of greatest importance in ensuring the constitutional conformity of postal and internet voting.[102] Implementation may also be obstructed by the absence of sufficient sanctions or by the insufficient or selective enforcement of the relevant sanctions. Furthermore, rule of law and democracy require that the process for enacting the law is transparent, accountable, inclusive and democratic.

The normative level of i-voting provisions is also important. If the constitution forbids or limits voting from an unsupervised environment, i-voting from an unsupervised environment (for example home) can only be introduced after amending the constitution. According to the Venice Commission, the fundamental elements of electoral law should be written in the constitution or at a level higher than ordinary law. Delegation of legislative power to regulate i-voting to the executive requires that the objectives, content and scope of the delegation of power are explicitly defined in the legislative act by the parliament.

To ascertain the constitutional conformity of an i-voting regulatory framework and practice, a judicial review or other appropriate forms of review should be foreseen. States must ascertain that detailed requirements for

101. Based on Driza Maurer A., "Legality, separation of powers, stability of electoral law: the impact of new voting technologies", in Venice Commission/Romanian Electoral Authority, Electoral Expert, 2016.

102. Venice Commission/Grabenwarter 2004: § 56.

i-voting fully reflect the relevant democratic principles. However, this has not been straightforward in several countries, as the discussion of the cases of Switzerland, Estonia or France (above) shows. At the beginning of i-voting experiments, courts have hesitated or refused to proceed to a constitutional review when no irregularities in the voting itself were alleged. The difficulty or even impossibility of proving such irregularities has not been discussed. However, things might be evolving, as the above discussion on Estonia shows. Furthermore, legislation, typically criminal laws, should foresee adequate sanctions for i-voting-related violations, which in most countries would require amendments to the criminal law.

Stability of the law is an element of the principle of legal certainty. According to the Venice Commission, the fundamental elements of electoral law should not be open to amendment less than one year before an election.[103] The introduction of internet voting (or even of postal voting) involves several such decisions (voting ahead of voting day, for more than one day, from home, etc.). A rule of thumb says that when envisaging the introduction of i-voting one should think of the over-next election.

Situation in Ukraine

The use of digital technologies and special communications in Ukraine is subject to specific regulations. For instance, the exchange of information through a special information-analytical system may only occur through special secure and certified communication channels. The key regulatory act here is the Law of Ukraine on information protection in information and telecommunication systems. At the same time, there are a large number of bylaws and technical regulations (requirements) in this area which are often ignored in practice. National legislation on data protection and information security in general is not efficient enough. The key regulatory act here is the Law of Ukraine on personal data protection, which does not correspond either to the Council of Europe's[104] or the EU's GDPR standards.[105] There is no proper regulation of cyberthreats and risks to critical infrastructure. All digitalisation attempts so far have been of an experimental nature and not properly regulated.

For the time being, the use of innovative technologies in electoral process in Ukraine has a very general regulation laid down in Art. 18 of the Electoral Code. Herewith, there is no comprehensive regulation on internet voting. Should such a regulation be introduced, it must be enacted through a special law to be adopted by the parliament (as required by Article 92 of the Constitution of Ukraine). Article 116 of the Law on all-Ukrainian referendums provides for electronic voting, without, however, regulating it or referring to another regulation. E-voting has never been used so far. Article 116 is no sufficient legal basis for introducing internet voting in Ukraine. Besides, this Article shall come into force only on the day when special law on application of innovative technologies on electronic (machine) voting will come into force.

Ukraine has experience of implementing various digital tools. For instance, the Unified State Web Portal of Electronic Services operates based on the regulation outlined in the Cabinet of Ministers of Ukraine's resolution. However, there is no detailed regulation by law (no parliamentary act). This situation creates a risk of improper use of the personal data of Ukrainian citizens. It is essential to emphasise that Ukraine's existing legislation on this matter is severely limited, and the Law of Ukraine on personal data protection is outdated and requires substantial updating. Currently, the work on improving the legal framework and institutionalisation of the effective state control over the circulation of personal data is ongoing in Ukraine.[106] Relevant legislative drafts have been registered in parliament but have not been considered as of yet.

103. Section II.2.b of the Venice Commission Code of Good Practice stipulates that "the fundamental elements of electoral law, in particular the electoral system proper, membership of electoral commissions and the drawing of constituency boundaries, should not be open to amendment less than one year before an election". Paragraph 110 of the Venice Commission's Reflections on the Respect for Democracy, Human Rights and the Rule of Law during States of Emergency notes that "Making a change [to] the election code as regards voting modalities less than one year before elections may possibly be in accordance with the Code of Good Practice in Electoral Matters if it is necessary for, or contributes to, fair elections".

104. See, for example, https://rm.coe.int/legal-analysis-on-institutialisation-of-the-data-protection-independen/16809ee579

105. Ukraine 2023 Report – Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2023 Communication on EU Enlargement policy, Brussels, 8 November 2023.

106. Respective working group was established under the profile Parliamentary Committee on Human Rights, De-occupation and Reintegration of Temporarily Occupied Territories of Ukraine, National Minorities and Interethnic Relations and tasked with devising proposals to align personal data-protection legislation with international standards. Several draft law initiatives have been registered and are pending consideration by the Parliament of Ukraine (for example, draft law no. 8153, available (in Ukrainian) at: https://itd.rada.gov.ua/billInfo/Bills/Card/40707; draft law no. 6177 available (in Ukrainian) at: https://itd.rada.gov.ua/billInfo/Bills/Card/27996).

3.2. Vote from an uncontrolled environment and for more than one day

International principles

Internet voting (except what is called "kiosk voting", which is organised in kiosks set up by election authorities) takes place from an environment outside the control of the electoral authorities. The law should provide for such a possibility. Furthermore, the law should introduce legal and regulatory provisions which need to ensure that principles are upheld given that any channel other that polling stations introduces risks and should be accepted under certain conditions only (some democracies subject any votes from uncontrolled environments to certain conditions). Similar to voting from an uncontrolled environment, voting before election day introduces certain risks and is accepted under certain conditions which aim at guaranteeing the relevant constitutional principles.

Situation in Ukraine

National legislation does not provide for voting from an uncontrolled environment. The only vote from an uncontrolled environment is voting at special polling stations (in hospitals, for instance). However, during previous electoral campaigns in Ukraine, there has been concern about a significantly higher risk of violating electoral legislation by voting from special polling stations compared to voting at regular polling stations. As a result, trust in election results where a large number of voters votes at special polling stations and/or from home is substantially lower.

Furthermore, the Constitution of Ukraine clearly defines elections as taking place on a Sunday (Article 77, which prescribes that regular elections to the Verkhovna Rada of Ukraine shall be held on the last Sunday of October of the fifth year of the term of the Verkhovna Rada of Ukraine; similar provisions exist for the election of the President of Ukraine and local elections). Therefore, organising voting over several days would formally contradict the Constitution of Ukraine. Furthermore, considering Ukrainian experience and the experience of certain post-Soviet countries, allowing multiple days for voting facilitates falsifications and violates the constitutional principles of electoral rights.

The Constitution of Ukraine does not provide such a discretion for the parliament to introduce voting from an uncontrolled environment (for example home) during an extended voting period (more than one day) (see the following provisions of the Electoral Code: Article 5 on voting day; Article 173 on organisation and voting procedure; Article 174 on the procedure for organising voting by place of residence; Article 17 on personal voting; Article 62 on premises of precinct election commission and voting premises). Hence, to introduce voting from an uncontrolled environment and for an extended voting period, respective changes in the constitution are necessary. According to Civil Network OPORA, any doubts on the constitutionality of early voting and voting for more than one day might be lifted by the Constitutional Court. Suggestions to have internet voting taking place on one day, on election day, from 8 a.m. to 8 p.m. (local time) are criticised.[107] As illustrated by the Ecuador example, this is not only against good practice but means, almost with certitude, that the system will be targeted by DDoS attacks.

3.3. Security

Security is not a specific electoral principle but an overarching one: it is the assurance that all principles that apply are correctly implemented in the regulation and in the system and are respected during the effective use of the system. Technical evaluations address security properties like integrity, authenticity, availability, secrecy or confidentiality, the verifiability of votes, information or voting systems, security evaluations and trust assumptions, as discussed in the Council of Europe Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States.

107. See IFES Ukraine (2023b) which emphasizes that the introduction of Internet voting in one day carries the risks of server overload and system failures, which will negatively affect the trust in the voting results.

Voter identification

International principles

Council of Europe Recommendation CM/Rec(2017)5 on standards for e-voting states that "unique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured". It also defines voter authentication as "the provision of assurance of the claimed identity of a person or data".

Situation in Ukraine

The CEC keeps a record of voters in the State Voter Register (SVR), which is regulated by a separate Law on the State Voter Register.[108] Article 119 of the Electoral Code prescribes the procedure for organising voting in places where voters are staying. The SVR contains information on a voter's official place of residence, which is periodically received from local authorities (local councils, territorial bodies of the Ministry of Justice, etc.). The operation of the State Voter Register was temporarily suspended by the CEC on 24 February 2022 to preserve the integrity and inviolability of voters' personal data.[109] The CEC has carried out a test launch of the State Voter Register and has announced work to restore the functioning of the SVR by approving periodic updating of the SVR database.[110]

Different stakeholders recommend going from passive to active registration for OCVs: voters submit a statement of intention to vote abroad and provide information on their place of stay and or contact details (phone, e-mail). This requires important information efforts in addition to registering such information and keeping it up to date.

Since 2019, IDPs and other voters have had the right to change (in the State Voter Register) at their own discretion their voting address. It can be done online without additional conditions or restrictions, using a qualified digital signature. However, this process is valid only for residents. There seems to be a growing consensus to also allow OCVs to temporarily change their voting address. But this will require changes in the legislation. Stakeholders note that the law should foresee a sufficient period of time before the election, for example 15 days, when such changes are no longer possible to allow the administration to control and consolidate registers and issue printed versions of voter lists for precinct election commissions.

Another issue is that of authentication of a voter, that is, verification that a person is indeed the voter he/she pretends to be. Many forms of e-ID and digital signature providers exist but there is no central control to avoid duplications. In the past, authentication could be done through applications like Diia, which was deemed a success in technical terms. But it could not mitigate for problems such as the use of fake signatures and the delegation of signatures (entrepreneurs, for instance, delegate their signature to accountants for business purposes). It is not known whether any such cases were prosecuted, let alone punished. Furthermore, it is not known how providers like Diia are working on technically solving the problems. Their codes are not published and it is unknown whether there is co-operation with external experts. Hence, some interlocutors interviewed (Civil Network OPORA) recommend keeping the in-person registration at the embassy as one among possible solutions. Herewith, the competent Ministry of Foreign Affairs refers to previously and currently insufficient resources for that purpose.

During the last election, there were no complaints from domestic or international observers about the accuracy of the State Voter Register. The OSCE/ODIHR noted the good work of the State Voter Register and the good quality of the voter lists.[111]

Voters' authentication in polling stations is done manually using identity documents (see Article 173 on the organisation and voting procedure and Article 8 on documents confirming a voter's identity and citizenship of the Electoral Code). In recent years, the CEC has been studying the possibility of introducing electronic identification of voters in polling stations.

108. https://zakon.rada.gov.ua/laws/show/698-16#Text (in Ukrainian).

109. CEC Resolution No. 61 of 24 February 2024, available (in Ukrainian) at https://zakon.rada.gov.ua/laws/show/v0061359-22%23Text

110. https://cvk.gov.ua/novini/tsvk-uhvalila-rishennya-pro-chastkove-vidnovlennya-funktsionuvannya-derzhavnogo-reiestru-vibortsiv.html (in Ukrainian).

111. OSCE/ODIHR, Ukraine Local Elections, 25 October 2020, ODIHR Limited Election Observation Mission, Final Report, Warsaw, 29 January 2021, p. 14; ENEMO (European Network of Election Monitoring Organisations) International Election Observation Mission – Local Elections, Ukraine, 25 October 2020, Statement of preliminary findings and conclusions, p. 7; Council of Europe Congress of Local and Regional Authorities, Information report on the local elections in Ukraine, 25 October 2020.

Verifiability

International principles

A voter has the right to express his or her opinion in a free manner, without any coercion or undue influence. Recommendation CM/Rec(2017)5 requires that:

> *"the voter shall be able to verify that his or her intention is accurately represented in the vote [cast-as-intended] and that the sealed vote has entered the electronic ballot box without being altered; any undue influence that modifies the vote shall be detectable [recorded-as-cast]" (Appendix I, paragraph 15).*

Cast-as-intended and recorded-as-cast are also known as individual verifiability. Furthermore,

> *"the system shall provide sound evidence that each authentic vote is accurately included in the respective election results and such evidence should be verifiable by means that are independent from the e-voting system" (Appendix I, paragraph 17),*

also known as tallied-as-recorded.

> *"The system shall provide sound evidence that only eligible voters' votes have been included in the final result. The evidence should be verifiable by means that are independent from the e-voting system" (Appendix I, paragraph 18),*

also known as eligibility verifiability. These requirements are also known as universal verifiability. Standards laid down in paragraphs 15 to 18 of Appendix I introduce verifiability mechanisms which develop the concept of a chain of trust in e-enabled elections. They do not prevent potential manipulation of the vote but may allow verification that the vote and the overall result have not been tampered with. The use of such techniques should respect the confidentiality of the vote: individual verifiability tools should not be used to prove one's vote. Individual verifiability can be implemented provided adequate safeguards exist to prevent coercion or vote buying. Also, there should be clear regulations on how to proceed in cases where verification shows that the vote has been tampered with.

Situation in Ukraine

The verifiability techniques described above are relatively new and specific to e-voting. With respect to "traditional" voting channels, good organisation (for example, the "four eyes principle") and meaningful observation (chain of custody) are the main ways to ensure confidence in the result. References in the Electoral Code include Article 168 (election ballot); Article 169 (procedure for production of election ballots); Article 170 (the procedure for transferring election ballots to election commissions); Article 178 (the procedure for transporting and transferring election documents to the district election commission or the Central Election Commission (for a foreign constituency)); Article 179 (procedure for acceptance and consideration of documents from precinct election commissions by the district election commission).

In Ukraine, election commissions only do manual counting of ballots (Article 175 of the Electoral Code on the procedure for counting votes at the polling station). The counting of votes at polling stations is carried out by members of precinct election commissions nominated to these commissions by political parties and candidates. Official observation can be carried out by the observers representing candidates, parties (local party organisations) participating in the election process, civil society and international organisations authorised to provide official observers (Articles 58 and 59 of the Electoral Code on official domestic and foreign observers; Article 167 on official observers from the parties). Domestic observation plays an important role in Ukraine as it enables civil society to carry out public oversight of the electoral process and its compliance with the national legal framework as well as international standards and good practices.

Vote secrecy

International principles

Recommendation CM/Rec(2017)5 introduces a general requirement of secrecy of the vote which applies throughout the entire procedure: there should be no way of establishing a link between the voter and the vote (Appendix I, paragraph 19). "An e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties" (paragraph 23). Secrecy also covers intermediary results which should be not established or published (paragraph 24) and previous (deleted) choices (paragraph 25); the counting

stage in particular should be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter (paragraph 26); and where the number of (i-)votes is particularly small, aggregation methods should contain the necessary technical and procedural safeguards to ensure consolidation of results before results are disclosed, thus ensuring secrecy.

More generally, the voter has the right to vote secretly, and the state has the duty to protect that right. Secrecy must be ensured towards the authority that organises and conducts the voting process, including any company that may operate the system or its components (applications, verification servers, etc.). Protection must be in place against third parties (family, friends or any others who illegally observe the voter's computer) as well. The first type of secrecy, concerning the authority, is absolute. The extent to which the voter may give up the right to secrecy where family or friends are concerned is matter of debate. The extent to which the voter may give up secrecy rights when it comes to malware installed on their computer (of which the voter is usually unaware of) has not been addressed by legal research. Constitutional law experts are generally adamant that all aspects of secrecy should be preserved. Yet, this issue has so far not been clarified. The law should clarify the level of secrecy required and this necessitates first an informed public debate.

Situation in Ukraine

National legislation establishes stringent requirements for ensuring the secrecy of the vote. Voting should take place by secret ballot. It is prohibited to control the content of voters' expression of will and to establish or disclose the content of a particular vote in any manner. While the voting ballot is being completed, the presence of other persons or any type of photo or video recording are prohibited. The Criminal Code of Ukraine provides in Article 159 legal liability for the violation of voting secrecy. The practical application of this article is extremely limited, primarily serving a more preventive role. The Criminal Code of Ukraine imposes liability for the illegal use of the voting ballot (in an election or referendum), namely for voting more than once, theft, damage, concealment or destruction of the ballot (Article 158-1). This provision aims to prevent non-personal voting.

National legislation stipulates that every voter must vote in person. Voting for others or transferring the right to vote to any other person (proxy) is prohibited. The only exception to the requirement of personal voting is assistance to individuals with health problems who cannot fill out the voting ballot or cast it in the ballot box by themselves as a result of disability and/or poor health.

There have been very few complaints about the violation of voting secrecy in recent elections. However, some difficulties with these norms arose during voting outside regular polling stations.

Vote buying constitutes a criminal offence. Article 160 of the Criminal Code establishes liability for the bribery of a voter in an election or referendum, or of a member of an electoral/referendum commission. Criminal sanctions apply to the acceptance of a proposal and the promise or receipt of any unlawful benefit, whether of a material or non-material nature. The practice of applying this article and the number of cases of actual prosecutions of individuals responsible are negligible.

Electoral legislation also includes a series of restrictions to prevent the misuse of administrative resources in elections or other abuses of authority. However, the practice of countering corresponding criminal manifestations is rather patchy. During the recent elections, there were no direct attempts of bribery identified. However, indirect forms of incentivising voters to support certain candidates are encountered extremely frequently.

National legislation does not provide detailed regulation concerning coercion-resistance. Serious examples of compelling individuals to vote or forcibly voting for specific candidates during recent election campaigns have not been formally identified. At the beginning of Ukraine's independence, cases of electoral rights violations in prisons and other facilities with restricted access were quite widespread. There were often instances of compelling individuals to vote for certain candidates. However, during recent election campaigns, such have not been publicised or documented.

According to domestic observers,[112] vote buying is a huge problem in Ukraine and combating electoral fraud among OCVs is a major preoccupation. Stakeholders fear that i-voting will take away the existing transparen-

112. Interview with representatives of Civil Network OPORA held on 1 December 2023.

cy of both voting and counting. It is also feared that the judicial system will not be able to cope with the challenges of i-voting.

Multiple voting is not allowed in Ukraine. It would contradict the requirements of equal, secret and personal voting (Article 71 of the Constitution of Ukraine, Articles 12, 16 and 17 of the Electoral Code of Ukraine). In practice, there have been numerous cases of multiple voting in the past (for example, in the 2004 Presidential elections). The majority of attempts at abuse were curtailed after the introduction of the State Voter Register in 2007. The effectiveness of forming the State Voter Register and the procedures for preparing voter lists for each precinct in a centralised manner have prevented large-scale abuses in this regard. During recent electoral campaigns (since the 2014 Presidential elections), no such abuses were identified according to international and domestic election observation reports. Therefore, it is critically important to restore the operation of the State Voter Register in its previous format with improvements to certain procedures and responsiveness to post-war challenges in the first post-war elections.

Trust assumptions

International principles

The concept of trust assumptions, their disclosure and the evaluation of their realistic nature is important, although this is a subject that has only recently been addressed by Council of Europe instruments (see the 2022 Guidelines on ICT in elections). The security of all voting solutions, be they paper and manual or ICT backed, usually relies on some assumptions. It is assumed that users will interact in a certain manner with the voting solution, that potential attackers will only have certain capabilities, that certain parts of the system should be trusted, etc. Only if the underlying assumptions hold true can the legal principles and requirements that apply to internet voting be ensured. If the assumptions are not realistic, they will very likely not hold true in practice and thus the applicable constitutional principles, namely those of free and democratic elections, will not be respected. Making assumptions explicit enables more informed discussions by experts and better-informed decisions by election officials. Furthermore, assumptions should be analysed as part of the regular risk assessment (see in particular guidelines 1 and 9 in the above-mentioned Council of Europe 2022 Guidelines on the use of ICT in electoral processes).

Situation in Ukraine

Presumably this topic (the concept of trust assumptions, their disclosure and their evaluation) is not currently discussed in Ukraine at the level of relevant stakeholders. It is however important to be considered in particular if internet voting is envisaged. The internet voting provider should be ready to disclose and discuss the assumptions with decision makers.

