

Identifying Factors Studied for Voter Trust in E-Voting – Review of Literature

Yannick Erb ¹, David Duenas-Cid ^{2,3}, Melanie Volkamer ⁴

Abstract: Trust is a precondition for the adoption of novel technologies (see, e.g., [ES21]). As more and more electoral commissions consider introducing e-voting solutions, research into voter trust in these systems grows in importance. As a basis for future research on trust in e-voting, we conducted a literature review. We identified 13 papers researching various factors influencing voters' trust in e-voting. In these papers, we determined a total of 64 potential factors, while the direction of their influence on voter trust may be either positive, negative, or both (positive/negative). These factors were subsequently systemized into five categories, ranging from socio-political to technology-related factors. These are then described and discussed. We also find shortcomings in the current empirical research on voter trust and propose directions for future research in order to address these.

Keywords: e-voting; i-voting; voter trust

1 Introduction

Digitization in society is now integrating digital technologies into all aspects of people's everyday lives, replacing analogue information with a digital form so it can be stored and processed digitally [FGR19] or creating new digital processes affecting our physical world [BMY20]. With a few exceptions, integration of digital technologies has not been as successful as expected in relation to democratic processes, such as elections and voting. In the early 2000s, the vision of voting remotely over the internet was voiced alongside growing interest in information and communication technologies (ICT), and experts were convinced that every democratic elections would be conducted using electronic voting in polling stations (e-voting) or remotely via the internet (i-voting) [Li21]. Even though ICT has been around for years, and there are success stories such as the Estonian i-voting system [En], we still cannot observe [In] widespread use of ICT for democratic processes. Use of ICT may deliver advantages for the field of voting, among others, offering improved

¹ Karlsruhe Institute of Technology, Institute of Applied Informatics and Formal Description Methods, Kaiserstraße 89, 76133 Karlsruhe, Germany. <https://orcid.org/0009-0006-7797-2061>. yannick.erb@kit.edu

² University of New South Wales, School of Information Systems and Technology Management, NSW 2052, Sydney, Australia

³ Gdansk University of Technology, Department of Informatics in Management, 11/12 Gabriela Narutowicza Street, 80-233 Gdańsk, Poland. <https://orcid.org/0000-0002-0451-4514>. david.duenas.cid@pg.edu.pl

⁴ Karlsruhe Institute of Technology, Institute of Applied Informatics and Formal Description Methods, Kaiserstraße 89, 76133 Karlsruhe, Germany. <https://orcid.org/0000-0003-2674-4043>. melanie.volkamer@kit.edu

accessibility to elections, higher efficiency in tallying [AS20] or greater convenience for younger or busy voters [LK17]; but also downsides that should likewise receive equal consideration such as security issues [LK17, FGR19], trust issues [Gi16], and social challenges such as computer literacy of the voting population [Tr16]. In the end, although offering advantages, e-voting is not only technically challenging but also impacts society and politics [Bu18].

Amongst the previous elements, “trust” appears to be one of the most relevant ones. Trust has been identified as a precondition for adoption and use of novel technologies [ES21]. The effects of missing trust in the e-voting system employed can be severe and may lead to a loss of voter confidence in elections and in overall comprehension of democracy, as was the case in the 2020 U.S. elections [SSP20, UL20]. Thus, establishing trust in e-voting solutions is crucial for democracies using such technologies. In order to tackle the topic, we aim to answer the following research question: “*Which factors influencing voters’ trust in e-voting have been researched in expert literature?*” in a generalistic manner, i.e., not focusing on specific countries, e-voting methods, or types of election.

To answer this question, we conducted a review of literature, studying empirical factors reported which potentially influence voter trust in e-voting. We consider research from different countries and regions, as well as different voting methods and types of elections. Following identification, factors are grouped thematically to enable a thematic discussion on these factors. While we identified 13 relevant papers with 64 such factors overall, and the direction of their influence on voter trust can be either positive, negative, or both (positive/negative), we also identified systematic issues with some of the research conducted and discuss directions for future research in order to encourage future research to focus on trust-related research questions in the context of e-voting.

2 Background

2.1 Electronic Voting and Internet Voting

E-voting is an umbrella term for “any process that benefits from use of [. . .] electronic technology by the election authorities [. . .] to run elections” [Bu18], including electronic voter registration, vote casting, tallying, and communication of results [Bu18].

Several countries have e-voting systems in use. The United States, for example, uses a mix of direct recording electronic voting machines and optical mark or character recognition [In]. Other countries, like Brazil, which employed an e-voting system in 1996, switched from paper voting because of election fraud [dFM17].