Reliable alternative channels

International principles

Paragraph 3 of Appendix I in Recommendation CM/Rec(2017)5 states that unless i-voting is universally accessible, it shall be only an additional and optional means of voting. Additionally, as mentioned in the Estonian context above, maintaining a voting channel in addition to internet voting is necessary to offer voters the possibility to vote in privacy (multiple voting in Estonia). It is furthermore necessary as a fall-back voting channel if voters are unable to vote online because of technical problems or if the individual verification shows that their vote was not registered as intended (cf. legal requirements in Switzerland). The polling station option should always remain available.

As shown in the examples of Estonia and Switzerland, individual verifiability requires a second channel for verification purposes. This can be the postal channel (Switzerland), smartphones (Estonia) or another channel. This means that an internet voting channel is not enough; a second communication channel is necessary for verifiability purposes, with the additional costs that this entails.

Situation in Ukraine

It is unclear to what extent proponents of i-voting in Ukraine agree with the necessity of maintaining polling station voting in addition to i-voting and with the necessity of having a different communication channel for

verification purposes.[113] If there is no fall-back channel, namely polling station voting, it would be impossible to implement i-voting in line with international standards.

Quality and transparency of the security evaluation and of controls

International principles

The Council of Europe recommends transparency in all aspects of e-voting and considers it a means for building public trust and confidence in the electoral system and in election administration. Being transparent about the e-voting system, the processes surrounding it and the reasons for introducing e-voting will contribute to voters' knowledge and understanding, thereby generating trust and public confidence (paragraph 31 of Appendix I of Recommendation CM/Rec(2017)5). According to the Council of Europe's standards, trust in the electoral administration is a prerequisite for the use of ICT in elections (preamble to CM/Rec(2017)5).

Ways to be transparent include clearly informing voters (paragraph 32), disclosing critical elements of the system to independent evaluation (paragraph 33) and allowing observers, to the extent permitted by law, to verify that the e-voting system itself is designed and operated in a way which respects the fundamental principles of democratic elections and referendums (paragraph 34).

EMBs should develop technical requirements for e-voting systems and their evaluation and ensure that they fully reflect the relevant legal principles for democratic elections (paragraph 36). A number of controls are recommended (see paragraphs 42 and 43).

Situation in Ukraine

Public oversight of elections has several levels. Primarily, this involves the opportunity for independent observation of the electoral process. All types of elections in Ukraine provide for the possibility of activity by official observers. The Electoral Code outlines three types of official observers: from candidates and parties (local party organisations) participating in the election process; from non-governmental organisations authorised to provide official observers for the respective elections; and from foreign states and international organisations. Official observers have a fairly broad spectrum of rights that cover all stages of the electoral process, allowing them to directly observe (including taking photos and videos and making documentary recordings) procedures and react (by submitting statements and complaints) to identified violations. In practice, the activity of observers varies, but their presence in most cases enables the prevention of certain violations or the proper documentation of violations that have already occurred. Official observers from non-governmental organisations are the most active and often document violations, file relevant complaints with election commissions and, in some cases, initiate legal challenges.

Media activity, according to the Electoral Code of Ukraine, is divided into two components: information support for elections and participation in campaigning. Information support includes not only informing about candidates and the voting process but also the opportunity to be present at polling stations, during the vote count and when establishing election results. The presence of the media often serves as a deterrent against abuse and falsification.

In the 2012 parliamentary elections, Ukraine implemented an interesting experience of online broadcasting of the voting process from each polling station. Online observers could not only witness the voting but also observe the vote count and the establishment of election results. While this was a costly project, legally the results of such video surveillance did not serve as the basis for legally significant decisions. The violations identified and recorded by cameras were not subsequently used by the courts. Therefore, this experience was highly ineffective, and the project was abandoned immediately after its completion.

According to reports from international election observation missions,[114] the level of openness and transparency in administering elections is well regulated. In practice, the majority of provisions of the Electoral Code

113. IFES Ukraine (2023b) considers online voting as one of three alternative voting methods in addition to expanded in-person voting and postal voting, focusing on the advantages and disadvantages of each method in the context of exercising electoral rights. Moreover, each of these voting methods is considered in the report as an alternative in addition to the existing in-person voting mechanism.

114. OSCE/ODIHR, Ukraine Presidential Elections, 31 March and 21 April 2019, ODIHR Election Observation Mission, Final Report, Warsaw, 20 November 2019; OSCE/ODIHR, Ukraine Early Parliamentary Elections, 21 July 2019, ODIHR Election Observation Mission, Final Report, Warsaw, 20 November 2019; OSCE/ODIHR, Ukraine Local Elections, 25 October 2020, ODIHR Limited Election Observation Mission, Final Report, Warsaw, 29 January 2021.

of Ukraine are duly followed, but occasionally there are relatively gross violations (though not widespread, they are often quite prominent).

Meetings of election commissions at all levels are open. The meeting agendas must be announced in advance and relevant materials should be provided for review, not only to the commission members but also to other interested parties (such as candidates and their representatives, official observers, the media, etc.). Decisions of the election commissions are drafted and posted on official boards in their premises. Additionally, decisions must be transmitted for publication on the website of the Central Election Commission.

Specific procedures are established for the meetings of all election commissions regarding the vote count and the establishment of election results. At this stage, there is a limited list of individuals who can be present at such meetings. However, legislative restrictions are proportionate and quite effective. In addition to commission members, candidates, their representatives, official observers and media representatives can also be present.

Nonetheless, in practice, there have often been misunderstandings over the application of the provisions of the electoral legislation regarding transparency and openness. Sometimes, because of objective circumstances or a lack of professionalism, these requirements have been violated or ignored. This issue was particularly acute in local elections.

3.4. Effective dispute resolution

International principles

Effective dispute resolution is an important electoral principle included in the Venice Commission Code of Good Practice in Electoral Matters. It is not specifically mentioned in Recommendation CM/Rec(2017)5 but the recommendation provides a reminder about the legal consequences of different breaches. The term "effective" relates not only to the possibility to have access to a judge but also to the judge's understanding of the issues and possibility to make a rapid and well-founded decision. As mentioned above (Estonia, Switzerland, Belgium), i-voting is highly complex and, furthermore, providing evidence of irregularities and of their impact on the final results – as requested when other voting channels are used – may be impossible for i-voting. Another question is what happens if verifiability shows that the vote was tampered with? Currently, for instance, Swiss regulation stipulates that the voter must contact the authority to inform them about the failed verification and must be given the right to vote through another channel. What if the voter raises such queries after the election? What if he/she is not eventually allowed to vote through the second channel? Effective dispute resolution in i-voting remains an area of open legal questions where further research is needed.

Situation in Ukraine

As part of the judicial reform, an electronic court web-platform system (Unified Judicial Information and Telecommunication System) was launched in Ukraine in 2019,[115] which provides for the exchange of procedural documents in electronic form between the courts and institutions of the justice system, the court and the participants in the trial and the participants in the trial themselves. Litigants can file procedural documents (claims, motions, etc.) in electronic format. Upon successful submission, the litigant can track the motion and status of their case in court. Information on the delivery of the document, its registration and other information is sent to the electronic cabinet of an applicant in automatic mode. If internet voting is used, it is expected that this platform might also be used for electoral dispute resolution.

Some interlocutors interviewed[116] noted that post-war elections will be even more challenging than "regular" elections. Therefore, any new procedures, first and foremost related to digital solutions, need to be piloted before their actual introduction into the electoral process. More challenges might arise with election dispute resolution and ensuring accountability for electoral violations in cases of out-of-country voting. Ensuring prosecution and extending Ukrainian jurisdiction to polling stations abroad is subject to agreements with other states for polling station voting. Such co-operation is necessary for prosecuting i-voting-related fraud abroad as well. It is however much more difficult to achieve.

115. The Law of Ukraine on the judiciary and the status of judges, adopted on 2 June 2016, provided for the introduction of a Unified Judicial Information and Telecommunication System, which was launched as a test regime in 2019. Since 18 October 2023, the presence of an electronic account in UJITS became mandatory for the participants in civil and administrative proceedings.

116. Civil Network OPORA.

3.5. Co-ordination and co-operation among institutions and allocation of responsibilities

International principles

The Council of Europe recommends that the electoral management body shall be responsible for the respect for and compliance with all requirements even in the case of failures and attacks. The EMB shall be responsible for the availability, reliability, usability and security of the e-voting system (paragraph 40 of Appendix I of CM/Rec(2017)5). This is also the case when the system is developed and operated by a private supplier. The overall responsibility falls on the EMB and cannot be delegated, for instance to a voting system supplier. Furthermore, competent authorities should remain in command of the electoral process and should not outsource essential parts of it to vendors.

States should devise a clear framework for the institutional responsibilities as well as those of all other actors involved. Private entities may be involved to different degrees in providing i-voting solutions. The regulatory framework should guarantee that non-state entities are subject to the requirements of the rule of law and accountable in a manner comparable to those of public authorities.

Situation in Ukraine

The introduction of electronic voting must have a proper regulatory framework. An integral element of such regulation should be the mechanism of interaction between the Central Election Commission and other government bodies which may be involved in i-voting.

In this respect, there is already some experience of digitisation. For example, the establishment of the State Voter Register in 2007, with the support of the OSCE, was an extensive and ambitious project. Despite all the challenges, the Central Election Commission successfully organised the operation of this register, which is still considered one of the most comprehensive databases of Ukrainian citizens. The parliament often imposes obligations on the Central Election Commission to provide temporary access to the register to other government bodies when adopting new legislative changes. This experience serves as a good foundation for piloting an electronic interaction system with other government bodies.

Testing e-voting will require a significantly different scale of work. The Central Election Commission will need to have a key role in controlling the respective process. With regard to piloting and introducing e-voting, the CEC Secretariat should possess sufficient expertise, as well as corresponding financial and technical support.

The current allocation of competences and responsibilities between the CEC and other state institutions, including the Ministry of Digital Transformation of Ukraine, the Ministry of Interior of Ukraine, the Ministry of Foreign Affairs of Ukraine and other state or regional authorities, regarding the organisation and conduct of elections is addressed by the Law of Ukraine on the Central Election Commission, section III, Powers of the Commission, Article 17, General powers of the Commission; Article 18, Powers of the Commission regarding the organisation of preparation and conduct of the elections of the President of Ukraine; Article 21, Powers of the Commission regarding the organisation of preparation and holding of elections of deputies of the Verkhovna Rada of the Autonomous Republic of Crimea, deputies of local councils, villages and settlements, and city mayors.

The organisation and conduct of elections in Ukraine have always been accompanied by significant political activities. The current model of organising and conducting elections represents a delicate balance between political players, state authorities and society as a whole. As a result, Ukraine has managed to conduct several election campaigns and there have been no serious questions about their democratic nature and openness, either within Ukraine or among international partners. This is of significant value, as not all post-Soviet countries and countries in transition to democracy have been able to find such a balance. Elections in Ukraine have led to democratic changes in power several times. Considering this, the key institutional elements of election administration functioning must be preserved and developed and any changes should be made extremely carefully. It is critically important not to disrupt this fragile balance.

Regarding the organisation of voting and counting, several important points should be emphasised.

The work of the Central Election Commission is often criticised and politicised. However, such a model of a collegial body provides, on one hand, the opportunity to represent the interests of various political players, and on the other hand, it allows achieving a certain level of professionalism and objectivity in electoral procedures. It is crucial not to shift the balance in favour of the government or individual political players. Estab-

lishing an electoral model where the influence of the executive branch is minimised has been a challenging process in Ukraine. Therefore, attempts to strengthen certain ministries' roles in the electoral process (be it the Ministry of Digital Transformation, the Ministry of Foreign Affairs or others) will undermine the independence of the Central Election Commission as the main body responsible in Ukraine for the organisation and conduct of elections.

Mechanisms for administering elections through the system of election commissions need some improvement. The current advantage of administering elections by commissions entirely composed of representatives of political parties is the higher level of trust in their work. However, political delegation of candidates often turns the work of such commissions into a political forum. Another significant drawback is the lack of professionalism in election commissions which, in many cases, results from the last-minute replacement of election commissioners by nominating political parties. Therefore, it is essential to review the mechanisms for forming election commissions, preserving trust in the formation process while increasing professionalism.

3.6. Voter education and training of officials

International principles

The Recommendation CM/Rec(2017)5 includes a recommendation (vi) to member states to translate and disseminate the recommendation as widely as possible to all involved stakeholders, including officials and citizens, and to raise awareness about the issues. The OSCE/ODIHR Handbook on the observation of new voting technologies underlines the key obligations of training officials and educating voters.[117] The idea is that voters should be able to make their choices and cast ballots without assistance and officials should have a basic understanding of how the system works in order to respond to potential technical problems, to explain the technology and answer questions about its use, to inform voters and help build their confidence in the system. Special attention should be given to providing education materials in minority languages. The OSCE/ODIHR notes that ideally the new system should have been tested by voters before election day (for example by organising mock elections as an education tool).

Situation in Ukraine

Voter information and education is well regulated by the current legislation. Recent CEC activities are quite effective in terms of educating voters, as proved by the 2020 local elections.[118] The CEC has also developed numerous awareness-raising materials under the umbrella of the "CEC: prosvita" awareness raising online platform. Some efforts to increase computer and internet literacy have been made by the Ministry of Digital Transformation of Ukraine via its online platform "Diia. Education" and the creation a series of awareness-raising videos (there are some dedicated to digital literacy as well as to local elections).[119]

However, unfortunately, a significant part of society has very limited knowledge and skills in the field of digitisation.[120] A quick transition to other formats may lead to the exclusion of a considerable proportion of society from the electoral process and political discourse in general, which will be particularly crucial in the post-war period. Hence, the main method of voting in elections in Ukraine will remain paper ballots for a long time.

While maintaining the use of paper-based voting, other crucial processes related to the counting of votes and the determination of election results need further development and support. It is critically important to investigate the automation of processes like the completion of protocols by election commissions and the transmission of information to higher-level commissions. These aspects of digitising Ukraine's electoral administration are developing quite confidently and need continued support. Such steps should be taken with the aim of enhancing the openness and transparency of the work of all subjects administering elections.

117. OSCE/ODIHR, Handbook for the observation of new voting technologies, Warsaw, 1 October 2013.

118. OSCE/ODIHR, Ukraine Local Elections, 25 October 2020, ODIHR Limited Election Observation Mission, Final Report, Warsaw, 29 January 2021.

119. https://osvita.diia.gov.ua/courses

120. According to the 2023 Digital Literacy Research in Ukraine (available at https://osvita.diia.gov.ua/research), conducted by the Ministry of Digital Transformation of Ukraine, 38% of the adult population of Ukraine has above basic digital skills and 40.4% of the adult population of Ukraine has a digital skills level below the basic level.

Ensuring a high level of trust in all electoral procedures, not just voting and election results, is critically important. In Ukraine, political and legal disputes often arise during the nomination of candidates, their official registration, the production and printing of ballots, etc. It is crucial to add openness and transparency to these stages as well. Election commissions must operate under rules that minimise administrative discretion abuse.

3.7. Costs

International principles and practice

Paragraph 27 of Appendix I of Recommendation CM/Rec(2017)5 notes that member states that introduce e-voting shall do so in a gradual and progressive manner. The guidelines related to the implementation of this recommendation note the importance of organising formal feasibility studies which must contain, among other things, a cost-benefit analysis. Furthermore, all standards introduced by the recommendation require that the member state has the adequate budgetary and human resources to ensure their implementation and respect.

Identifying the costs related to internet voting is very difficult for several reasons. Complex systems like i-voting include many components whose costs may be difficult to retrieve; the costs of the alternative systems (for example postal voting or polling station voting) are not readily available either so it is difficult to compare costs. It is difficult to calculate the cost of "remaining risks", namely the financial implications of risks if they materialise. Furthermore, the cost of implementing internet voting can vary significantly depending on the scale of the election, the technology used and the specific security measures implemented. Developing and maintaining a secure and reliable internet voting system involves substantial expenses related to software development, infrastructure, testing and ongoing security measures. Governments considering internet voting need to invest in robust cybersecurity measures to protect against potential threats and ensure the confidentiality and accuracy of votes and need also to include ongoing maintenance and support costs. Security threats and solutions evolve over time, and this may have important financial repercussions. Furthermore, good security practices such as public scrutiny, the examination by mandated experts, bug bounties, etc., involving competent experts worldwide, attract additional costs. Related costs like the costs of maintaining a fall-back, paper-based option (polling station voting) as a security measure and the cost of providing a second communication channel for verifiability purposes should also be accounted for. Costs not directly associated with the technological solution of internet voting include public awareness campaigns, training for election officials and ongoing media outreach to sensitise the electorate and political parties and build trust about the security of an internet voting system. With these caveats in mind, existing experiences in some countries are referred to below.

In Estonia, a study of internet voting[121] concluded that the adoption of multi-channel electoral systems poses new challenges to election administrations (in terms of workload, vulnerability to double voting, length of the voting period, overlapping voting periods, etc.). The study also proposes a methodology aimed at delivering comparative results of the costs of different voting channels for multi-channel electoral systems. By applying their method to one specific election (local elections 2017) in Estonia, the study found that i-voting was the cheapest voting channel proposed at that specific election because of its acceptance by citizens and the reduced costs involved in deployment; however, the conclusions are valid for that specific election alone. A change of voters' electoral behaviour in further elections (for example having fewer i-voters) would impact the distribution of costs by changing them substantially. The methodology allows an assessment of the administrative costs of running elections, however the authors of the Estonian study note that the debate on its suitability can be re-focused on other dimensions, namely on trust and security. The proposed methodology however does not consider the technical or legal merits of the solution and does not account for costs associated with the potential materialisation of risks and follow-up measures on issues that may be discovered by audits, verification, etc. Importantly, it does not include the costs related to maintaining polling station voting in parallel to i-voting, which, according to the Supreme Court of Estonia, is mandatory given that the possibility of overriding votes, including a paper vote eventually overriding an internet vote, is considered by the court as the only solution capable of ensuring acceptable levels of coercion resistance and is a condition for accepting i-voting.

121. Krimmer R. et al. (2018), "How much does an e-vote cost? Cost comparison per vote in multichannel elections in Estonia", in Krimmer R. et al., E-Vote-ID 2018 Proceedings, TUT Press.

A more recent Estonian study which discusses evidence from eleven elections (2005-2019)[122] concludes that internet voting complicates election administration instead of simplifying it. By deploying i-voting, governments take on a long-term obligation to develop technology, build legal frameworks, adjust election administration and defend the system against attacks, criticism and disinformation in both the domestic and international arena; the challenge of deploying i-voting and administering it in parallel with the conventional paper-based voting system should not be underestimated. In sum, the Estonian experience suggests that large-scale deployment of i-voting increases administrative complexity and augments the workload of electoral authorities. This means that countries with significant election administration problems and understaffed or underfunded electoral authorities should refrain from deploying remote internet voting on a large scale. Online voting should be seen as an advanced service, as opposed to a quick fix to existing problems.

In Switzerland, experts estimated the costs of independent control components, the cost of implementing an independent verifier and the one-off costs for adapting the cryptographic protocol, among other things.[123] The experts advocate the use of manufacturer-independent software for the important components ("control components" and "verifiers"), which entails higher costs and leads to greater complexity in the operation of the system but brings added value. In relation to an improved second-generation system, the study lists the following costs: manufacturer-independent verifier and control components (very high costs), the weakening of trust assumptions in the printing process (high costs) and a public bulletin board (high costs). According to another Swiss study, despite some savings, paperless e-voting does not necessarily result in overall savings as fixed costs can outweigh or exceed these savings.[124] The study concludes that the federal government cannot expect any substantial savings in the medium term. At the cantonal level, Geneva eventually stopped its i-voting system in June 2019 because of the financial impossibility of covering, alone, the development of its system in accordance with evolving federal requirements. The costs involved in securing an i-voting system are a major issue for cantons when envisaging the potential introduction of i-voting.

In Australia,[125] no internet voting took place in the 2022 federal election, but forms of electronic voting exist in some states and territories but generally only for particular groups of voters. Without a significant and sustained investment in secure, reliable and robust internet platforms, this is likely to remain the case.[126] The estimation of potential cost savings with the introduction of internet voting depends on the opportunities to offset costs with savings and may be limited in the short term as it may not be clear in advance how many voters will actually use it and how long the adapted internet voting will be in use.

In France,[127] about 1.43 million voters registered in the 11 constituencies representing French citizens living abroad could vote online during the 2022 elections, but several technical and computer malfunctions prevented many citizens from exercising their right, and this resulted in the re-run of elections in two districts with additional costs due to the system errors. Claims by the industry that the scalability of such systems facilitates economies of scale[128] and that online voting entails cost savings compared to paper voting, and especially compared to postal voting, do not consider malfunctioning. I-voting was still the preferred mode of

122. Ehin P. et al. (2022), "Internet voting in Estonia 2005-2019: evidence from eleven elections", in Government Information Quarterly 39 (2022), https://doi.org/10.1016/j.giq.2022.101718

123. Swiss Federal Chancellery, Redesign and relaunch of trials – Final report of the Steering Committee Vote électronique (SC VE), p. 14, www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/berichte-und-studien.html

124. Swiss Federal Chancellery, Expert Group Vote électronique, final report in German: Schlussbericht Expertengruppe elektronische Stimmabgabe EXVE, April 2018, p. 34, available at www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/berichte-und-studien.html

125. "iVote, the 2021 NSW government elections and the future of internet voting", in Australian Public Law: https://www.auspublaw.org/blog/2022/06/ivote-the-2021-nsw-government-elections-and-the-future-of-internet-voting, accessed 10 December 2023; Electoral Council of Australia and New Zealand, Internet voting in Australian election systems: https://www.ecanz.gov.au/sites/default/files/2021-10/internet-voting-australian-election-systems_0.doc, accessed 10 September 2023, p. 70.

126. In January 2022, the NSW Electoral Commission (NSWEC) petitioned the NSW Supreme Court to void the outcome in three local council elections held on 4 December the previous year on the basis of the petition launched by the NSWEC saying there was a "defect or irregularity" in the electronic iVote system. The court refrained from voiding the elections on the basis of the costs of re-running the elections and the time, costs and personal impacts associated with additional election campaigns.

127. Le Monde, 3 June 2022: https://www.lemonde.fr/politique/article/2022/06/03/elections-legislatives-2022-les-rates-du-vote-des-francais-de-l-etranger_6128791_823448.html, accessed 10 December 2023.

128. Scytl, "What does it cost to vote?", 16 March 2022: https://medium.com/edge-elections/what-does-it-cost-to-vote-78eed7b5722c, accessed 10 December 2023.

voting with 77% of voters using internet voting, with a total of more than 230 000 votes in the first round, and 270 000 in the second round.[129]

Situation in Ukraine

The public discussion around out-of-country voting has highlighted the general issue of a lack of financial and human resources. Discussions with stakeholders confirmed that the financial repercussions of internet voting, in particular the cybersecurity aspects, cannot be addressed with existing resources.

4. Additional challenges specific to Ukraine

The introduction of e-voting in Ukraine faces challenges which may be similar to those faced by other countries in central and eastern Europe. However, Ukraine also has specific features driven by the ongoing war and the state of economic development which significantly complicate progress in this direction. Moreover, defending against the threat to national security and sovereignty is the top priority.

Active hostilities and aggression from Russia take place on all possible fronts. The digital component is also a serious battleground. Websites, servers and other technological components of public authorities face constant and highly aggressive attacks from the aggressor state. Consequently, even piloting new voting formats will be perilous in a wartime environment. Introducing such complexities and innovations in the initial post-war election campaign is unlikely to be appropriate. The challenges of post-war recovery will hinder the proper preparation of society (technologically and through educational measures). Careless application of such serious tools as i-voting could jeopardise the sovereignty of the state and its institutions.

The level of societal digitalisation is relatively high, but it does not fully meet the requirements for implementing such a large project as i-voting. Despite the widespread use of smartphones in Ukraine, the level of digital literacy and adherence to safe internet practices is still relatively low. It is worth noting the significantly lower percentage of citizens using computers (desktops and laptops). Furthermore, the use of unlicensed (pirated) software remains a serious issue.

Furthermore, the introduction of different voting modalities abroad compared to those to be used in Ukraine may significantly undermine trust in the election results.

D. Conclusions (legal part)

The conclusions presented below are broadly shared by member states of the Council of Europe. They should assist the Parliamentary Committee not only when assessing i-voting piloting for OCV in post-war elections but also when assessing i-voting for political elections (for example, in universities or other institutions/organisations) more generally.

1. Rights and voting methods for OCVs (other than internet voting)

1 With the exponential increase in the number of citizens residing abroad since February 2022 and in the difficult context related to war, the Ukrainian authorities face the challenge of finding proper solutions for ensuring voting rights for out-of-country voters in the post-war elections in Ukraine. Whether non-resident nationals should be given voting rights, and if yes, to what extent, is largely unregulated in international law and shaped by national law. Ukraine already grants OCVs the right to elect the national parliament and the President. The current framework foresees that OCVs vote in foreign diplomatic institutions of Ukraine, in person, on voting day (8 a.m. to 8 p.m. local time) and through the completion of a paper ballot; counting is conducted manually, at polling stations. Some restrictions apply to OCVs, namely they must actively register with the embassy or consulate in order to vote; in parliamentary elections, they can only vote for nationwide parties' lists but cannot elect candidates on regional lists; they cannot stand as candidates after a certain period of residing abroad.

129. For example, in the second district, only 11% voters had received their password at the opening of the voting phase and only 38% by the end of the voting phase. See Cortier V. et al. (2023), French 2022 legislative elections: a verifiability experiment, 13 September 2023: https://inria.hal.science/hal-04205615

2 Proposals to relax the restrictions for some OCVs, namely those who left because of the war, include allowing this group of OCVs to temporarily change their voting location without altering their electoral address, thus aligning with the rights of IDPs; offering them the right to also vote for candidates on regional lists and offering them the right to be candidates, despite the length of time spent abroad. If accepted, such proposals will create different sub-categories of OCVs whose characteristics and rights should be clearly defined. The new standards should also be communicated clearly and understandably to OCVs.

3 On the question of enabling the exercise of OCVs' voting rights, international law does not oblige states to introduce a system that ensures the exercise of the right to vote to their non-resident citizens from their place of residence. It notes that elections abroad should generally meet the same standards for democratic elections as in-country procedures. The design of a system for voting abroad depends on the particular circumstances of a country, including its administrative, infrastructural and budget constraints, the in-country election arrangements and the level of public confidence. Each country should find a balance between secure and universal suffrage.

4 Ukrainian law already provides for a voting system: the in-person voting in premises of foreign diplomatic institutions of Ukraine on paper ballots. The main obstacle so far has been the very limited number of polling stations abroad that could not meet the more modest needs of past elections. Without changes, these will not meet the needs of post-war elections. Hence, a range of voting methods to be offered to OCVs is being discussed. In the case of internet voting, OCVs should have two voting channels available, not just one; the existing polling station option should remain available to them in addition to internet voting, for security reasons.

5 Expanding the network of polling stations abroad beyond the premises of foreign diplomatic institutions of Ukraine, and securing them, requires significant and active co-operation and co-ordination with the governments of hosting states to overcome logistical and legal challenges. This might be particularly challenging in some countries. Furthermore, specific regulation for voting in polling stations abroad other than embassies and consulates must be introduced. Sufficient funding and human resources for staffing election commissions is another challenge. Electoral legislation requires that the organisation and conduct of elections must be funded only from the state budget.

6 The introduction of alternative voting channels such as remote voting and the extension of the duration of the voting period (early voting), which comes with postal voting (and internet voting), requires legislative changes. A major challenge is to prevent vote selling/buying, which is considered a significant issue in Ukraine. Measures to promote personal and secret suffrage remain lex imperfecta if their control is impossible in practice and there is no general trust that they are respected in remote voting. Furthermore, the functioning of postal services within Ukraine raises concerns regarding the quality and reliability necessary for the election-related purposes. Consequently, it might significantly undermine trust in the election results if some votes are delivered by post, even for the part that may be properly organised by reputable postal operators in other countries. Supervising the printing process and giving the electorate time to become acquainted with postal voting are other challenges. Strict identity checks are required to avoid impersonation: these are a major challenge in remote voting. Another issue would be for the Ukrainian authorities to verify the accuracy of addresses of OCVs abroad. Such accuracy is important for sending them voting material for postal voting (ballot papers, for example) and i-voting (such as verification codes). Of the two remote voting options, postal voting presents the advantage of offering a paper trail and thus the possibility of recounts, which internet voting does not.

7 Although used in some countries, the generalised use of proxy voting for voters abroad is not in line with international standards and thus not recommended. It should be noted that the same concerns related to proxy voting are valid for both postal and internet voting.

8 Returning to vote in Ukraine is not foreseen by legislation. OCVs who have not registered with an embassy or consulate can return to vote in their constituency or opt for an alternative polling location; those who have registered will be required to modify their electoral address within a certain time frame. More generally, returning to vote in Ukraine is extremely complex and largely depends on the security situation. Furthermore, it obscures the importance of the engagement of voters in the overall electoral campaign.

9 Mobile voting stations abroad are not foreseen by legislation either. Home voting exists in Ukraine but there is a relatively low level of confidence in voting outside regular polling stations in Ukraine.

10 Election observation is necessary, but a majority of parties most probably will lack necessary organisational and financial resources for observation and are unlikely to develop them even after the war.

11 Legislation establishes sanctions for infringement of electoral rights; however, their effective application is limited and is already an issue. It will be even more difficult to ensure the application of sanctions in a context of remote voting. If and how the administrative and criminal law of Ukraine can apply to potential violations of voting rights that occur abroad, namely in/around polling stations, should be addressed in agreements with hosting states, which still need to be concluded. Agreements may vary from country to country though, affecting the principle of equality. Mishaps being inevitable, it is necessary to anticipate and mitigate risks and manage them actively.

12 Some other issues specific to Ukraine include the following. The introduction of different modalities of voting in Ukraine and abroad may be seen by some as a violation of the principle of equality of voters; given existing criticism towards those who have left, it may trigger unfavourable social reactions. Several aspects of out-of-country voting rely on support from respective national governments; currently Ukraine has difficulties even to obtain information about the number of Ukrainians residing in specific countries. Changing the voting model abroad would require substantial financial resources, which are currently unavailable in Ukraine. Even funding for conducting elections within Ukraine under the old model will be exceptionally challenging.

2. International experiences of internet voting

1 The application of electoral principles to i-voting is not straightforward, given its technical complexity. The Council of Europe has established soft-law instruments that offer guidance to countries on how to regulate such technologies with a focus on compliance with electoral principles. Other relevant instruments include those developed by the Venice Commission and the OSCE/ODIHR. Experiences from other countries are relevant.

2 Internet voting development in Switzerland is influenced by it being a federal state where voting is a cantonal competence; being a semi-direct democracy with frequent votes; having generalised postal voting; a lack of concern for coercion, vote buying and selling; and mutual trust between voters and the election administration. Internet voting has been experimental since 2003 (security prevails over speed). It is complementary to polling station and postal voting. The Swiss Post internet voting system offers individual and universal verifiability with postal mail used as a second communication channel. The system has been developed in co-operation with IT experts worldwide; the source code and other important system documents are published; and Swiss Post organises public intrusion tests and has a bug bounty programme. Switzerland has the most detailed i-voting regulation.

3 Internet voting development in Estonia is influenced by it being one of the most digitally advanced societies, with compulsory e-ID and integrated e-government services. Internet voting is available to all voters as an alternative to in-person voting in polling stations, advance in-person voting and postal voting. The country has addressed concerns about voter coercion and lack of secrecy by allowing individuals to modify their online vote multiple times over the internet and eventually at the polling station: the paper vote overrides the i-vote. This is considered by the Supreme Court to be the only way to ensure secrecy and mitigate coercion. It follows that internet voting cannot replace paper voting – it must always be offered in parallel with paper voting. Individual verifiability uses the smartphone as the second channel for sending verification information. Recently Estonia has been considering a shift to mobile devices as the primary devices for voting. The issue of ensuring verification (through a communication channel independent from the voting one) is being discussed. So far, the independent communication channel is the smartphone.

4 France and Australia have less detailed and specific regulations for i-voting. Ecuador's 2023 experience illustrates the specific risk faced by internet voting if it is organised only on voting day, that is the risk of being completely disrupted by large-scale DDoS attacks. Internet voting can thus be highly vulnerable to effective disruption, as the paralysis of a single hosting infrastructure may be sufficient to disrupt the access to the voting system. The unavailability in the middle of the election day of the internet voting system used in the 2023 national elections in Ecuador offers an illustration of this concern. Such cyber-attacks can be particularly challenging to mitigate. The concerns raised by the typical protection mechanisms in the context of elections are explored by research. The consequence, as in Ecuador, could be to organise a repetition of that part of the election whose results could have been affected by the attack with the political risk of seeing winning candidates contest such reruns.

5 Experiences from Switzerland and Estonia show that detailed regulation on internet voting (prepared by government agencies) has grown complex and its constitutional conformity needs to be checked by the supreme courts and/or parliament, or other bodies who are competent to decide on the interpretation of constitutional electoral principles.

6 Investigations of and court decisions on internet voting in Germany, Austria, Finland, Belgium and the US show that internet voting is not an option for the time being for political elections. This was also the conclusion of the latest biennial meeting held at the Council of Europe on this topic. Security-related open questions and the issue of public control over the election are some main obstacles, in addition to preoccupations related to ensuring secrecy and addressing coercion.

3. The main legal requirements and implications for internet voting in Ukraine

1 Legality requires that any use of i-voting that produces results which are binding for the authorities, including pilot schemes, should be legally regulated. The Ukrainian legislator should develop detailed requirements and must ascertain that they fully reflect the applicable constitutional principles. Regulation should be clear to make implementation possible. Article 116 of the Law on all-Ukrainian referendums is not a sufficient regulation for introducing internet voting in Ukraine.

2 If the constitution forbids or limits voting from an unsupervised environment, internet voting can only be introduced after amending the constitution. The Constitution of Ukraine does not provide such a discretion for the parliament to introduce voting from an uncontrolled environment (for example home) during an extended voting period (more than one day). Hence, the introduction of internet voting requires changes in the constitution to address voting from an uncontrolled environment, even if internet voting is held only on voting day, which is not recommended.

3 Fundamental elements of electoral law should be written into the constitution or at a level higher than ordinary law. The delegation of legislative power to regulate i-voting to the executive should clearly describe the objectives and limitations of such delegation.

4 Criminal law should foresee adequate sanctions for i-voting-related violations. In most countries this requires changes in the criminal law to be considered by the legislator.

5 Changes introduced shortly before elections cause instability. Electoral legislation in Ukraine has undergone frequent changes, resulting in a lack of established and institutionalised practices. The new electoral system for parliamentary elections, introduced by the Electoral Code in 2019, has never been applied in practice. This should be considered when envisaging any other future implementation of new instruments, such as remote voting or internet voting. When envisaging i-voting, one should think of the over-next election, at least.

6 Within Ukraine, elections organised at the local or national level make use of different systems (simple majority in multi-member constituencies, first-past-the-post plurality-based system, first-past-the-post absolute majority-based system in joint single-member city constituencies or a proportional representation system using open electoral lists). Any voting system, including internet voting, should be designed

to cater for all potential kinds of elections and referendums. Currently, OCVs only vote for the party and a predefined list of candidates from that party at the national level, a rather simple system. If some OCVs are granted additional voting rights, as is being currently discussed, namely the right to elect candidates at the regional level, then the system needs to reflect that possibility too. And if, in accordance with good practice, a potential internet voting system is initially tested for smaller-scale elections (usually at local level), then it also needs to cater for different systems used at that level. The internet voting system should be designed to cover all these possibilities (system scalability). If there are different groups of OCVs with different voting rights, the system should be able to differentiate between those groups too.

7 The experience of digitalisation in other areas in Ukraine is quite risky (from a legality perspective) and does not fully comply with the requirements of the Constitution of Ukraine. The introduction of new voting modalities will require proper legislative regulation at the appropriate level of a law adopted by the legislature.

8 Voter identification and authentication requires addressing problems identified in the past, namely the existence of several e-ID and digital signature providers without central control to avoid duplications, the issue of delegation of signatures and related impersonation, the necessity of prosecuting and punishing abuses and the transparency and security of main providers like Diia. Registration at foreign diplomatic institutions of Ukraine should remain a primary option for OCVs.

9 There is consensus that, to be accepted, internet voting should offer to the voter the possibility to check that his/her vote was cast-as-intended and recorded-as-cast (individual verifiability), and to the public the possibility to check that the overall result was tallied-as-recorded and only eligible voters' votes were included in the final result (universal verifiability). Such E2E verifiability mechanisms develop the concept of a chain of trust in e-enabled elections. However, the use of such techniques should respect the confidentiality of the vote and not be used to prove one's vote. Hence, individual verifiability can be implemented provided adequate safeguards exist to prevent coercion or vote buying. In Estonia, for instance, this has been addressed by multiple voting. In Switzerland, it is not solved but coercion and vote buying are, so far, not considered problematic, given the general use of postal voting. Also, regulation should address how to proceed in case the verification shows that the vote has been tampered with. Polling station voting should be open to internet voters.

10 The primary obligation of voters is to ensure the secrecy of voting. With secrecy, vote selling and buying in particular, and coercion being important issues in Ukraine, this seems to preclude any form of voting from an uncontrolled environment.

11 The concept of trust assumptions, their disclosure and the evaluation of their realistic nature are especially important in internet voting. Regulation should address this issue and the internet voting provider should be ready to disclose and discuss the assumptions with decision makers.

12 Internet voting so far has been developed as voting from a personal computer. This is the version discussed here. It is not a stand-alone channel. It requires maintaining polling station voting in addition to internet voting as a fall-back security measure and it requires an independent communication channel for verification purposes (for example, a postal channel in Switzerland or a smartphone in Estonia). The regulation should make these aspects clear. Changes in the design of internet voting, namely voting from smartphones instead of voting from a personal computer, have an impact on the organisation of verification, which needs to be properly addressed.

13 To build trust, internet voting should be organised in a transparent manner, including publication of source codes and other system documents to make controls by researchers and the public possible. Other good practices include co-operation with research in setting up and developing the system, public intrusion tests and bug bounties.

14 Regulation should foresee dispute resolution mechanisms. Effective dispute resolution in i-voting remains a difficult legal area and further research is needed.

15 The overall responsibility of internet voting falls on the EMB and cannot be delegated, for instance, to a voting system supplier. Furthermore, competent authorities should remain in command of the main steps of the electoral process such as counting and should not delegate it to vendors. This requires adequate capacities at the EMB level. States should devise a clear framework for the institutional responsibilities as well as those of all other actors involved. Ukraine has managed to conduct several elections without serious questions about their democratic nature and openness, either within Ukraine or among international partners. This is of significant value; any changes should be made extremely carefully not to disrupt this fragile balance.

16 A significant proportion of Ukrainian society has very limited knowledge of and skills in the field of digitisation. A quick transition to digitally backed voting methods may lead to the exclusion of a considerable portion of society from the electoral process and political discourse in general, which is particularly crucial in wartime and the post-war reconstruction of the country. Any development in this direction requires information, education and time to adapt.

17 Member states of the Council of Europe should have adequate budgetary and human resources to ensure that any new voting methods respect the standards. The cost of implementing internet voting can vary significantly depending on the scale of the election, the technology used and the specific security measures implemented. Developing and maintaining a secure and reliable internet voting system involves substantial expense. Related costs like the costs of maintaining a fall-back, paper-based option (polling station voting) as a security measure, as well as the cost of providing a second communication channel for verifiability purposes, should be accounted for. Additionally, costs not directly associated with the technological solution of internet voting may include public awareness campaigns, training for election officials and ongoing media outreach to sensitise the electorate and political parties and build trust about the security of an internet voting system. As noted by an Estonian study, countries with significant election administration problems and understaffed or underfunded electoral authorities should refrain from deploying remote internet voting on a large scale. Online voting should be seen as an advanced service, as opposed to a quick fix to existing problems.

18 The risks of introducing i-voting are extremely high. Ukraine is not prepared for such an initiative, from neither a legislative nor organisational standpoint. Even piloting the relevant tools requires the conclusion of the state of war and the return of society to normal political life without security, informational or other threats to the sovereignty of Ukraine.

Part II

TECHNICAL PERSPECTIVE

A. Technical assessment of existing voting and counting system(s) in Ukraine

An overview of the current electoral infrastructure has been published in reports by IFES prior to and following the 2019 presidential elections.[130]

The State Voter Register (SVR) is developed and operated by the CEC and is updated on a monthly basis via input from local register administration bodies/register maintenance bodies (RABs/RMBs). The registration is passive, that is, all eligible Ukrainian citizens are automatically included in the register. The voters can check their register status via a website, for which they have to authenticate using a variety of methods, including social media accounts or online banking. Based on the voting register, the voter lists are printed and distributed to electoral districts in time for the election day (no later than two days before the election).

The result management system (RMS) is implemented as a centralised database, to which district election commissions (DECs) are connected to enter the results they receive from precinct election commissions (PECs). The results are reported to the public via the results reporting system. A paper trail is furthermore available for all the reported results, so that a compromising of the RMS does not lead to a compromising of election results.