Envisioned by technology leaders like Bill Gates and Tim Cook, the idea of “cast(ing) [...] ballots from home or [...] wallet PCs” [GMR96] or “voting on phones” [SC21] has become a reality in what is referred to as ‘remote e-voting’ or, simply, i-voting (e.g., [ES21], [Li21]) or online voting (e.g., [BGG19], [GGB18]). For the purpose of simplicity, both terms for this special type of voting by e-voting will be subsumed under i-voting, as a clear distinction is not made in literature, and the terms are used interchangeably (see, e.g., [Li21]).

I-voting adoption has been prominently studied in the case of Estonian i-voting [FGR19, Li21], which has been used systematically since 2005, and provides much election data [ES21, SK19, So20]. Estonian i-voting, for example, is described as “cast[ing] [. . .] ballots from any internet-connected computer anywhere in the world” [En].

Licht et al. [Li21] offer an overview of literature concerned with i-voting and identify drivers and barriers to i-voting that can be observed in various contexts.

2.2 Trust in (New) Technology in General

Trust, representing a transversal concept that has been approached by different fields of research, can be broadly defined as “the belief that somebody [or something] is good, [. . .] and will not try to harm or deceive you” [Ox]. However, its inherent transversality crystallizes in the existence of various discipline-related definitions, and, in the end, the concept suffers from a lack of clarity [ES21]. Trust has been related to the need to reduce complexity and make social action affordable [Lu79], with the need for stability, transparency, and accountability [Sz03], or with the need to balance unequal knowledge distribution when facing complex systems [Gi91]. As suggested by Mayer et al.’s [23] definition (trust as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party”), trust involves a number of participants that includes a trustor, a trustee and, in some occasions, an intermediary element such as an organization.

In this regard, technology appears as a mediating element [Bo21] that is generally understood by analyzing its capacity to provide expected outcomes due to the impossibility of inferring intentionality from it [DC22a] (although recent discussions connected with AI might question this [Hu17]). Trust in technology, hence, differs from trust in organizations or people, as the trustee is no longer a moral agent but a technological artifact created by humans that has limited capabilities [Mc11]. This point of departure allows us to approach trust in relation to electoral technology, such as e-voting [ES21]; but such an approach should not prevent understanding the role played by those stakeholders having the capacity to provide trust or distrust of the system even if not directly related to its functioning [DC22a].

3 Methodology – Conducting a Literature Review

To answer the research question, a literature review is undertaken of proceedings from E-Vote-ID conferences from the years 2016–2022. The E-Vote-ID conference serves as a meeting point for interdisciplinary experts related to e-voting (i.e., merging technical topics and governance-related topics), and their proceedings will be considered as a reference for research in this field. The conference produces two proceedings per year, one includes only academic papers published in the Springer LNCS series and a second publication including

all⁵ the peer-reviewed papers presented in the conference (published by different university press jackets⁶). The E-Vote-ID proceedings for the period 2016–2022 contain 247 unique records, of which 96 were published in Springer LNCS, and 151 were published under university jackets only.

This literature review is done *ad hoc* for the conference and serves as a measure of how the topic is approached in the conference community, tracing some general guidelines to understand the strengths and weaknesses of current approaches.

3.1 Description of the Steps of the Literature Review

The steps of the literature review and number of records included/excluded in the process are displayed in Fig. 1 and are explained in more detail in the following paragraphs.

In a first step (S1), we excluded the “PhD Papers” or “Demo” articles (n=68) from the 247 records, as they report the work briefly, and in the main with no detailed explanation. To identify relevant records, we searched for explicit use of the expression “*trust*” in full text recorded (S2) in the remaining 179 records, which led to removing 44 records not containing the expression. For the remaining 135 records, the full text PDF files were retrieved as papers (S3), and a two-step eligibility assessment (S4-S5) was carried out. Exclusion criteria for the eligibility assessment (S4-S5), screening step (S2), and initial removal of demo/PhD records (S1) are displayed in Tab. 1. In the first step of the eligibility assessment (S4), the remaining 135 papers were again searched for the expression “*trust*” and corresponding passages were read in detail, searching for factors that may influence voter trust in e-voting. That allowed us to exclude non-relevant records as “No Factors” (n=63). As this review sets out to identify empirically studied factors that influence voters’ trust in e-voting, a second assessment step (S5) reports that neither report a user nor expert study nor a literature review with matching focus were excluded as “No Study” (n=59). The final number of records fulfilling the research criteria (n=13) were included in the review (In1).