The eligibility and integrity of the election results therefore depends both on the accuracy of the SVR, including the input from RABs/RMBs as well as on accurate reporting of the election results by PECs/DECs. Vote secrecy is ensured providing that the voter cannot be observed while casting their vote in the polling booth; however, reports of issues that can lead to violations of vote secrecy, such as usage of transparent ballot boxes or voters taking photos of their ballots, were reported in the 2019 election.[131]

The IFES 2018 report furthermore discusses previous attacks on Ukraine's critical infrastructure, including reports of attacks or reports of identified vulnerabilities related to the election infrastructure. As such, an attack on the 2014 election was reported, where hackers managed to conduct a denial-of-service attack on the RMB shortly before the election. Another reported and failed attack consisted of putting fake results on the CEC website. There was no evidence of any cyberattacks during the 2019 election. However, concerns over vote buying and general lack of transparency on behalf of the CEC were raised by the Civil Network OPORA, and a number of complaints about a variety of violations, including complaints about vote buying, were submitted to either the CEC or the police.

Following the 2019 election, a number of initiatives have emerged to facilitate further digitalisation of the electoral process, such as enabling voters to change their registration address online or an improved procedure for result reporting by PECs.

Since the start of the war of aggression, reports by the Council of Europe and IFES have outlined and discussed the challenges for conducting elections in post-war Ukraine. The challenges particularly relevant for the aspects of elections related to information security include difficulties in keeping the voter register up to date, given the large number of displaced persons both internally and abroad, the availability of communication channels and disinformation campaigns aimed at disrupting elections. Cybersecurity risks are furthermore likely to remain a highly relevant issue, as shown by attacks during the full-scale invasion. In particular, the attack on Kyivstar, one of the largest telecom providers in the country, has disrupted mobile communications

130. IFES (2018); IFES, 2019 Presidential Election in Ukraine, Post-Election Report, May 2019.

131. OSCE/ODIHR, Ukraine Presidential Elections, 31 March and 21 April 2019, ODIHR Election Observation Mission, Final Report, Warsaw, 20 November 2019; OSCE/ODIHR, Ukraine Early Parliamentary Elections, 21 July 2019, ODIHR Election Observation Mission, Final Report, Warsaw, 20 November 2019.

for over 20 million Ukrainians, showing the extent to which such attacks can be damaging for the digital infrastructure.[132]

B. Technical assessment of i-voting use in selected countries from an IT security perspective (case studies)

1. Estonia/Cybernetica

Internet voting was introduced in Estonia in 2005 in nationwide local elections, after a change of legislation allowing online voting in 2002 and a security analysis of a possible i-voting solution conducted in 2003. While only less than 2% of participating voters cast their votes online in the first i-voting election, this share has increased over the years, with over 50% of participating voters casting their vote online in the 2023 parliamentary elections. From its inception, the i-voting system relied heavily on the national digital identity infrastructure providing authentication via e-ID smartcards (later also supplemented by mobile ID allowing authentication using a mobile SIM card) that allowed cryptographic operations such as digital signatures. The e-ID infrastructure has been available to Estonian citizens since 2002 and is widely used for a variety of digital services. The early available version of the internet voting system did not provide any way to verify that the votes had not been manipulated, although such functionality has been partially introduced following recommendations from the OSCE/ODIHR. As such, the voting system used for the elections in 2015 allowed voters to verify that their cast vote contained their intended choice and was stored correctly by the voting system, and another update in 2017 allowed auditors to verify that the stored votes were counted correctly.[133]

Most recently, the Estonian government introduced plans to allow internet voting via mobile devices in the next elections.[134] A technical report outlining the risks and benefits of such a system was published in 2020,[135] noting among other findings that a second device (for example a PC) will nonetheless be required for vote verification.

1.1. General overview of the system

Voting phase

The voter authenticates themselves to the vote collector server (VCS) using their smartcard or mobile app and proceeds to select their options. When voters send their choice, their vote is signed with their private key, encrypted on the voting client and transferred to the VCS, which then transmits the vote to the registration server (RS), obtaining a confirmation token from the RS that is then forwarded to the voting client. After the vote is cast, the voting client furthermore displays verification data in the form of a QR code, which the voter can use to verify that their vote has been correctly stored by the voting system. Such verification is optional and for the purpose of preventing voter coercion is only available for 30 minutes after the vote has been cast. If the voter chooses to verify their vote, they use a second verification device (for example a smartphone) to obtain the verification data by scanning the QR code. The verification device uses these data to obtain the voter's encrypted vote from the VCS and to decrypt the vote.[136] The decrypted vote is displayed to the voter, who can check that it corresponds to their choice. For preventing voter coercion, up until the end of the i-voting period, the voter can cast another vote, so that only the last cast vote will count. The voter can furthermore cast their vote at a polling station in person, in which case the vote they cast online is discarded.

132. https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/

133. www.sciencedirect.com/science/article/pii/S0740624X2200051X

134. https://news.err.ee/1609078918/government-plans-to-allow-voting-by-smart-device-from-next-elections

135. Cybernetica. Mobile voting feasibility study and risk analysis. Technical document. 16 April 2020. Available at https://www.valimised.ee/en/internet-voting/more-about-i-voting/reports-and-studies-i-voting

136. Note that such decryption is only possible for a specific vote for which these verification data have been created.

Tally phase

After the voting period is over, the cast votes from both the VCS and the RS are transferred to the ballot box processor (BBP), which prepares the votes for being tallied by comparing to ensure that both the VCS and the RS contain the same list of votes, checking digital signatures to ensure that only eligible voters have cast their vote, removing updated votes (including the votes of voters who cast their vote in person) and removing the signatures. The BBP furthermore applies a mix net for shuffling the cast votes, so that they cannot be linked to the decrypted votes representing the tally result. The shuffled list of votes is transferred to the election organiser, who proceeds with decrypting the votes. The decryption is done in a distributed manner, so that a predefined number of key holders need to provide their input in order to unlock the secret key used for decryption.

For both applying a mix net and decrypting the votes, integrity of these processes is ensured via zero-knowledge proofs, which is a set of mathematical values designed to prove that a specific calculation (namely, the shuffling of the cast votes and the decryption of the shuffled result) has been performed correctly, without revealing any secrets. These proofs are stored to be audited by data auditors.

Infrastructure

The following infrastructure is required for the voting system:

- two trusted separate components available online during vote casting (a vote collector server and registration server);
- two trusted separate components used for election set-up and tallying (an election organiser and ballot box processor);[137]
- a trusted digital identity infrastructure for voter authentication;
- a trusted channel for verification, for example via a smartphone app;
- a number of key holders responsible for handling the input required for unlocking the secret key for decryption;
- auditors that verify the zero-knowledge proofs produced during the tally.

1.2. Security properties

Cast-as-intended

Cast-as-intended is ensured via the use of the voter verification option, thus requiring the following assumptions:

- either the verification device/app or the voting device/app is trustworthy;
- or the voter verifies their vote correctly (note, as the verification step is optional, the number of voters verifying their votes has been consistently low throughout elections, estimated at less than 5% of all online voters).[138]

Recorded-as-cast

Similarly to cast-as-intended, recorded-as-cast is ensured if the voter verifies their vote correctly. Furthermore, the attacker can potentially manipulate or invalidate the stored votes unless the following assumptions are ensured:

- the VCS or the RS are honest;
- the digital identity infrastructure is trustworthy;

137. Note that depending on the system implementation, additional services such as mixing can be implemented as a separate component for further trust distribution.

138. Piret Ehin, Mihkel Solvak, Jan Willemson, Priit Vinkel, Internet voting in Estonia 2005–2019: Evidence from eleven elections, Government Information Quarterly, Volume 39, Issue 4, 2022, https://doi.org/10.1016/j.giq.2022.101718

- the verification app is trustworthy, as demonstrated by correctly verifying the signature on a cast vote.

It should be noted that violating only the first assumption – that is, an attacker compromising both the VCS and the RS – would only enable the attacker to remove the stored votes. Compromising the digital identity infrastructure, on the other hand, would also allow the attacker to replace cast votes or add new votes via what is called ballot stuffing.

Tallied-as-recorded

The integrity of the tallying process is preserved via zero-knowledge proofs, the verification of which is assumed to be correctly performed by the data auditors.

Eligibility

Eligibility is ensured under the following assumptions:

- the digital infrastructure coupled with the voter register is trustworthy and up to date in terms of determining the public keys of eligible voters;
- each citizen's smart card/mobile ID card and corresponding secret keys remain only in their possession, preventing anyone else from authenticating on behalf of the citizen.

Vote secrecy

Vote secrecy relies on several trust assumptions, namely:

- the voting client is trustworthy and does not leak information about the voter's choice;
- the voting server hosting the voting client is trustworthy;
- the mixing is performed correctly and the information linking the cast votes to the shuffled output is not preserved;
- the secret key for decrypting the votes is not leaked.

The attacker can furthermore learn some information about the voter's choice by compromising the verification app, but only if the voter actually uses the app for verification of their vote (as opposed to not verifying at all or using a different app).

Coercion resistance

Coercion resistance is provided to a limited extent, relying on the mechanism of vote updating – that is, allowing the voters to cast a new vote online or cast it in person. It should be noted that while voters are allowed to verify that the stored vote corresponds to their intention and can present the results of the verification as a receipt to the coercer/vote buyer, the verification can only be conducted at the latest 30 minutes after the vote has been cast, allowing the voter to change their vote after this time limit has passed. Coercion resistance is therefore preserved as long as a malicious attacker cannot detect the voter updating their vote, which requires the following assumptions.

- Both the VCS and the RS are trustworthy (thus no information about updated votes is leaked by either one of them to an attacker).
- The tallying process is trustworthy (thus the coercer is not able to observe which ballots have been updated either via casting another vote online or by casting a vote at a polling station).
- If the voter decides to update their vote by casting another vote online, attackers are not able to observe the communications between the voter and the voting system (for example by eavesdropping on network communications or physical observation).
- If the voter decides to update their vote by casting it at a polling station, attackers will be unable to detect it (by physical observation or by observing the records of voters who cast their vote in person and whose online votes are to be discarded from the tally).

Furthermore, as a general violation of vote secrecy violates coercion resistance as well, the assumptions outlined above for ensuring vote secrecy must also hold.

Quality of security assurances

Observing the procedures related to i-voting, including tallying the votes, is open to the public; however, parts of the process, such as the identities of the voters who cast their votes in the polling station, must be obscured to prevent violations of vote secrecy/coercion resistance. Parts of the source code of the system are also published, together with several documents containing the specifications of the system;[139] however, security experts have voiced criticism about the published information only partially covering the workings of the system and thus being insufficient for a proper auditability of the system.[140] Academic papers detailing the system have been published in several peer-reviewed publications.

Since the introduction of i-voting, several security vulnerabilities have been detected within the system. As such, during the 2011 election a student demonstrated an attack via malware on a voter's device that could have led to the manipulation of the cast vote.[141] The attack attracted extensive press coverage, following which the next versions of the i-voting system introduced individual verifiability, allowing the voter to check the validity of their cast vote using a second device (see 2.1.2). A group of security experts analysed the system used in the 2013 municipal elections,[142] identifying security flaws stemming from insufficient procedural security controls as well as vulnerabilities in the application code. The authors of the report concluded that the identified flaws could enable the attacker to manipulate the election results; furthermore, they noted the complexity required to implement a secure internet voting system, concluding with a recommendation to discontinue the use of internet voting. Following the report, the system has undergone a significant update, with additional security assurances introduced in 2017. Further vulnerabilities in both the specification and the source code affecting vote integrity or vote privacy have been identified and reported in recent years.[143] While fixes for these vulnerabilities were proposed by the report authors, the effects of some of these fixes on other security properties of the system would be challenging to estimate; furthermore, lack of specification of the system has been highlighted as one of the reasons for not being able to identify the flaws earlier despite extensive audits.

1.3. Conclusion

The Estonian i-voting system has been in use for over 15 years in a variety of elections. It has been consistently trusted by a majority of voters,[144] and the share of voters willing to cast their vote online has been steadily growing since its introduction. It has furthermore been subjected to an extensive number of audits from technical experts and election observers. Nonetheless, a rising level of polarisation in trust towards i-voting was noted following the latest parliamentary election in 2023 (see section 2.5.2), demonstrating the challenges of establishing i-voting processes that are trusted across the political spectrum of the population. Furthermore, the security of the Estonian i-voting system has been criticised on several occasions. The criticism noted vulnerabilities in the implementation of cryptographic techniques, lack of sufficient procedural security controls and insufficiently transparent documentation, showing the complexity of developing a system with a high level of security, including a sufficient level of transparency to enable effective audits.

139. https://www.valimised.ee/en/internet-voting/documents-about-internet-voting

140. Anggrio Sutopo, Thomas Haines, Peter Rønne. On the Auditability of the Estonian IVXV System and an Attack on Individual Verifiability. Workshop on Advances in Secure Electronic Voting, May 2023, Bol, brac, Croatia, https://hal.science/hal-04216242/document

141. Heiberg, S., Laud, P., Villemson, J., The Application of I-voting for Estonian Parliamentary Elections of 2011. In: Post-proceedings: 3rd international conference on e-voting and identity, Tallinn, Sep 29th-30th, 2011. Section 3.2, available at https://cyber.ee/research/library?year=2011

142. Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman. 2014. Security Analysis of the Estonian Internet Voting System. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14). Association for Computing Machinery, New York, NY, USA, 703–715. https://doi.org/10.1145/2660267.2660315

143. Anggrio Sutopo, Thomas Haines, Peter Rønne. On the Auditability of the Estonian IVXV System and an Attack on Individual Verifiability. Workshop on Advances in Secure Electronic Voting, May 2023, Bol, brac, Croatia, https://hal.science/hal-04216242/document; Müller, J. (2023). Breaking and Fixing Vote Privacy of the Estonian E-Voting Protocol IVXV. In: Matsuo, S., et al. Financial Cryptography and Data Security. FC 2022 International Workshops. FC 2022. Lecture Notes in Computer Science, vol 13412. Springer, Cham, https://doi.org/10.1007/978-3-031-32415-4_22; Pereira, O. (2023). Individual Verifiability and Revoting in the Estonian Internet Voting System. In: Matsuo, S., et al. Financial Cryptography and Data Security. FC 2022 International Workshops. FC 2022. Lecture Notes in Computer Science, vol 13412. Springer, Cham. https://doi.org/10.1007/978-3-031-32415-4_21

144. Piret Ehin, Mihkel Solvak, Jan Willemson, Priit Vinkel, Internet voting in Estonia 2005–2019: Evidence from eleven elections, Government Information Quarterly, Volume 39, Issue 4, 2022, https://doi.org/10.1016/j.giq.2022.101718

While part of the code of the voting system has been openly published, it has been criticised for insufficient documentation and other issues that prevent its proper auditability. These issues become a problem if the system were to be used and adapted by a different developer.

The voting system furthermore relies on a number of assumptions. As such, it requires a separation of duty, ideally with different components developed and maintained by different entities to prevent collusion for a malicious purpose such as violating vote secrecy (in case, for example, the trustees combine their secret key shares to decrypt the votes before their anonymisation) or vote integrity (in cases where, for instance, both the verification app and the voting app are compromised or the vote collector and the registration server collude). It also relies on voter verification for ensuring vote integrity, while several attacks have shown the possibility of circumventing verification. Even if such attacks are thwarted, it must be assumed that the voter has performed verification process correctly, which can be a problem given that only a small number of voters verify their vote at all.

Furthermore, the security of the system heavily depends on the digital infrastructure, ensuring that only the votes of eligible voters are included in the tally. In Estonia, such a digital infrastructure is well established and well integrated into the daily lives of Estonian residents, with people being familiar with the use of smartcards for a variety of digital services. The absence of such an infrastructure that is both secure and trusted by the population would lead to additional security issues.

Finally, internet voting in Estonia is one of several available voting channels. In particular, this becomes critically important if voters are unable to use the i-voting system for casting their vote, for example because of technical issues.

2. Switzerland/Swiss Post

Postal voting is common practice in Switzerland, with a large proportion of citizens that vote by post rather than in person. For example, on 18 June 2023 in the Geneva canton, 93% of votes were cast by post and 7% in person.[145] Hence, electronic voting complements postal voting. Even when electronic voting is allowed, postal voting remains a largely popular option. For example, in 2016 in the Geneva canton, 20% votes were cast on the internet and 74% by post. The existence of a large proportion of postal voting indicates that it is largely accepted that the postal channel is both secure and reliable in Switzerland. Moreover, postal voting is a standard practice and internet voting replaces postal voting and not on-site voting.

Electronic voting was introduced for the first time in Switzerland in 2003.[146] The requirements for electronic voting are defined by the Swiss Chancellery[147] and are highly demanding. For example, voters should be able to verify that their vote has been counted even if the voting server and their voting device are compromised. Moreover, it is required that the specification of the system and the code are open to public scrutiny. Not only are both the code and the specification public but experts are also mandated to audit them and a bug bounty programme awards reported bugs from anyone (rewards can be up to €230 000).[148] While this offers a highly transparent system that can build trust among citizens, it also requires a very mature system and the associated financial capacities.

2.1. General overview of the system

For the purpose of this study, only the system developed by Swiss Post and used in 2023 is described below.[149]

Voting phase

With the Swiss system, the voter receives a voting sheet by postal mail. The voting sheet is issued by an authority, called the set-up component, typically run by the canton of the voter. The voter connects to the

145. https://statistique.ge.ch/domaines/17/17_03/tableaux.asp#6

146. https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/chronik.html

147. https://www.fedlex.admin.ch/eli/cc/2022/336/fr

148. https://yeswehack.com/programs/swiss-post-evoting

149. https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/master/System

voting server and starts by entering a starting code and their birth date or birth year. They can then access the election questions and select their option. Their voting device encrypts the options and sends the resulting ballot to the voting server. Four independent control components compute, in a distributed manner, a four-digit return code, for each selected option by the voter. The voter compares the return codes with the ones printed on their voting sheet and checks that they are associated with their selected voting options. Hence the voting sheet lists all possible options, each with a corresponding return code. If the voter is satisfied with the return codes, they enter a confirmation code. This code is transmitted to the four control components that compute, again in a distributed manner, a final vote return code. The voter checks that the vote return code corresponds to the one printed on their voting sheet, which completes the voting procedure. It should be noted that while the voter is expected to conduct all steps related to verification, there is no means to force them to do so or to verify that they did so.

If a voter detects a problem during the verification, they should contact the authority and inform them about it. In that case, they are given the right to vote at a polling station or through postal mail.

Tally phase

The ballots received by the four control components are tallied at the end of the election, after four successive mixing and decryption steps. The secret key for the election is split among the four control components and trustees from the electoral board.

Infrastructure

The voting system requires a rather large infrastructure:

- a trusted postal channel from the authorities to the voters;
- a trusted set-up component for generating the voting material (in particular the voting sheets);
- four control components, run on independent servers, which are online during the election;
- auditors that check the evidence produced by the control components during the voting and the tally phases.

2.2. Security of the system

Cast-as-intended

Cast-as-intended is ensured thanks to the return code mechanism: in case the voting device encrypts a voting choice different from the one selected by the voter, it will not be able to display the right return code to the voter. This protects a voter against the modification of their vote, provided that:

- the set-up component (responsible for issuing the voting sheet) is honest;
- the printed return codes are confidential;
- at least one control component is honest (they compute the return codes in a distributed way);
- the voter is aware of and properly conducts all the verification steps.

A recent attack[150] suggests that a malicious voting device can trick the voter into performing a slightly different task (entering the return codes instead of verifying them), which completely ruins the cast-as-intended property. The general idea of this attack may apply to other cast-as-intended mechanisms. Hence the cast-as-intended property also assumes that voters are properly instructed and trained.

Recorded-as-cast

The return codes can be computed only if the four control components see the voter ballot. So the voter is guaranteed that their ballot is recorded provided that the four previously listed assumptions are fulfilled.

150. https://andreaskuster.ch/blog/2023/CVD-EVoting-Swiss-Post/

Tallied-as-recorded

The Swiss Post system guarantees proxy tallied-as-recorded verifiability: due to the zero-knowledge proofs of correct mixing and correct decryption, mandated auditors can check that the result of the election corresponds to the encrypted ballots recorded by the control components. Hence tallied-as-recorded assumes one honest auditor.

Eligibility

The voting sheet needs to be authenticated to the voting server and also to confirm a ballot. A valid ballot cannot be forged without the corresponding voting sheet. Hence voters are guaranteed that only ballots cast by legitimate voters are tallied, provided that:

- the set-up component (responsible for issuing the voting sheet) is honest;
- the voting sheets are confidential and are securely routed and distributed to voters. This assumes accurate voter addresses, secure postal services and secure voter mail boxes.

Vote secrecy

Vote secrecy is ensured through encryption (by the voting device), mixing (ballots are not directly decrypted) and distribution of the decryption key. Vote secrecy is ensured provided that:

- the voting device is honest (it sees the vote as selected by the voter);
- the voting server is honest (it could provide a malicious voting javascript);
- the set-up component is honest (it could leak the secret key of the voter, which could breach privacy and leak to the dishonest control component);
- at least one control component is honest (responsible for the mixing and decrypting) or the electoral board is honest as a whole (each member of the electoral board detains a share of the decryption key; the electoral board performs a final mixing and decryption step).

Coercion resistance

The system does not provide resistance against vote buying or coercion. Indeed, the voting material, received by surface mail, solely suffices to cast a vote. Hence, a voter may sell their voting material (or be forced to give it away). The only counter-measure is that a voter may request to vote in-person, pretending something wrong happened during the voting phase, which would erase the electronic ballot. This seems unlikely if the voter is under coercion or if they breached the law by selling their vote. Moreover, it requires that another voting method should be readily available.

Quality and transparency of the security evaluation

The Swiss Post system has been reviewed extensively by several academic experts, either mandated by Swiss Post or the Swiss Chancellery. Moreover, the specification and the code are public and the bug bounty programme has rewarded several external bug reports. Finally, a cryptographic proof of security has been provided, as required by the Chancellery, which is a state-of-the-art practice when designing security protocols.

2.3. Conclusion

The Swiss Post system is sufficiently mature to be open to a public and an academic review. However, the first public review in 2019, of a system developed by Scytl, revealed several flaws in the system,[151] followed by extensive press coverage. This compelled the authorities to stop electronic voting in Switzerland, to modify the legislation and restart the development of e-voting, with a detailed road map for improvement established in collaboration with the Swiss Chancellery and experts. As a consequence, and while electronic voting has been

151. Sarah Jamie Lewis, Olivier Pereira, Vanessa Teague. Ceci n'est pas une preuve. The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiability of the Scytl-Swiss Post Internet voting system, 12 March 2019, https://cva.unifr.ch/content/ceci-n%E2%80%99est-pas-une-preuve-use-trapdoor-commitments-bayer-groth-proofs-and-implications

used for two decades in Switzerland, only 65 000 voters were authorised for e-voting in the National Council elections in October 2023, around 1.2% of the Swiss electorate. The last time e-voting was used in National Council elections was in 2015, when it was authorised for 132 134 voters (with a total of 13 370 cast electronic votes).[152]

The example of Switzerland highlights the fact that developing a secure e-voting system requires a lot of time, first to identify the security requirements and the trust assumptions adapted to the country, then to build a secure system, and finally to allow for security evaluation.

Moreover, the Swiss Post system assumes reliable and secure postal mail. It should not be used if out-of-country voters do not have a stable address, known by the authorities, or if the voters live in a country with high security risks (or if the postal material needs to travel through countries with high security risks). Otherwise, the material could be opened, which would allow an attacker to vote in place of the absentee voters, typically towards the end of the election to avoid detection by voters. The attacker could even modify the votes without being detected if it can compromise the device of the voters.

As discussed in the previous section, the Swiss Post system does not offer protection against vote buying or coercion resistance, hence it cannot be used in a country in which corruption is a concern.

Also, the system relies on the fact that Switzerland places a high confidence in the Swiss Post company, which hosts the four servers, run by independent teams. If the IT teams collude, the company could selectively remove ballots, with low chance of detection. Hence, as in Estonia, such a system is acceptable only if the citizens place a high confidence in the entity running the "independent" servers and if the risk of external attacks and of internal corruption is low. Alternatively, several institutions should be used, with different software, which probably doubles the development cost and time.

3. Australia/Scytl

New South Wales, Australia, provided an option to cast one's vote online in state general elections in 2011, 2015 and 2019 and in multiple local elections from 2011 to 2021 via the iVote system.[153] The system consisted of multiple components, with the components used for voter registration and credential management developed by the New South Wales Electoral Commission (NSWEC), and the components used for voting and verification developed by third parties, namely Everyone Counts (in 2011) and Scytl (from 2015).[154] The verification functionality, including processes for cast-as-intended and recorded-as-cast and tallied-as-recorded verifiability, was introduced in 2015 and further refined in 2019. A total of 234 401 votes have been cast using iVote in the 2019 election.[155] The number of voters attempting to cast their vote online, however, dramatically increased to over 600 000 votes in the 2021 local election, leading to system failures that prevented some voters from casting their vote within the allotted time. As the audit reports from the 2021 election highlighted several security issues with the system,[156] it was decided by the NSWEC not to use the system for the 2023 state general election. Currently, alternative solutions for technology-assisted voting are being investigated to support voters with disabilities who might require such assistance.

3.1. General overview of the system

This description pertains to the version of the system used in the 2019 election, based on the official documentation and protocol description related to both the 2015 and the 2019 version of the system.[157]

152. https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-97361.html

153. https://elections.nsw.gov.au/about-us/reports/ivote-reports

154. Roger Wilkins AO. Report on the security of the iVote system. May 2018. Available at: https://elections.nsw.gov.au/about-us/reports/commissioned-reports/reports-on-the-ivote-system

155. https://elections.nsw.gov.au/about-us/reports/ivote-reports/data-on-ivote-for-sge2019

156. NSW Electoral Commission report on iVote system (by Deloitte). May 2022. Available at: https://elections.nsw.gov.au/about-us/reports/ivote-reports

157. See NSW Electoral Commission. iVote refresh project for the 2019 NSW State elections. February 2019; NSW Electoral Commission. An overview of the iVote 2015 voting system at https://elections.nsw.gov.au/about-us/reports/ivote-reports

Voting phase

Prior to voting online (from three to six weeks before the election until 1 p.m. on the election day), voters must register by providing their enrolment details (full name, address, date of birth) and creating their login password on the registration server (RS) website. The registration server verifies via the voting register that the provided details are correct and that the voter is eligible for voting online and has not yet cast their vote via another voting channel. If the verification steps succeed, it transfers the application to the credential management server (CMS). Once the CMS receives the application, it creates a unique credential (iVote number) and sends it to the voter via their chosen channel (post to their registered address, SMS or e-mail). In order to receive their number via SMS, e-mail or phone, the voter needs to provide a secondary means of identity confirmation, such as their passport. Voters additionally have the option to reapply to iVote to obtain new credentials, for example in case of credential loss/compromise or coercion; in such cases, the CMS marks their old credentials as invalid.

After the iVote number is received, the voter can use it together with their password as secret credentials to log into the voting website and select their voting option, which is then encrypted and signed using keys derived from the voter's secret credentials. After the encrypted and signed vote has been cast, the voter has the option to verify that their cast vote encrypts the intended option using either a phone call or a verification app. This verification works in a similar way to the Estonian i-voting system (see section 2.1): after casting the vote, the voting website displays a QR code containing the receipt number that can be used to locate the cast vote. The voter uses the verification app on a second trusted device to scan the QR code and input their iVote number and password, after which the verification app retrieves and decrypts the cast vote, displaying it to the voter for verification. If the voter chooses to verify their vote using a phone call instead of scanning the QR code, the voter provides a receipt number, their iVote number and password via a phone call to the verification server, which then reads the voter's choice back to them. If the voter has reapplied for an iVote, they can update their vote by casting another vote using their new credentials; while their old vote will still be accessible via the system (hence can be verified using the process outlined above, provided that the voter has stored the verification data either as a QR code or as a receipt number), only the last vote will be counted in the tally. The receipt numbers of cast votes are published on the receipt-checking website where the voters can verify that their vote is recorded within the system.

Tally phase

Once the voting period is over, the votes are cleansed by verifying the signatures and removing invalid votes (for example, votes that have been updated by the voter either by reapplying for an iVote and casting a vote with the new credentials, or casting a vote via another voting channel), as well as removing the voter identification information from the encrypted votes. Afterwards, the votes are shuffled by applying a mix net, which removes the link between the cast votes and the decrypted votes that will be included in the tally. After the mixing, the votes are decrypted using threshold distributed key sharing, requiring a quorum of Election Board representatives to perform the decryption.

Infrastructure

The following infrastructure is required for the voting system:

- three separate components responsible for hosting registration and credential management systems (online), voting and tallying (online and offline) and verification (online);
- a trusted channel for the authorities to distribute voter credentials to eligible voters (for example by SMS, e-mail or post);
- a trusted channel for verification, for example via a smartphone app or a phone call;
- a number of trustees responsible for handling the secret key shares for decryption;
- auditors that verify the zero-knowledge proofs produced during the tally.

3.2. Security properties

Cast-as-intended

Cast-as-intended is ensured due to the use of the verification option, which assumes that:

- the corresponding verification channel (that is, either the app or the phone channel) is trustworthy;
- the voter performs the verification (note that 47% of the cast votes were verified by voters during the 2019 state general election).[158]

Recorded-as-cast

The same mechanism that ensures cast-as-intended also ensures that the cast vote has been recorded by the system. The voter can furthermore ensure that their cast vote is not deleted after the verification by checking that the receipt number of their vote is published on the receipt-checking website. Additionally, an attacker can invalidate the cast and recorded votes if either of the following assumptions is violated:

- the registration server is honest;
- the credential management server is honest (see also the discussion on eligibility below).

By violating the registration or the credential manipulation server, an attacker can invalidate the cast vote by requesting or recording new credentials on behalf of an eligible voter, thus leading to the cast votes being marked as invalid.

Tallied-as-recorded

Tallied-as-recorded of the stored votes that have not been marked as invalid is ensured via zero-knowledge proofs that are assumed to be verified correctly by the auditors.

Eligibility

Eligibility relies on the following assumptions.

- The registration server is honest, namely, it is assumed to correctly perform the eligibility checks and only forward applications submitted by eligible voters to the CMS.
- The credential management server is honest, namely, it is assumed to generate credentials only for applications from eligible voters and to correctly mark the old credentials of voters who reapplied for an iVote as invalid.
- The voting register is trustworthy.
- The credentials delivered to the voter are known only to the voter (thus also assuming the security of the corresponding delivery channel).

Vote secrecy

Vote secrecy can be violated in several ways, and the following assumptions are needed to be relied on to prevent a violation.

- The voting client does not leak information about a voter's choice.
- The key generation process is not compromised, so that the secret key used for decryption is not leaked.
- The infrastructure used for the vote verification is honest.
- The mixing of cast votes during tallying does not leak any secret information (that is, information that allows a link between the output ciphertexts and the input ones).
- Enough secret key shares are not leaked, preventing any malicious attacker from decrypting the cast votes before they are anonymised.

158. https://elections.nsw.gov.au/about-us/reports/ivote-reports/data-on-ivote-for-sge2019

It should be noted that in the final example in the list above the attacker would also need to learn the link between the iVote number and the identity of the voter, which can be done by compromising the credential management server, eavesdropping on the credentials as they are sent to the voter or leaking the voting credentials directly from the voter (via phishing attacks, for example). Note also that a compromise of the verification channel (either compromising the verification app or eavesdropping on the phone call used for verification) can lead to violation of vote secrecy to some extent, but malicious attackers would not be able to use such compromise to learn about the vote that the voter did not verify using the compromised channel.

Coercion resistance

Coercion resistance relies on the possibility for the voter to reapply for an iVote and cast another vote using new issued credentials or cast their vote via another voting channel. As in the Estonian system, coercion resistance is therefore ensured under the following assumptions.

- The voter can communicate with the voting system without being observed by a malicious attacker. This implies that an attacker cannot detect the voter reapplying for an iVote, which can be done for example by physical observation of the voter, eavesdropping on network communications or monitoring other channels such as SMS, phone or post that the voter might choose to receive their credentials.
- The registration and the credential server are honest (that is, an attacker is unable to detect the voter reapplying for an iVote).
- The cleansing process is not compromised (that is, an attacker has no way of detecting votes marked as invalid that are excluded from the tally).

Furthermore, because a general violation of vote secrecy violates coercion resistance as well, the assumptions outlined above for ensuring vote secrecy must also hold.

Quality of security assurances

The security evaluation of the iVote system involved several stages and audits, including audits by independent experts from industry and academia,[159] sharing the source code of the application with experts and publishing the protocol description in peer-reviewed academic publications. A number of attacks have been identified, including a vulnerability involving the use of a third-party library that was discovered by Teague and Halderman in the iVote version used in the 2015 election while the election was running, potentially allowing an attacker to circumvent the verification mechanism and manipulate the votes cast.[160] Another vulnerability was discovered by Teague in the 2019 election, potentially allowing an attacker to circumvent verification of zero-knowledge proofs during tallying and therefore manipulate the election result.[161] For both of these vulnerabilities, fixes have been proposed by the system developers.[162] Nonetheless, an audit by Deloitte in 2021[163] found a number of security issues with the system, such as a lack of technical controls (like two-factor authentication for administrative access to certain system components) and insufficient reporting regarding implemented security controls to NSWEC. These issues led to the voting system being discontinued from future use.

159. https://elections.nsw.gov.au/about-us/reports/ivote-reports#ivoteatthe2021nswlocalgovernmentelections

160. Halderman, J.A., Teague, V. (2015). The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. In: Haenni, R., Koenig, R., Wikström, D. (eds) E-Voting and Identity. Vote-ID 2015. Lecture Notes in Computer Science, Vol. 9269. Springer, Cham. https://doi.org/10.1007/978-3-319-22270-7_3

161. Vanessa Teague. Faking an iVote decryption proof. Why the decryption proof flaw identified in the SwissPost system affects the iVote system too. The University of Melbourne, Parkville, Australia. 13 November 2019. https://thinkingcybersecurity.com/iVoteDecryptionProofCheat.pdf

162. Response from the NSW Electoral Commission to iVote security allegations: https://elections.nsw.gov.au/about-us/reports/ivote-reports/response-to-ivote-security-allegations, and Scytl review of the attack described in the report "Faking an iVote decryption proof" by Vanessa Teague. 21 November 2019, updated on 28 November 2019.

163. New South Wales Electoral Commission. ASAE3150 assurance report over NSW Electoral Commission's iVote system (by Deloitte). May 2022. Available at: https://elections.nsw.gov.au/about-us/reports/ivote-reports

3.3. Conclusion

The iVote system was developed using state-of-the-art techniques for verifiable internet voting and underwent a thorough process of security evaluation. Nonetheless, after several of these evaluations, serious vulnerabilities were still found within the system, with some of them, if exploited, potentially capable of changing the election result. Such findings once again highlight the complexity of developing and evaluating a secure internet voting system; furthermore, they point to the limitations of the evaluation process of the system, such as placing restrictions on access to the system source code, leading to several experts deciding against going through the official review process, inspecting the limited information available to the public instead.

Furthermore, even if the security assurances described above hold, the system relies on several strong assumptions. As such, it requires a true separation of duty, so that the system components that are assumed to be independent are actually implemented and administered by independent entities – otherwise, a number of security properties can be violated if several such entities collude with a malicious goal. As the system components in the iVote system were developed by NSWCE and Scytl, the extent to which the existing implementation can be reused for other elections is open to question.

To ensure that only eligible voters participate in the election, a reliable communication channel, such as post, between the voters and the voting system is required, ensuring that voter credentials are only received by eligible voters. Establishing such a channel can be a problem for voters without a stable residential address. While alternative communication channels such as SMS or e-mail can be used, establishing voter authentication within these channels (for example, ensuring that a particular phone number belongs to a legitimate voter and is not accessed by anyone else) can remain a challenge.

Furthermore, such a channel needs to be sufficiently covert to prevent coercion risks. Otherwise, an attacker can potentially detect that a voter has requested a new set of credentials, for example, if the attacker lives in the same household as the voter (such as refugee home or a shared apartment). In such a case, the attacker would also recognise whether the voter obeyed the coercer instructions.

The system also relies on voters verifying that their vote has been cast as intended via the verification app or phone-based verification. While the verification rate in New South Wales elections has been comparatively high, it remains an open question whether the voters who conducted verification actually did this correctly, as mistakes in the verification process can lead to vote manipulations going undetected, and studies of related verification techniques show that such mistakes are not uncommon.

4. France/Voxaly

Internet voting was introduced in France in 2012[164] for a national election, namely the legislative election. It is available to out-of-country voters only, who could also vote in person or by postal mail. For the following legislative elections in 2017, the option to vote by internet was cancelled three months before the election after shortcomings were identified during a full-scale test and as a result of an "extremely high threat level".[165] Internet voting was reintroduced for the 2022 legislative elections, for out-of-country voters, who were again offered the option to vote in person or by postal mail. Out-of-country voters elect 11 of the 577 deputies in France, and 77% of them chose internet voting in 2022 (22.6% voted in person and 0.4% by postal mail).

Internet voting is regulated by the CNIL (Commission nationale de l'informatique et des libertés), an independent French agency that defines security recommendations that are legally non-binding. These recommendations apply to all kinds of elections and are based on three levels of security, the third level being the highest. Internet voting for out-of-country voters in legislative elections is organised by the MEAE (Ministère de l'Europe et des Affaires étrangères), the French ministry for Europe and foreign affairs. For these high-stake elections, the ministry is advised by the ANSSI (Agence nationale de la sécurité des systèmes d'information), the French security agency. Hence the voting system must comply with the ANSSI security considerations as well as the CNIL recommendations. For the first time in 2022, and as a result of the new CNIL recommendations in 2019, the notion of verifiability was introduced to the legislative election.

164. Anziani A., Lefevre A., Parliamentary report No. 445 (2013-2104), 9 April 2014 (in French): https://www.senat.fr/rap/r13-445/r13-445.html

165. Question to the government No. 25385 – 14th legislature, Response of the Ministry of Foreign Affairs and international development, 27 April 2017 (in French): https://www.senat.fr/questions/base/2017/qSEQ170325385.html

4.1. General overview of the system

In 2022, the internet voting system for out-of-country voters was developed by the Voxaly company and operated by the MEAE, under the supervision of ANSSI. As recommended by the CNIL, the MEAE mandated a group of experts to act as a third party for verifiability. A (partial) specification of the system was made public,[166] for the first time. Additional documentation can be found in the report by the third party[167] and in a publication from the researchers that reverse-engineered the code.[168]

Voting phase

The voter authenticates on the voting server using a login and password that they receive before the election through two different channels: the login by e-mail and the password by SMS. The voter's voting device encrypts their choice and sends the resulting ballot to the voting server. The voting server registers the ballot and sends a receipt to the voter, a PDF document, which contains the (hashed) ballot of the voter, signed by the voting server. The voter is invited to check that their ballot has been counted. To do so, they are given two options (both are proposed in the PDF document). They can either follow a link to the voting server and submit their (hashed) ballot – in which case the voting server checks that the ballot is present in the ballot box – or they can visit the website of the third party and submit the signed ballot, to check that the signature is valid. If not, they should complain. If the signature is valid, they are invited to visit again the third party website at the end of the election: at that time, the third party will be able to check that the signed ballot is included in the ballot box and has been counted.

Tally phase

The ballots are encrypted with a homomorphic encryption scheme (ElGamal). Hence, they can be combined homomorphically to obtain a single ciphertext that contains the number of votes for each candidate. This ciphertext is decrypted by the decryption authorities, who also produce a proof of correct decryption. This approach based on homomorphic encryption is a simpler alternative to the mixing procedures used for example in Estonia, New South Wales and Switzerland, which is possible in the French system for overseas voters because the number of candidates – the 11 deputies representing overseas constituencies – is small. The encrypted ballots and proof of correct decryption are sent to the third party that checks the correctness of the proofs. The third party also publishes, on its website, the hash of each received ballot. This allows voters to publicly check that their vote has been counted.

Infrastructure

The voting system requires:

- a voting server, online during the election;
- two secure channels from the server to the voters, namely through e-mail and text message;
- a third-party auditor that can host an online server during and after the election (but its availability is less critical than the voting server).

4.2. Security of the system

Cast-as-intended

The system does not offer cryptographic protection against the corruption of a voting device. Hence a corrupted device may change the vote of a voter, for example by encrypting A when the voter selects B.

166. VOXALY. MEAE – Transparency and verifiability V2. Specifications v.2.04. 22 February 2023. https://www.voxaly.com/wp-content/uploads/VOXALY-LEG2023-Transparence-et-Verifiabilite-Specifications-publiques-v2-04.pdf

167. Véronique Cortier, Pierrick Gaudry, Stéphane Glondu, Sylvain Ruhault. French 2022 legislatives elections: a verifiability experiment. The E-Vote-ID Conference 2023, October 2023, Luxembourg City, Luxembourg. hal-04205615. https://inria.hal.science/hal-04205615

168. Alexandre Debant and Lucca Hirschi. Reversing, breaking, and fixing the French legislative election e-voting protocol. Université de Lorraine, Inria, CNRS, France. 25 September 2023. https://eprint.iacr.org/2022/1653

Recorded-as-cast

If the voter visits the third-party website at the end of the election and if they receive confirmation that their hashed ballot is present, then they are guaranteed that their ballot is recorded, provided that the third party is honest. However, very few voters do these checks. For example, in the first round of the French legislative elections, only 357 voters visited the third-party website, out of the 237 379 voters that cast a vote by internet.