Fig. 2 provides an overview of papers per year according to whether they are related to trust or not and those actually conducting empirical studies on factors influencing voters’ trust. It reveals that research on topics related to voter trust makes up a substantial part of the conference proceedings, with at minimum 28% of articles (2022) published being related to voter trust. However, empirical research on voter trust does not reach the same numbers. Starting from 2017 (n=1), on average, only 7.27% of articles are concerned with empirical research on voter trust. Linear trend data shows increasing interest in empirical research into voter trust while the general interest in voter trust related topics seems to decrease. Interest in empirical research on voter trust peaked in 2019 and 2021.

⁵ Except for the proceedings of the E-Vote-ID 2022. Here, papers that are part of the Springer LNCS publication are not part of the university press cover publication.

⁶ 2016–2017: TUT Press, 2019–2020: TalTech Press, 2021–2022: University of Tartu Press

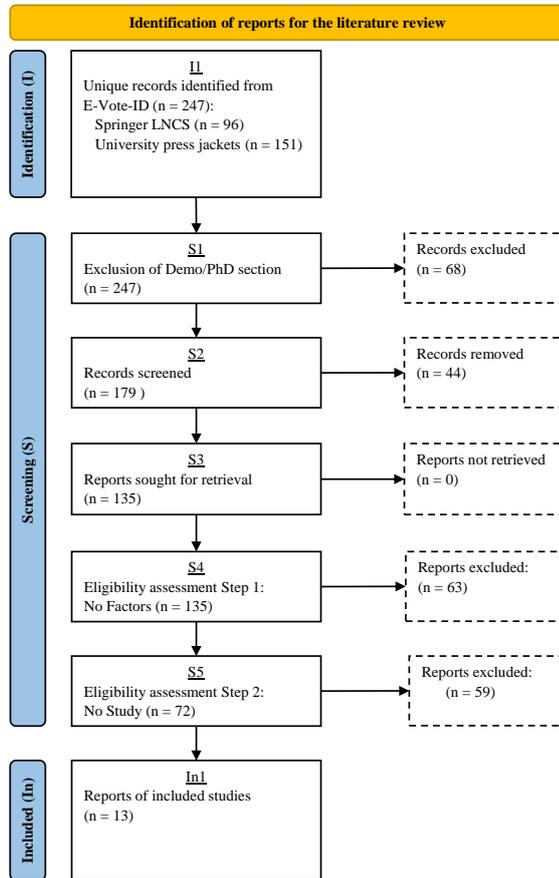


Fig. 1: Process of the literature review from the E-Vote-ID conference (adapted from [Pa21])

Step	Criterion	Description / Explanation	#Records excluded
S1: Exclusion of demo/PhD Section	Demo/PhD Paper	Papers of the E-Vote-ID PhD paper or demo section, being short and stating research is in progress.	68
S2: Screening	Not “*trust*”	All records that do not contain “*trust*” in the full text are excluded as they are outside the scope of this review.	44
S4. Eligibility assessment – Step 1	No factors	Papers for which no text passage that may hold a factor influencing voter trust could be identified (e.g., “trust” only in the name of institutions).	63
S5. Eligibility assessment – Step 2	No study	Papers that did not report user or expert studies; or were literature reviews with a matching focus.	59

Tab. 1: Overview of exclusion criteria for the different steps

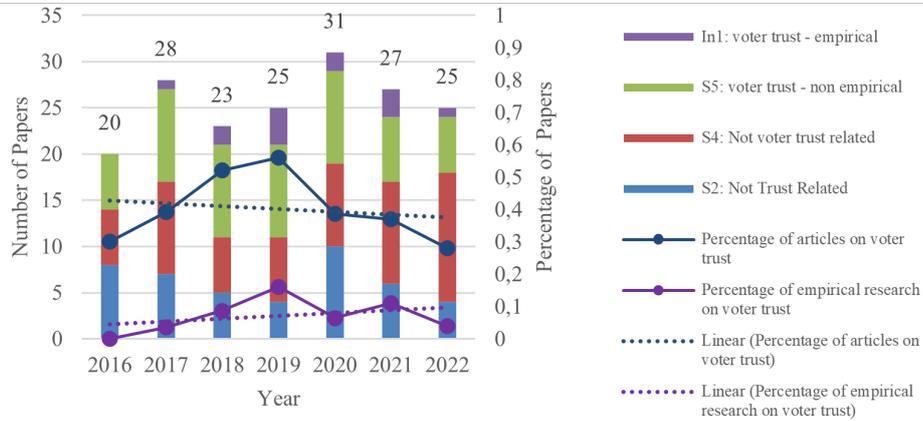


Fig. 2: Distribution of E-Vote-ID articles relating to trust (after excluding demo/PhD section records (S1))

The 13 papers included in the review are [Ag22], [AS20], [BGG19], [ES21], [FGR19], [GGB18], [Li21], [LK17], [SK18], [So20], [SK19], [Zo19], and [