Moreover, even when voters receive a message that shows that the system did not function properly, they do not necessarily complain. During a re-run of the election for three deputies in 2023, the website of the third party was not configured properly with respect to the first round, for 11 days after the election.[169] Eighteen voters encountered an error message saying that their ballot was not counted. Only one out of 18 voters filled in a form to complain, and the complaint was only addressed after one week, yielding an update of the website. This lack of complaints may affect the effectiveness of verifiability of other voting systems as well.

Tallied-as-recorded

The Voxaly system guarantees proxy tallied-as-recorded verifiability. Indeed, because of the zero-knowledge proofs of correct decryption, the third party can check that the result of the election corresponds to the set of received encrypted ballots. The hash of these encrypted ballots are then made public. Hence, tallied-as-recoded assumes that the third party is honest or that the tally server is honest.

Eligibility

Eligibility is ensured through the authentication of the voter with a login and password. Voters are guaranteed that only ballots cast by legitimate voters are tallied provided that the voting server is not corrupted and that both the login and password of voters, sent through two distinct channels, are not stolen.

Vote secrecy

Vote secrecy is ensured through encryption (by the voting device) and threshold distribution of the decryption key among the decryption authorities. Four out of 16 decryption key shares suffice to decrypt. Each share of the key is generated and stored on an MEAE computer, encrypted with the password of the corresponding decryption authority. Vote secrecy is ensured provided that:

- the voting device is honest (it sees the vote as selected by the voter);
- the voting server is honest (it could provide a malicious voting javascript);
- at least 13 authorities are honest;
- the computer in charge of generating the key and decrypting is not corrupted.

Coercion resistance

The system does not provide resistance against vote buying or coercion. Indeed, the voting material, received by e-mail and SMS, solely suffices to cast a vote. Hence, a voter may sell their voting material (or be forced to give it away).

Quality and transparency of the security evaluation

Most of the security evaluation is done by the ANSSI, the French national agency, which may mandate external experts to audit the solution. Reports from experts and from the ANSSI are not made public. The only public reports are those from the third party that attest that the result of the election corresponds to the encrypted ballots they received. The source code is not public and the published specification is only partial.

169. Véronique Cortier, Pierrick Gaudry, Stéphane Glondu, Sylvain Ruhault. French 2022 legislatives elections: a verifiability experiment. The E-Vote-ID Conference 2023, October 2023, Luxembourg City, Luxembourg. hal-04205615. https://inria.hal.science/hal-04205615

Despite the lack of documentation, independent researchers revealed[170] that the voting client does not check whether the ballot displayed in the voter's receipt (the PDF document) does really correspond to the voter ballot, yielding an attack against recorded-as-cast. They also discovered various attacks against vote secrecy, due to the fact that ballots were insufficiently linked to the election they belonged to.

4.3. Conclusion

The Voxaly system has the advantage of being simple. However, it does not offer resistance against cast-as-intended nor against vote buying and coercion resistance. The system is not yet ready for public evaluation.

The use of SMS may be an issue when SMS messages are not properly delivered. As explained earlier, out-of-country voters elected 11 deputies. Two of the elections for these 11 deputies had to be re-run in 2023 as a result of poor mobile phone reception in some countries and problems with delivering SMS messages. A third election was re-run for other issues. For example, in Argentina, only 11% of the SMS messages containing the passwords were received before the voting phase, and only 38% were received by the end of the voting phase.[171] Similar issues were encountered in Algeria.[172] Such issues can affect other voting systems as soon as they use SMS.

The voting server is operated by a single entity (the MEAE). If corrupted, it could add ballots (in place of absentee voters), without being detected. Hence the Voxaly system can be used only if citizens have a high level of confidence in this entity and if the risk of external attacks and of internal corruption is low. Similarly, the decryption keys of the election are all generated on a single computer (operated again by the MEAE). Hence this system can only be used in a context where the risk of attacks against vote secrecy is considered to be low.

C. Technical assessment of alternative voting options (other than i-voting) for OCVs from an IT security perspective

1. Postal voting

The methodology for analysing internet voting may be applied to postal voting as well. The exact security of postal voting depends on the system. Some security measures may mitigate some of the risks mentioned here.

1.1. Cast-as-intended

Postal voting is much simpler than internet voting. The voter can easily be sure that their paper ballot contains their intended vote. Clear instructions should be given to voters so that they can fill out the ballots appropriately.

1.2. Recorded-as-cast

Recorded-as-cast is a real issue in postal voting. Even without deliberately malicious activities, cast ballots may not arrive at their destination or arrive too late. Moreover, once received, ballots are often stored before being all counted together. This forms a sweet spot for an attacker that could remove some ballots, for example depending on the region (if some regions are more in favour of some unwanted candidates). Ballots may even be replaced by other ballots of the attacker's choice. Security procedures may mitigate this risk by

170. Alexandre Debant and Lucca Hirschi. Reversing, breaking, and fixing the French legislative election e-voting protocol. Université de Lorraine, Inria, CNRS, France. 25 September 2023. https://eprint.iacr.org/2022/1653

171. Decision of the Constitutional Council No. 2022-5813/5814 AN. 20 January 2023. https://www.conseil-constitutionnel.fr/decision/2023/20225813_5814AN.htm

172. Decision of the Constitutional Council No. 2022-5760 AN. 20 January 2023. https://www.conseil-constitutionnel.fr/decision/2023/20225760AN.htm

limiting the access to the ballots and by limiting the feasibility of copying/modifying ballots. A ballot may also contain a tracker that allows a voter to check that their ballot has been received. It remains however difficult to guarantee that the chain from the voter's home country to the polling station is secured.

1.3. Tallied-as-recorded

Postal voting offers the same counting process as traditional on-site paper voting. Hence observers can check that ballots are correctly counted, as usual.

1.4. Eligibility

Eligibility is another issue in postal voting. Sometimes, the paper ballot material contains an identifier that prevents attackers from forging material (but material can be copied when carried by postal services). Authentication may be implemented by requiring voters to provide a copy of their ID card. This mitigates large-scale fraud. But the exact security of authentication heavily depends on the chosen postal voting system.

1.5. Vote secrecy

Vote secrecy is typically ensured by sealing the vote in a first envelope. Hence voting secrecy relies on the assumption that entities carrying the ballots do not open the envelope. Alternatively, vote secrecy may rely on the assumption that the ballot no longer contains any identifying material (name, ID card), but this may conflict with the authentication measures for eligibility.

1.6. Coercion resistance

Coercion resistance is typically not ensured by postal voting since a voter may be forced (or bribed) to give their postal voting material to a coercer.

1.7. Quality and transparency of the security evaluation

Postal voting is much simpler than internet voting and many steps can be evaluated without technical expertise (counting ballots, for example). However, the exact and complete procedure, from the content of the voting material to the tally of the ballots, is rarely public and therefore cannot be transparently audited.

1.8. Conclusion

The security offered by postal voting is low compared to on-site voting. Compared to internet voting, large-scale fraud (involving, for example, the removal or modification of ballots) is typically harder to conduct for postal elections. Postal voting is much easier to understand than internet voting and therefore postal voting may be considered more trustworthy (or less untrustworthy) by voters. The security and trust offered by on-site voting, with paper ballots, is much higher than both postal voting and internet voting.

2. In-person voting abroad on election day

2.1. Cast-as-intended

The voter can easily verify that their paper ballot is marked in a way that reflects their intended choice.

2.2. Recorded-as-cast

If counting of the votes occurs in the polling stations, the assumptions for recorded-as-cast are the same as for traditional voting. If the ballots are transferred, for example from abroad to Ukraine, the issues relevant to postal voting are also relevant here; in particular, lacking a reliable postal communication channel, the ballots

from some of the polling stations might arrive too late or not at all, or be potentially altered before reaching their destination.

2.3. Tallied-as-recorded

The security challenges are the same as for in-person voting at a polling station within the country (hereafter – traditional voting), with the additional challenges of ensuring the integrity of the tallying process in remote polling stations abroad.

2.4. Eligibility

Voters need to have a way to authenticate themselves. The voter register should be updated and reliable, also taking into account international travel for example of refugees whose whereabouts might be challenging to reliably account for. Additional challenges occur if there are issues with voter identification, for example due to the absence of valid documents.

2.5. Vote secrecy

This is the same as for traditional voting, except it can be more challenging to guarantee in smaller polling stations.

2.6. Coercion resistance

As with traditional voting, this is more difficult to guarantee in smaller polling stations or places where the election process can be more easily compromised (for example in countries that cannot provide sufficient oversight).

2.7. Quality and transparency of the security evaluation

In-person voting abroad has for the most part the same security properties as traditional voting has, with the added challenges of ensuring the integrity and transparency of the election process.

2.8. Conclusion

In-person voting abroad is easily understood by voters. The security challenges are comparable with traditional voting. Additional care needs to be exercised in areas where it is particularly challenging to ensure proper oversight of the electoral process and protection of the voters (especially in countries with high security risks), but these challenges would persist with internet voting as well.

3. Proxy voting

3.1. Cast-as-intended

The proxy is trusted to deliver the vote according to the voter's intention.

3.2. Recorded-as-cast

Given that the proxy delivers the vote in person, recorded-as-cast is ensured under the same assumptions as traditional voting.

3.3. Tallied-as-recorded

Same as recorded-as-cast, tallied-as-recorded is ensured under the same assumptions as traditional voting.

3.4. Eligibility

The proxy requires authorisation from an eligible voter, which, depending on the implemented processes, can be forged.

3.5. Vote secrecy

Vote secrecy in proxy voting is not ensured, as the proxy will know how the voter wants to vote. Vote secrecy against entities other than the proxy is ensured under the same assumptions as in traditional voting.

3.6. Coercion resistance

Coercion resistance is not ensured against proxies, that is, a proxy can coerce a voter to delegate their vote to them. Depending on the mechanisms in place that the voter can use to cancel the proxy's vote (for example by voting themselves in a polling station), coercion resistance might be ensured under the assumption that the proxy does not detect the use of such mechanisms by the voter. Against attackers other than the proxy, coercion resistance is ensured under the same assumptions as traditional elections.

3.7. Quality and transparency of the security evaluation

Proxy voting has similar procedures to traditional voting, with the exception of a proxy who can be seen as an additional threat. It therefore presents additional challenges to ensure that the proxy option is not misused, for example for voter coercion.

D. Technical assessment of the risks and feasibility of i-voting for OCV in post-war elections in Ukraine from an IT security perspective

Based on information about the existing electoral system and the electoral administration's preparedness for i-voting for OCV in post-war elections; on an assessment of experiences with i-voting elsewhere; and on the security evaluation of other voting options for OCVs, this concluding section of the technical chapter assesses the security risks of i-voting, its desirability and technical feasibility in post-war Ukraine.

1. Security assumptions

As described in case studies, internet voting systems rely on a number of assumptions to ensure an acceptable level of security. These assumptions, as well as their applicability in the context of post-war Ukraine, are described and discussed below.

1.1. Voting system and infrastructure

Separation of duty

Several of the important security properties (for example recorded-as-cast verifiability) are ensured through the separation of duty, that is, the assumption that at least some out of several system components are trustworthy. Such an assumption requires independent implementation and administration of said components, otherwise a single compromised entity (for example a company developing the system) can violate these properties. Ensuring independent implementation and administration of all the required components, however, increases the complexity of the system, including cybersecurity measures required to protect the system

and its individual components against cyberattacks. These measures include technical procedures as well as cybersecurity hygiene, ensuring that everyone involved in managing the individual components of the voting system has sufficient cybersecurity awareness and knowledge.

Availability of reliable software

State-of-the-art internet voting systems rely on complex cryptographic protocols, which have to be implemented in a secure way. As of now, there are no standard implementations of such protocols, for example as third-party libraries that have been thoroughly reviewed and tested by independent security experts. Implementing these protocols therefore remains a task for the developers of individual systems, which would require extensive expertise in secure software development, cryptography and specifically cryptographic techniques used in internet voting. As experience shows, faults in the implementation of cryptographic protocols are hard to prevent, and such faults are often detected after the system has been in use, despite a thorough process of auditing the system beforehand. Depending on the timeline for implementing internet voting in post-war elections, such faults could be especially hard to detect in proper time.

Reliable voting register

All of the reviewed systems rely on the integrity of a voting register in order to determine voter eligibility. Concerns about the timely update of such registers, especially with regard to displaced persons, had already been voiced before the full-scale invasion. These issues are likely to have become even more critical after February 2022, as the number of displaced persons, including persons whose location cannot be reliably verified, dramatically increased. Furthermore, in terms of internet voting, such a voting register would need to be accessible online and include information required to enable remote voter authentication, such as credentials or cryptographic keys, making it even more complex to develop and securely maintain. It must be noted that the Ukrainian election authorities have been constantly dealing with security issues related to the maintenance of the State Voter Register IT infrastructure, including measures on temporary suspension of its functioning (as adopted by the CEC resolution on 24 February 2024) as a result of the war of aggression. The re-launching of the fully functioning State Voter Register, including updated information on voters' whereabouts, will be an additional challenge to that of ensuring cybersecurity and protection of all personal data contained therein. Regarding voters' electronic signatures used for authentication purposes, there are still risks that they may be delegated to third persons (employees of a company, for instance) as electronic signatures are also used for other purposes in public and private activities.

An authentic and reliable alternative communication channel

Both the Swiss and the Australian systems depend on postal communication for delivering important materials to the voters (such as voter credentials). In the absence of such communication (perhaps in cases where postal communication is unreliable or slow, or where the living situation of a voter does not allow for receiving sensitive and confidential communication), security properties such as eligibility, vote secrecy, vote integrity or coercion resistance can be violated. While the voting system in Estonia does not rely on postal communication, it strongly depends on the digital infrastructure that was well established before the start of internet voting. A variant of such an infrastructure can be implemented via the Diia app that is widely used by Ukrainians for a variety of digital services. However, the question of whether the application is mature enough in terms of cybersecurity remains a controversial issue, with a number of criticisms raised on behalf of activist organisations.

Reliable alternative voting channels

Similarly, to address the issues with internet voting that might occur for some voters (for example verification failures or coercion), voters are assumed to have the option of casting their vote via an alternative channel, for example by going to a polling station. Both the voters and the election organisers in Ukraine have no experience of conducting online elections, and such elections present a number of new challenges compared to traditional voting. Therefore, alternative voting channels such as going to a polling station to cast one's vote would reduce the impact of issues with internet voting, if such occur, and limit the extent to which these issues affect the overall election. However, if postal voting is chosen as an alternative voting channel, that would also multiply the challenges to both election authorities and voters, as neither online elections nor postal voting have ever been used in elections in Ukraine.

1.2. Voter environment

Device security

For preserving vote secrecy, the voting device is assumed to be secure in all of the systems reviewed in the case studies above. While proposals to avoid this assumption exist in associated literature, they present an additional complexity and burden to the voter and have so far not been used in practice. For ensuring vote integrity, the voting systems in Estonia and Australia rely on a second device for vote verification, which is usually assumed to be a smartphone. As with the voting system components, it is important to ensure the independence of this verification device from the voting device, as well as the independence of the verification app from the voting app. It should be noted that the requirement for such a device would be specifically challenging to ensure if a smartphone is used as a main voting client (for example via a dedicated app). To ensure independent verification, another device (either a second smartphone or a desktop computer) should be used or the security assumptions of the system would weaken significantly.

Digital literacy of voters

At the most basic level, digital literacy is required from voters to be able to use the voting website, which includes basic cyber hygiene knowledge and habits such as being able to prevent leakage of their voting credentials via phishing attacks. However, in terms of verifiable voting systems, the burden on the voters becomes even higher. As such, voters are assumed to conduct several actions that are not familiar to them from traditional voting, most importantly: 1) verifying their own vote, which, as studies show, many voters have problems with; 2) applying countermeasures in case of voter coercion (for example, updating one's vote while the attacker is not observing). In particular for voter verification, studies show that voters struggle with this concept and are often unable to detect vote manipulations, especially if the attacker manages to manipulate the user interface of the voting client. This implies the need for extensive voter education as well as providing sufficient support, including options to vote via an alternative channel (see 1.1.5) to voters experiencing issues.

2. Use of a blockchain

The proposition of using a blockchain arises regularly in the context of e-voting and has been widely discussed within the e-voting community, which has reached consensus on the issue:

> *blockchains alone are insufficient for a secure electronic voting system. At most a blockchain could serve as the public bulletin board in a greater electronic voting protocol; one would still need to devise ways to achieve the voting [minimal] requirements, such as a secret ballot, voter-verifiability, and contestability.*[173]

This statement still holds in 2024.

Blockchains implement a public decentralised bulletin board. They do not solve the main issues of e-voting such as voter authentication (unless one assumes that each voter is already a blockchain user), vote secrecy or voter verifiability. Blockchains can be used to further improve a solid solution but not be the main ingredient. Hence voting systems that describe blockchain as their key solution should be heavily scrutinised. For example, votes should still be encrypted, ballots should be authenticated and the tally process should not open the ballots before re-randomisable mixnets or homomorphic combination.

3. Risks

The risks that can arise from a violation of security assumptions are described in this section.

3.1 Election result manipulation

While election manipulation is a risk in any voting system, use of election technologies, in particular, relying on centralised processes such as storage or tallying of votes, can lead to large-scale manipulation if system

173. Park S. et al. (2021), "Going from bad to worse: from Internet voting to blockchain voting", in Journal of Cybersecurity.

components are compromised by the attacker. Internet voting in particular attempts to mitigate this problem by introducing end-to-end verifiability. However, as demonstrated by case studies and shown by related research, such verifiability is challenging to implement correctly, and if voters have to perform some verification steps themselves, they are not always capable of doing so correctly. Completely preventing manipulation is therefore challenging if not impossible. Furthermore, in cases where manipulation is detected via the use of verification mechanisms, proper response measures and processes need to be in place to ensure that the issues can be fixed without needing to repeat the election.

3.2. Voter coercion

Voter coercion/bribery and its prosecution has been identified as an issue in the context of Ukrainian elections. These issues can be exacerbated by the use of internet voting or other kinds of voting in an uncontrolled environment (for example postal voting). While voting systems in other countries attempt to mitigate coercion by providing the opportunity to revote, this option can present additional challenges to voters, such as lack of access to a voting system or voting materials without notifying the coercer (if the coercer resides in the same household as the voter, for instance) or lack of knowledge about the procedures for revoting. Furthermore, prosecution of identified cases of voter coercion would be a challenge if it occurs outside of Ukraine's territory.

3.3. Denial-of-service attacks

In an attempt to disrupt an election, attackers can conduct denial-of-service attacks, making the voting system as a whole or its individual components (such as verification) unavailable. As denial-of-service attacks have become common in the past, as have attacks on Ukraine's critical infrastructure, including election-related infrastructure such as the CEC website, such risks need to be considered. Unless there is a reliable alternative channel (for example going to a physical polling station), denial of service would disenfranchise voters as well as potentially undermine trust in elections.

3.4. Lack of trust leading to election de-legitimisation

While the aforementioned risks can potentially present serious issues by themselves, they can also lead to decreased trust in the election outcome if voters feel that they have reason to believe that results have been manipulated. As internet voting systems rely on complex technologies, its security evaluation can be very challenging even for security experts – and, as shown by case studies, even after such an evaluation one cannot guarantee that there are no remaining vulnerabilities that cannot be potentially identified and exploited by an attacker. Such lack of definite assurance can furthermore be exploited by malicious actors who might attempt to spread disinformation narratives, for example claiming that election fraud has occurred even in the absence of evidence.

E. Conclusions (technical part)

1 Post-war elections in Ukraine must be defended against a large variety of risks. In particular, the combination of risks seems much higher than the one faced in most other countries. As discussed above, Ukraine needs a system that can defend against vote buying and voter coercion. Moreover, given the high level of threats from powerful external attackers (like Russia), voting devices may be infected on a large scale; therefore, Ukraine should use a system that offers cast-as-intended. Also, given both the high level of threats from external attackers and the possible risks of internal corruption, the voting system needs to provide defences if the voting server itself is attacked or corrupted.

2 Hence, there is a need for a strongly verifiable system, with cast-as-intended, recorded-as-cast, tallied-as-recorded and eligibility verifiability, which also provides vote-buying resistance. Unfortunately, no deployed system satisfies all these constraints together at the moment. Only Estonia offers some resistance against vote buying, but this is only a mitigation and the system assumes a strong public-key infrastructure that citizens trust and are used to operating, which is not the case in Ukraine. Moreover, Estonia does not offer a high level of verifiability if the authorities are not trusted. Switzerland offers a high level of verifiability but at the cost of a bulky infrastructure and, more importantly, at the cost of relying on a secure postal

system, from the generation of voting material to their delivery. Such an assumption is not appropriate for out-of-country voters. The two other considered systems are less mature. In conclusion, no existing IT system can fulfil the Ukrainian needs at the moment.

3 Finally, it should be studied if the companies and the countries operating the considered internet voting systems are willing and ready to sell their software or provide internet voting as a service. Helping another country to build, operate and monitor the complex infrastructure needed for the system is a completely different job from what it is currently done at the moment. Moreover, any failure of the system if used in post-war elections in Ukraine may create doubt about other national elections using the same system, independently of the context differences. This may prevent countries or companies from allowing their systems to be used in such an insecure context.

4 The challenges outlined above show that conducting online voting elections within a short time frame would be unfeasible, given the security requirements and present threats outlined in this section. If online voting is to be considered in the long term, in addition to legal aspects, focus should be placed on following technical challenges.

- A reliable public digital infrastructure needs to be developed, which includes the introduction of digital identity. Such an infrastructure needs to provide a high level of security and voters need to familiarise themselves with how to use their digital identity to access digital services, as well as learn cyber hygiene practices to protect themselves from identity fraud. While existing projects such as Diia could potentially serve as a basis for such an infrastructure, rigorous testing needs to be done to ensure their proper security protection against cyberattacks.
- A thorough security analysis of the electoral processes needs to be conducted, identifying relevant threats for the election (for example, inside threats, attacks on individual system components, attacks on voters' devices or denial-of-service attacks from abroad). The resulting threat model, as well as proposed mitigation measures for the identified threats, should be communicated to security experts for review and evaluation; furthermore, reports should be available for the public to access, in order to increase the overall transparency of the election.
- To avoid a single point of compromise (that is, a server or individual entities that may break privacy or verifiability), one usually needs to run independent servers and have independent tally authorities. This usually requires independent machines and independent software. How to build and fund such independent services should be carefully planned. Similarly, reliable channels must exist between voters and the authorities (for example, physical postal addresses, e-mail addresses, phone numbers).
- Transparency should be promoted: a high-level description of the system should be provided to the general public and a technical specification should also be made public for experts, as well as the source code of critical components. Calls for public scrutiny should be made, for example, through bug bounty programmes and public intrusion tests. Reports of the resulting findings should be made public, as well as how decisions are made (rationale of the threat model, fixes of the system, etc.). Such transparency is necessary to build trust. It may be difficult to make everything public at the beginning, when the system and the threat model are still too immature, but in that case, it is also a strong sign that the system is not ready for high-stake elections.
- Involving independent experts, including academic experts, in evaluating the voting system used in elections. The evaluators should be provided with a comprehensive description of the system, including its source code and documentation to enable effective audits.
- Processes for voter support, including the transparent handling of complaints during the election, need to be defined and communicated to voters. As such, voters experiencing issues when verifying their vote, concerns with voter coercion or general issues with accessing the system should be aware of how to get help and, if needed, obtain assurance that their vote will be properly counted.
- The use of technology for online voting needs to be gradually introduced to voters. As such, before introducing full-scale online voting, processes such as digital access to the voting register or use of technology to secure postal voting (see section F, Excursus, below) and a general digital identity infrastructure can be introduced to improve paper-based election processes and help voters familiarise themselves with the use of technology in elections. If a decision to introduce online voting for elections is taken, it is recommended that pilot schemes are carried out before its actual introduction.

F. *Excursus:* Can we still use technology to improve the voting process for OCVs?

This section is a contribution made by a reviewing expert, Olivier Pereira.

Remote voting creates central challenges. Ballots are much harder to trace when they are not cast and tallied in a publicly observable way, making election verifiability crucial. Confidentiality is also challenged, offering opportunities for vote buying and coercion. We can outline two approaches to remote voting that address, to varying degrees, these challenges.

Postal voting

The increased adoption of postal voting in several countries has motivated recent research efforts to improve the verifiability and vote confidentiality of this approach. Postal voting has the important appeal of offering cast-as-intended verifiability by default: people see what they write on the ballot that they send by post. This is highly valuable since, as discussed above, this form of verifiability showed to be by far the most complicated to obtain in practice in all the countries that deployed internet voting. In particular, the security failure of the proposed process for cast-as-intended verifiability was a central reason to suspend internet voting in Switzerland, and that same property was broken in several ways during recent years in the Estonian and New South Wales systems; the French system also does not offer that property.

Still, current postal voting systems offer very little or nothing to support the recorded-as-cast and the tallied-as-recorded verifiability properties and offer very little protection for the secrecy of the votes. But, thanks to the cast-as-intended verifiability that comes "for free" in postal voting systems, the sole addition of the two other forms of verifiability may lead to solutions that are technically much simpler to design and deploy than verifiable internet voting systems. For instance, postal voting is described as a use case for the ElectionGuard[174] open-source software development kit designed to support end-to-end (E2E) verifiable elections. Even though ElectionGuard has been deployed in various government elections in the US – but not yet in the context of postal voting – the ElectionGuard documentation warns that internet voting raises many challenges that "are mitigated but not fully solved by E2E verifiability".[175] In Europe, a study by a consortium of Belgian universities, commissioned by the Belgian federal government, presents the development and deployment of verifiable postal voting as a strategy for building expertise on the possible future deployment of internet voting.[176] In both cases, verifiable postal voting is presented as feasible and simpler than internet voting.

Still, the existing verifiable postal voting proposals essentially remain academic work and, to the best of our knowledge, have not yet been deployed in public elections, even as pilot programmes. Vital expertise and significant effort are still needed in order to bring these systems to the level of readiness that would be appropriate for general usage in a government election. Besides, since postal voting is unsupervised, it is actually very difficult to verify who is voting and whether the vote is expressed freely. As such, it should only be deployed in contexts where remote identification mechanisms are available and where coercion and vote buying are minor concerns.

"Kiosk voting"

An interesting middle ground between formal polling stations and postal voting could be the deployment of supervised mobile "voting kiosks". This could involve buses circulating various cities, allowing voters to cast their ballot under the protection of a voting booth and the supervision of observers. This option would address the two main challenges of postal voting outlined above: kiosks make it possible to have strong guarantees on the identity of the voter, and the voting booth supports the free expression of the vote. The use of paper ballots and of a ballot box also offers cast-as-intended verifiability.

Still, and compared to traditional polling stations, kiosks could be expected to offer much weaker guarantees about the integrity of the chain of custody of the ballots cast in mobile ballot boxes. As such, the deployment

174. https://www.electionguard.vote/

175. Josh Benaloh and Michael Naehrig. ElectionGuard. Design Specification. Version 2.0.0. Microsoft Research. 18 August 2023. See page 5. https://github.com/microsoft/electionguard/releases/download/v2.0/EG_Spec_2_0.pdf

176. https://elections.fgov.be/informations-generales/etude-sur-la-possibilite-dintroduire-le-vote-internet-en-belgique

of verifiability techniques remains highly desirable in order to achieve recorded-as-cast and tallied-as-recorded guarantees.

Here again, techniques have been proposed that reached an increased maturity level with the deployment of pilot projects in several government elections. One can mention here the early deployment of the Scantegrity system in municipal elections in Takoma Park, Maryland, in 2009 and 2011,[177] the deployment of the vVote in the 2015 Victorian state election in Australia[178] and the integration of ElectionGuard in precinct scanners used in various US elections since 2020.[179] All these systems are directly compatible with kiosk voting or could be adapted easily. This is also true with the postal voting solutions outlined above, even though these have not been field tested. And all the systems mentioned would offer the desired recorded-as-cast and tallied-as-recorded guarantees.

Nevertheless, the deployment of supervised mobile kiosks would require significant effort and human resources for observation. Still, kiosks could save the significant effort that would be required in order to set up a voter identification infrastructure that is needed with the postal voting approach.

177. https://en.wikipedia.org/wiki/Scantegrity

178. Craig Burton, Chris Culnane, Steve Schneider. Secure and verifiable electronic voting in practice: the use of vVote in the Viktorian State Election. Victorian Electoral Commission, Victoria, Australia. University of Surrey, UK. 9 July 2018. https://arxiv.org/abs/1504.07098v1

179. https://www.electionguard.vote/Reports/E2EVerifiability/

Appendices

A. Nomination of candidates and territorial constituencies

In **presidential elections**, the presentation of candidates shall take place within a single nationwide constituency. Legislative provisions encompass the nomination of candidates by political parties as well as self-nomination. A party nominates a candidate for the President of Ukraine during a congress (meeting, conference) in accordance with the party's statute and internal regulations. Self-nomination is accomplished through the candidate personally submitting documents to the Central Election Commission.

In **parliamentary elections**, nominations are simultaneously conducted in one nationwide constituency and in regional electoral lists. Regional lists of candidates are formed in 25 election regions (24 regions [oblasts; the Autonomous Republic of Crimea, the city of Sevastopol are united in one election region with Kherson Oblast] and Kyiv).

Only officially registered political parties have the right to nominate candidates for MPs. They do so at party's congress (meeting, conference) in accordance with the party's statute and internal regulations.

The nationwide electoral list of a party shall be composed of no more than 450 (total number of deputies of the Parliament of Ukraine according to the Constitution) candidates for MPs. The party shall form and approve regional lists of candidates for MPs in each election region. These consist of the candidates included in the nationwide electoral list, except for the candidates included under the first nine positions in the nationwide electoral list. The party's regional electoral list shall include no fewer than five and no more than 18 candidates.

During the creation of nationwide and regional electoral lists, the party should ensure the presence of men and women (no fewer than two candidates of each sex) in each of the five positions (positions from one to five, from six to 10, and so on) on each electoral list. In cases where a party forms national and regional electoral lists with a number of candidates that is not a multiple of five, the last-listed candidates (from 1 to 4) shall be subject to the requirement to alternate candidates of different sexes in the list.

In **local elections**, nominations are carried out depending on the type of electoral system. For the elections of village, town and city mayors, joint single-member village, town and city constituencies are employed, encompassing the entirety of the respective village, town or city territorial community. The nomination of village, town and city mayors can be carried out through local party organisations or by means of self-nomination.

Multi-member constituencies are used for **small local councils**. The average indicative quantity of such multi-member constituencies shall be defined as the integer part of the quotient from the division of the quantitative membership of a respective council by three. When establishing multi-member constituencies, the deviation from their average indicative quantity may not be more than one constituency. Multi-member constituencies shall include approximately the same number of voters per one councillor mandate distributed in such constituencies. Where possible, the deviation of the number of voters in a multi-member constituency established within the territory of the respective village, town, city community may not exceed 15% of the indicative average number of voters in the constituency per one councillor mandate.

The right to nominate candidates for village, town, city councillors shall be exercised by the voters through the local party organisations or by means of self-nomination. The nomination by the party organisation in each multi-member constituency shall take place in its conference, meeting. The number of candidates for councillors included on a list of candidates to the respective council per each multi-member constituency should not exceed the number of mandates that are distributed in the respective multi-member constituen-

cy. During the creation of a list of candidates for the respective council, the party organisation should provide representation of not less than 30% of persons of each sex in the total number of candidates for the respective council.

A joint multi-member constituency and territorial constituencies are used for the elections of each **large local council**. The joint multi-member constituency shall cover, respectively, the territory of the oblast, rayon, district, city, village or town (the territory of a local council's jurisdiction). Territorial constituencies are formed as subdivisions of the joint multi-member constituency to ensure single open electoral lists (preference voting) (equivalent to electoral regions in parliamentary elections). The number of candidates for councillors to be included on a party organisation's joint electoral list should not exceed the quantitative membership of the local council. The first candidate shall be determined in the joint electoral list. All other candidates included on a joint electoral list (except for the first candidate) should also be included on one of the territorial electoral lists. A candidate cannot be included on a joint electoral list of the party organisation more than once or on two or more different territorial electoral lists.

B. Voting and counting. Distribution of mandates

Village, town, city councillors in territorial communities with fewer than 10 000 people (small local councils) shall be elected based on the system of simple majority in multi-member constituencies, into which the territory of a respective territorial community is divided. In each such constituency, at least two and no more than four councillors may be elected.

Elections for members of the Verkhovna Rada of the Autonomous Republic of Crimea, oblast, rayon, district councillors, as well as city, village, town councillors of territorial communities with at least 10 000 voters (large local councils) shall be held according to the system of proportional representation using open electoral lists of local political party organisations (hereinafter, electoral lists) in territorial constituencies, which shall be subdivisions of the joint multi-member constituency coinciding, respectively, with the territory of the Autonomous Republic of Crimea, oblast, rayon, city, district, village or town according to the administrative and territorial structure or the territory of city, village or town territorial community.

Elections for village, town, city mayors for cities with fewer than 75 000 voters shall be held according to the first-past-the-post plurality-based system in joint single-member village, town, city constituencies coinciding, respectively, with the territory of village, town or city according to the administrative and territorial structure or the territory of village, town or city territorial community.

Elections for city mayors for cities with at least 75 000 voters shall be held according to the first-past-the-post absolute majority-based system in the joint single-member city constituency coinciding with the territory of city according to the administrative and territorial structure or the territory of city territorial community.

The following voting and counting rules are general rules for all types of elections.

The CEC shall approve the text of the **voting ballot** for presidential and parliamentary elections; local territorial election commissions do so for local elections. It is to be noted that the voter can only elect candidates from published lists of candidates established through party organisations or, in some cases, self-nomination.

For the majoritarian system (presidential, local mayoral elections and elections for small local councils), the list of all candidates is included in the ballot. The ballot should include short information about each candidate. On the left, an empty square shall be placed opposite the information about each candidate. The order in which candidates are included on the voting ballot shall be determined by drawing lots, which shall be conducted by the CEC or the relevant territorial election commission. The voter shall put a plus (+) mark or another mark (v, *x*, etc.) to indicate his/her will on the voting ballot in the square box opposite the last name of the candidate for whom he/she votes. The voter may vote for only one candidate (this is true for multi-member constituencies too).

For the parliamentary elections, the form, colour and text of the ballot shall be approved by the CEC. The voting ballot shall indicate the number of each party determined by drawing lots, the full name of the respective party, the names and initials of the candidates for MPs included in the electoral list under the first nine numbers, and the sequential numbers, names and initials of each candidate for MP included in the corresponding regional electoral list of the party.

The voter, by identifying the party for which he/she votes, makes a plus sign (+) or another mark (v, *x*, etc.) in the square opposite the name of that party, indicating his/her will, and writes the sequential number of the candidate he/she supports, indicated in the party's regional list on the party's poster in the rectangle for writing the candidate's number near the text "I support the candidate of the political party for which I voted".

Elections for large local councils involve the use of a similar type of ballot. Its text is approved by the respective territorial election commission. The only distinction is that here, only one candidate included in the single electoral list is reflected, as opposed to nine candidates as in parliamentary elections. The voting procedure is the same as in parliamentary elections.

The **voting ballot for OCV in national elections** shall indicate the number of each party determined by lot, the full name of respective party and the last names and initials of the first nine candidates included in its nationwide electoral list. Accordingly, voters are legally allowed to vote only for a political party. This turns the electoral system into a closed-list system in this part.

Vote counting is conducted manually at polling stations. Precinct election commissions compile a protocol on the count and transport the ballots to the higher-level "intermediate" commission (the level of which varies depending on the type of election).

The election results are determined by the main election commission (the election commission that registered the candidates), for example, in the case of parliamentary elections, this is the Central Election Commission.

The counting of OCVs' votes should be done in the same way as for the vote counting in Ukraine, by special precinct election commissions for OCV. The Ministry of Foreign Affairs, through diplomatic bodies, participates in such precinct election commissions formation and assists with election documentation transportation to Ukraine.

In **presidential elections and mayoral elections in large cities** (with at least 75 000 voters), the majority system of absolute majority is employed. Therefore, if none of the candidates secures a majority of votes, a second round is scheduled.

For **parliamentary elections**, a 5% electoral threshold is applied (the total number of votes cast in support of electoral lists of candidates of all the political parties within the nationwide constituency). Mandates should be distributed at two levels. In each election region, MP mandates shall be distributed among the regional electoral lists of party candidates in proportion to the number of votes in support of the respective regional electoral list. In order to determine the number of MP mandates won by the regional electoral list of candidates from the party, the number of votes cast in the constituency in support of the respective regional electoral list shall be divided by the electoral quota (which is calculated nationwide). Unused votes must be distributed at the national level.

The CEC shall determine the order of candidates on the regional electoral list of each party, established in accordance with the voting results in the respective election region. Candidates who have received a number of votes equal to or exceeding 25% of the electoral quota are to be placed at the beginning of the regional electoral list of the respective party in decreasing order of percentage of votes cast by voters in support of the respective candidate. In case of an equal percentage of votes, the candidate placed higher in the regional electoral list of candidates from the party shall be placed in a higher position. After the candidates who have received a number of votes which is equal or greater than 25% of the electoral quota, other candidates shall be placed on the regional electoral list in the order determined by the party while nominating candidates.

A party that gains 5% or more of the votes is guaranteed to receive nine MP mandates, which are distributed in order of priority in accordance with the nationwide list approved by the party.

The Central Election Commission shall determine the number of mandates to be distributed in the national constituency by subtracting from the number of members of the Verkhovna Rada of Ukraine, as determined by the Constitution of Ukraine, the number of mandates received by regional electoral lists of parties eligible for distribution of mandates and the total number of mandates guaranteed for each party.

To determine the number of mandates won by the nationwide electoral list of each party eligible for distribution of MP mandates, the sum of the number of votes cast for the nationwide electoral list of each party in the foreign constituency and the number of undistributed votes cast for each party in all election regions shall be divided by the electoral quota. The integer part of the quotient thus obtained is the number of MP man-

dates received by the candidates for MPs who are included in the respective nationwide electoral list from this party. The fractional remainder of up to four decimal places shall be taken into account in the distribution of other MP mandates.

The parties with the largest fractional remainder in the nationwide electoral list resulting from the division shall each receive one additional MP mandate, starting with the nationwide electoral list of candidates from the party with the largest fractional remainder. If the fractional remainders are equal in two or more electoral lists of candidates from parties, the first additional MP mandate is to be received by such electoral list of the party whose candidates for MPs won the larger number of votes in the nationwide constituency.

For elections to **small local councils**, the system of simple majority in multi-member constituencies, into which the territory of a respective territorial community is divided, is used. In each such constituency, at least two and no more than four councillors may be elected.

For elections to **large local councils**, the system is very similar to parliamentary elections; however, only one seat in each joint multi-member constituency is guaranteed.

C. Right to stand for elections

As for right to be elected, the electoral legislation imposes certain restrictions.

- Conscripts, Ukrainian citizens residing abroad, persons found incompetent by the courts and Ukrainian citizens sentenced to imprisonment by the courts are considered to belong to no territorial community and are ineligible to vote in local elections.
- A citizen of Ukraine who is 35 years old on the day of the elections, is eligible to vote, is fluent in the state language and has resided in Ukraine for the last 10 years prior to the election day may be elected the President of Ukraine.
- A citizen of Ukraine who has reached the age of 21, has the right to vote and has been residing in Ukraine for the last five years before the election day may be elected an MP.
- A person who has been convicted of committing an intentional crime may be neither nominated nor elected as an MP, unless this conviction has been removed or expunged as provided by law.
- A citizen of Ukraine who has the right to vote as provided for in Article 70 of the Constitution of Ukraine may be elected a councillor, a village, town, city mayor. A person who has been convicted for committing a grave or especially grave crime, a criminal misdemeanour against citizens' voting rights or a criminal corruption misdemeanour may not be elected a councillor or a village, town, city mayor, unless this conviction has been removed or expunged as provided by law.

The above-mentioned restrictions on the terms of residence in Ukraine are detailed in the Electoral Code. For example, "residing in Ukraine" under this Code shall mean:

- residing in the territory within the state borders of Ukraine;
- being deployed on a ship sailing under the State Flag of Ukraine;
- stationing of citizens of Ukraine, pursuant to the procedure established by the law, in foreign diplomatic institutions of Ukraine, international organisations and their bodies as a result of their foreign assignment;
- being posted to Ukraine's polar station;
- stationing with the formations of the Armed Forces of Ukraine abroad.

Legislation establishes specific rules for the application of these restrictions regarding residency periods. In the first post-war elections, this may be a key impediment to the candidacy of individuals who left Ukraine because of the war of aggression. After staying more than 90 days abroad, a Ukrainian citizen loses the right to stand in elections. In the current circumstances of forced migration and war some proposals are being discussed by Ukrainian stakeholders to offer passive voting rights to forced migrants that left after 24 February 2022, even if they have stayed abroad for more than 90 days consecutively or for more than 183 days in total

for each annual period before the next voting day.[180] In this case, it will be necessary to distinguish between different OCVs. If the mentioned proposal is eventually accepted and implemented for the first post-war elections, this may have an impact on the organisation of registers of OCVs and the potential assignment of out-of-country voters and potential candidates to regions.

D. Overview of EU member states' out-of-country voting

Legal procedures for absentee voters residing abroad are in place in all EU member states except Malta. The right to vote for voters abroad is guaranteed in 24 member states. The exceptions are: Malta, where one needs to vote in person in-country; Ireland, which provides for postal voting for diplomats and defence force personnel only; and Denmark, where only certain groups of citizens residing abroad are eligible, and residency in-country is a general requirement for voting abroad, with an established practice that the stay abroad must neither be expected to be permanent nor have exceeded eight years.[181]

Table: Overview of provisions for absentee voters residing abroad in EU member states[182]

EU Member State	Voting abroad provision	Postal voting	In person voting	Internet voting	Proxy voting	Pres. election	Parl. Election	Regional/ municipal election	EP election	Referen-dum	Special seat(s)	Prior registration required	Election materials sent ex officio	All postal costs covered
Austria	yes	yes				yes	yes	yes	yes	yes		yes	yes, with abo	yes
Belgium	yes	yes	yes		yes		yes		yes			yes		no
Bulgaria	yes		yes			yes	yes		yes					
Croatia	yes		yes			yes	yes		yes	yes	yes, 3			
Cyprus	yes		yes			yes	yes		yes			yes		
Czechia	yes		yes			yes	yes (NA)					yes		
Denmark	yes, restricted		yes				yes	yes	yes	yes		yes		
Estonia	yes	yes	yes	yes			yes		yes	yes		yes	yes, with opt in	no
Finland	yes	yes	yes			yes	yes		yes					no
France	yes	yes	yes	yes	yes	yes	yes		yes	yes	yes, 11	yes	yes, with opt in	no
Germany	yes	yes					yes		yes			yes		no
Greece	yes		yes				yes		yes			yes		
Hungary	yes	yes	yes (res)				yes		yes, but	yes		yes	yes, with abo	yes
Ireland	yes, restricted	yes				yes	yes	yes	yes	yes		yes		yes
Italy	yes	yes					yes		yes	yes	yes, 8+4	yes	yes	yes
Latvia	yes	yes	yes				yes	yes	yes	yes				no
Lithuania	yes	yes	yes			yes	yes		yes	yes	yes, 1			yes
Luxembourg	yes	yes					yes	yes	yes	yes		yes		yes
Malta	no													
Netherlands	yes	yes			yes		yes		yes		indirectly		yes	no
Poland	yes		yes			yes	yes		yes			yes		
Portugal	yes	yes	yes			yes	yes		yes		yes, 4		yes	yes
Romania	yes	yes	yes			yes	yes		yes	yes	yes, 4+2			yes
Slovakia	yes	yes					yes		yes			yes		no
Slovenia	yes	yes	yes			yes	yes		yes				yes	no
Spain	yes	yes	yes				yes	yes (res)	yes			yes	yes	yes
Sweden	yes	yes	yes				yes		yes				yes	no

180. Civil Network OPORA/ IFES Ukraine Road map, 18 October 2023.

181. Added by the author as the Danish submission mentioned permanent residency abroad. See: https://valg.im.dk/vaelgere/udlandsdanskeres-valgret/

182. Table based on and adapted from Rabitsch A. (2023), discussion paper for the 18th European Cooperation Network on Elections (ECNE) meeting "Absentee voters residing abroad" and Election-Watch.EU Final Report Election Assessment Mission to the European Parliament elections 2019.

The most common voting options for absentee voters from EU member states residing abroad are voting by post (19 states) and voting in person (18) and sometimes both.[183] Other options provided in some cases are internet voting (2) and voting by proxy (3).

Seven member states – Bulgaria, Cyprus, Croatia, Czechia, Denmark (restrictions on eligibility of voters), Greece and Poland – only provide in-person voting abroad at an embassy/consulate and at specially set-up polling stations.[184]

Postal voting is the only option for voters abroad for citizens of six member states, namely Austria, Germany, Ireland (a restricted group of voters), Italy, Luxembourg and Slovakia.

Finland,[185] Latvia, Lithuania, Portugal, Romania, Slovenia and Sweden provide two options, in-person and postal voting for voters abroad, as does Spain, which also offers in-person advance voting at embassies/consulates between the eighth and third days, inclusive, prior to the day of the election. In Slovenia, all citizens with a registered permanent residence abroad automatically receive a postal ballot by priority mail.[186]

Hungary differentiates between voters with residence in Hungary who can only vote in person at an embassy/consulate and those voters abroad without residence in Hungary who must vote by post. Estonian citizens abroad can choose between voting in person at an embassy/consulate, voting by post and internet voting. Belgians living abroad can choose between voting in person, by post or by proxy. French citizens abroad can choose between voting in person, voting by post (parliamentary elections only), internet voting (parliamentary and consular elections only) and proxy voting. Dutch voters abroad can vote by post during the elections to the electoral college for non-residents but by postal vote or via proxy for the elections to the European Parliament and the Dutch Parliament.

In addition, voters abroad of some countries can also opt to vote in person within the territory of their country of citizenship, such as in Austria, Croatia, Belgium (also by proxy), Italy, the Netherlands[187] and Slovenia.[188]

E. Host country agreements[189]

There are no known good practice guidelines on setting up OCV inside and outside of embassies and consulates. There are however practical experiences with host country agreements and agreements with various service providers.[190] In cases of external voting across multiple countries, host country agreements often exhibit variations, necessitating a level of standardisation crucial for transparent and integral electoral processes, particularly concerning issues like elector eligibility and registration. While certain procedural and logistical differences may be inevitable in elections across countries at varying levels of development, host country agreements play a pivotal role in maintaining consistency. Past post-war OCV practices show the engagement of UN agencies like the International Organization for Migration (IOM) or international non-governmental organisations like IFES conducting or assisting the OCV process and negotiating memorandums of understanding (MoUs) with host governments.

183. In Hungary, voters abroad with residency in Hungary must vote at an embassy/consulate. With Hungary, it would be 19 countries that allow in-person voting.

184. For example, for citizens of Bulgaria, Cyprus and Greece abroad. Alternative places include churches, schools (for example in Cyprus), special post offices (in Lithuania) and, where the expatriate community is large, convention and exhibition centres (for example in France). Special polling stations can also be set up on ships (for example for Croatia and Denmark) and at military facilities such as peacekeeping operations and missions abroad (for example Croatia). For Croatia, see: https://www.morh.hr/en/voting-of-armed-forces-members-at-home-and-abroad/

185. In Finland, voters abroad can vote by post and in person at Finnish embassies or on Finnish merchant shipping vessels. See https://valtioneuvosto.fi/en/-/advance-voting-abroad-in-finland-s-2023-parliamentary-elections

186. https://www.dvk-rs.si/pogosta-vprasanja/

187. Also via proxy or – if they are able to vote in person in the Netherlands – via a voting pass. With this voting pass, they can vote in any polling station in the Netherlands.

188. https://www.dvk-rs.si/pogosta-vprasanja/

189. See also ACE Host Country Agreements at https://aceproject.org/ace-en/topics/va/host-country-issues/host-country-agreements

190. See also: p. 58 in: INE and UNDP, Electoral Studies in Compared International Perspective: Voting from Abroad in 18 Latin American Countries. Mexico: National Electoral Institute; United Nations Development Programme. May 2016. https://www.undp.org/publications/electoral-studies-compared-international-perspective; p. 23 in: International IDEA. Out-Of-Country Voting. Learning from practice. January 2021. https://www.idea.int/publications/catalogue/out-country-voting

In the context of the 2004 presidential election in Afghanistan, marked as the largest external voting programme to date in terms of registered electors and external turnout, MoUs were signed between the government of Afghanistan and the UN Assistance Mission in Afghanistan (UNAMA) with the governments of Iran and Pakistan. These MoUs outlined extensive support for the external voting programme, encompassing security provisions for registration and polling centres, escorts for transporting election material and backing for civic education and public information campaigns.

Concerning the role of third parties, while external voting agreements can be directly arranged between the host country and the electoral management body conducting the election, instances where the country of origin lacks democratic election experience or sufficient infrastructure may involve third parties. The IOM has played this role in various countries, including in Bosnia and Herzegovina, East Timor, Kosovo and, more recently, Afghanistan and Iraq. When third parties are engaged, agreements with the host country must accommodate their participation, acting not only where there is insufficient infrastructure but also as a safeguard against potential political or governmental influence from the host country. It is imperative that third parties serve strictly as implementers, leaving all politically oriented questions to the relevant governments, albeit at an additional cost to external voting programmes.

For host country agreements facilitating external voting programmes, several crucial criteria must be recognised and protected. Primarily, all parties must ensure the secrecy, neutrality and transparency of the external voting programme, free from local political or governmental influence. These agreements must also safeguard the integrity of the constitution and electoral laws of the country conducting the election, aiming to closely mirror the administrative activities of the country of origin. Additionally, external voting agreements should ensure that participation does not impact the political, social or economic inclusion of participating individuals within their country of residence.

Furthermore, agreements may need post-expiry clauses, particularly those protecting data collected during the process, to remain in force. Such clauses are crucial to prevent the sharing of information gathered during the external voting programme for purposes other than facilitating the vote. In cases where external electors are refugees, agreements can serve to prevent electoral participation from becoming a means of forced or premature repatriation. Specific provisions may state that the external voting programme will neither hinder nor delay the voluntary repatriation of refugees living in the host country. Notably, some MoUs between the IOM and countries hosting Iraqi refugees included language to ensure the respect of the principle of non-refoulement. However, challenges may arise, as seen in the case of Bosnia and Herzegovina, where the Dayton Agreement stipulated refugee repatriation during the electoral period. Such situations, where an electoral process defines the end of a peace agreement, raise the risk of violating the principle of non-refoulement by obliging refugees to return to their country of origin in order to vote.

For Iraqi OCV ahead of the 2005 elections, a MoU was signed by the EMB (IECI) and the IOM authorising the IOM to conduct the OCV programme in 14 countries. This gave them just over two months to complete the task. The IOM immediately started to negotiate MoUs for the programme with various governments. It established co-operation with host countries, deployed staff, identified offices, created materials and established polling and registration centres in an extremely short time. By 26 December 2004, 11 countries had signed agreements, with the other three signing shortly after. The concern over security issues had to be considered in each of the 14 agreements. In addition, two EMB regulations provided the legal basis for the OCV programme: 10/2004 (Out-of-Country Registration and Voting) and 16/2005 (Polling and Counting Outside Iraq). The regulations outlined the procedures and clarified the counting process.[191]

Often a certain number of citizens need to indicate their will to participate in an election for a polling station abroad to be erected, for example 10 people were required for a polling station abroad for North Macedonia. In addition, North Macedonia has an overall threshold of registered OCVs which must be met for the voting in polling stations abroad to go ahead.

Polling stations at diplomatic representations are staffed in most cases by employees of the embassies or consulates. In Croatia, for example, the foreign ministry nominates and the State Electoral Commission appoints the president and vice-president of the polling station committee while the political parties nominate other members to the committee.

191. ACE Project information on Iraq at https://aceproject.org/ace-ar/topics/va/country-case-studies/iraq-a-large-diaspora-and-security-concerns

From the comparative research carried out into in-person out-of-country voting in Bosnia and Herzegovina, Croatia and North Macedonia, voting procedures are similar to those in-country. However, in North Macedonia voting takes place the day before elections and for Croatians abroad the polling stations at diplomatic representations are open for two days instead of one day like in-country. For security reasons Bosnia and Herzegovina prints special OCV ballot papers with security marks and the name of the diplomatic representation on it. The identity of the voter tends to be verified at the polling station in the same way as EMBs carry this out in-country. However, Croatians abroad are also entitled to identify themselves with an ID issued by their host country. The counting can take place at the polling station abroad or if too few voters voted (fewer than 10 for the presidential elections and fewer than 50 for parliamentary elections in Slovenia) the ballots are returned to the CEC and counted there. If abroad, the counting usually happens at the same time as it does in-country. Yet, in North Macedonia, the counting takes place immediately after the voting abroad, one day ahead of election day. In cases where ballot papers need to be sent to the EMB in-country for counting, this may delay the announcement of final results.

F. Postal voting

Below are some international good practices on postal voting. Their application (or inability to be applied) in a specific context depends on the specific electoral framework.

- Conduct a thorough process of mapping and testing various posting and postal return options to fully understand the necessary time schedule, with detailed steps from packing postal ballot papers up to the inclusion of OCV ballots in the count.
- Minimise invalid postal ballots, build on international good practices in the drafting of well-designed information forms, outlining the various steps to voters and how best to ensure that voters sign the form or the outer envelope while safeguarding the secrecy of the ballot.
- Prepare and send out envelopes with postal ballot papers centrally to all those qualified for postal voting. This permits better monitoring and saves costs. The logistics could be outsourced to a professional company.
- Citizens abroad should specify where the postal ballot should be delivered, possibly to be picked up at a post office, to ensure safe receipt.
- Use registered post to ensure that the recipient, who should be the voter, can acknowledge receipt. Using special ballot papers with security marks for postal voting and tamper-evident envelopes would provide additional safeguards.
- The option of electronically checking the signatures of postal voters needs to be carefully considered and must ensure that this is a reliable way of ensuring a voter's identity and does not lead to disenfranchisement.
- For the purpose of strengthening electoral integrity, it is necessary to safeguard the secrecy of the vote of each individual voter by establishing procedures to prevent family voting, impersonation and coercion.
- Use QR/bar-coded envelopes, so that once a postal envelope is received by the election authority, the voter is marked off the voter register and thus cannot submit a second postal envelope or vote in person, thus preventing multiple voting.
- Further research needs to be done on whether requesting signatures of witnesses for postal voting would strengthen or jeopardise the secrecy of the vote.
- Postal envelopes need to be designed to meet international postal agreement standards. It needs to be ascertained if prepaid postal ballot returns are possible, reliable and advisable. Consultation is recommended with postal service providers about the most reliable, feasible and cost-efficient postal envelope format.
- Further research needs to be done on how best voters abroad could return their postal ballots to Ukraine. For this, various options could be tested and calculated. Option 1: the voter returns the postal ballot by registered post and the postal fee is collected from the recipient (CEC) (if possible, as the prepaid postal delivery service is not always reliable). Option 2: the voter returns the postal ballot and pays him/herself with the option of reimbursement. Option 3: the voter returns the postal ballot

to the diplomatic representation (in that country), which collects and forwards them by diplomatic mail to the CEC.

- Check whether private postal services are legally eligible to deliver postal ballots. A confidence survey about the various postal service providers could help decide.
- Examine the feasibility and level of acceptance among voters abroad of receiving ballot paper by e-mail, printing out their own ballot paper using an individual QR/barcode and returning the postal ballot at their own cost, or possibly prepaid or refunded.
- Introduce a ballot tracking system with QR/barcodes on the outer envelope. Voters can track their postal ballot envelope; the authority can inform voters about the receipt and possibly the inclusion, if considered valid, of the postal ballot in the count.
- Where possible, include the postal ballot papers in the count at the municipal/district (zone) level to avoid a differentiation in results of in-country and out-of-country voters and to facilitate timely results.
- Where possible, establish a special postal voting commission centrally and/or in each zone that specialises in handling and counting postal ballots.
- Examine the possibility of engaging private companies that specialise in postal ballots, which could assist in the process of printing the materials, packing, automatically printing addresses on postal ballot outer envelopes, sorting and posting them. The same applies for the receipt of postal ballots that can be processed manually or by machine. Dedicated regulations would need to be introduced for such processes.

Relevant documents

- Council of Europe (2004): Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting, adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies, available at https://www.coe.int/t/dgap/goodgovernance/activities/key-texts/recommendations/00Rec(2004)11_rec_adopted_en.asp

- Council of Europe (2017): Recommendation CM/Rec(2017)5 of the Committee of Ministers to member states on standards for e-voting, adopted by the Committee of Ministers on 14 June 2017 at the 1289th meeting of the Ministers' Deputies, available at https://search.coe.int/cm?i=0900001680726f6f

- Council of Europe (2022): Committee of Ministers' Guidelines CM(2022)10-final on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States, adopted by the Committee of Ministers on 2 February 2022 at the 1424th meeting of the Ministers' Deputies, available at https://search.coe.int/cm?i=0900001680a575d9

- Council of Europe (2002), European Commission for Democracy through Law (Venice Commission): Code of Good Practice in Electoral Matters, adopted by the Venice Commission at its 51st and 52nd sessions (Venice, 5-6 July and 18-19 October 2002), CDL-AD(2002)23, available at https://rm.coe.int/090000168092af01

- Council of Europe (2011), European Commission for Democracy through Law (Venice Commission): Report on out-of-country voting, adopted by the Council for Democratic Elections at its 37th meeting (Venice, 16 June 2011) and by the Venice Commission at its 87th plenary session (Venice, 17-18 June 2011), CDL-AD(2011)022, available at https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2011)022-e

- Council of Europe (2020), Driza Maurer A., Digital technologies in elections – Questions, lessons learned, perspectives, March 2020, available at https://edoc.coe.int/en/elections/8156-digital-technologies-in-elections-questions-lessons-learned-perspectives.html

- Council of Europe (2023), Kliuchkovskyi Y. and Venher V., "Organisation and holding of elections in post-war Ukraine. Prerequisites and challenges – needs assessment report", December 2023, available at https://rm.coe.int/en-organisation-and-holding-of-elections-in-post-war-ukraine/1680aedbaf

- European Commission, DG JUSTICE (2018), Lupiáñez-Villanueva, F. and Devaux, A. Study on the Benefits and Drawbacks of Remote Voting Justice and Consumers Specific, Brussels, 2018, available at https://commission.europa.eu/system/files/2020-06/20181121_remote_voting_final_report_final_clean.pdf

- IFES (2018), Petrov G. and Chanussot T., A cybersecurity playbook. Combating threats to Ukrainian elections through good practice, November 2018, available at https://ifesukraine.org/wp-content/uploads/2019/02/IFES-Ukraine-Cybersecurity-in-Elections-Playbook-v1-2019-02-15-Eng.pdf

- IIFES Ukraine (2020a), Applegate M., Chanussot T. and Basysty V., Considerations on internet voting: an overview of electoral decision-makers, April 2020, available at https://ifesukraine.org/wp-content/uploads/2020/04/IFES-White-Paper-Applegate-Chanussot-Basysty-%E2%80%98Considerations-on-Internet-Voting%E2%80%99-Mar-2020-Eng-1.pdf

- IFES Ukraine (2020b), Basysty V. et al., Feasibility study on the introduction of new elections technology in Ukraine, February 2020, available at https://ifesukraine.org/wp-content/uploads/2019/04/IFES-Ukraine-Feasibility-Study-on-the-Introduction-of-New-Elections-Technology-for-Ukraine-v1-2020-02-13-Eng.pdf
- IFES Ukraine (2023a), Kaplan J., "Focus group findings to facilitate out-of-country voting in post-war Ukraine elections", May 2023, available at www.ifesukraine.org/wp-content/uploads/2023/11/ifes-elections-abroad-eng-web.pdf
- IFES Ukraine (2023b), Denis A. et al., "Technical assessment report: out-of-country voting in Ukraine", Draft 1, January 2023, available at https://ifesukraine.org/wp-content/uploads/2023/05/ifes-ukraine-ocv-technical-assessment-report-v1-2023-05-11-eng.pdf
- OPORA, IFES joint road map for electoral reform in Ukraine – 2023 wartime edition, 18 October 2023, available at https://old.ifesukraine.org/wp-content/uploads/2023/10/ifes-ukraine-opora-roadmap-for-electoral-reform-in-ukraine-d7-2023-10-17-eng-1.pdf
- Ukrainian CEC Regulation of 27 September 2022, No. 102, "On proposals to improve the legislation of Ukraine, aimed at ensuring the preparation and holding of elections after the termination or abolition of martial law in Ukraine" (in Ukrainian only).

The Russian Federation's war of aggression against Ukraine has caused profound and unprecedented consequences for Ukraine and Ukrainian people, including challenges to democratic processes and participation. Millions of Ukrainians have been forced to flee their homes, seeking safety, protection and assistance either within Ukraine or in neighbouring countries. In this context, Ukrainian authorities are exploring ways and means to ensure the electoral rights of Ukrainian voters, including internally displaced persons and forced migrants abroad, in a post-war period. Among the options under consideration are alternative forms of voting, including internet voting.

This study assesses the risks associated with piloting and introducing internet voting in post-war elections in Ukraine from legal, organisational and technical perspectives. It also examines the feasibility of other alternative voting methods, such as postal voting. The analysis draws on legal and factual assessment of Ukraine's current situation, international legal standards, and the Council of Europe recommendations. Additionally, it incorporates current scientific and technical expertise, as well as the experiences of countries like Estonia, Switzerland, France and Australia in the introduction and use of internet voting.

The study aims to contribute to ongoing discussions, particularly regarding internet voting, among Ukrainian electoral stakeholders, and highlights necessary modifications in legal framework and practice when taking a decision on internet voting while also assessing the associated risks. It will also be of interest to legislators and election management bodies in other countries contemplating the introduction of internet voting.

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE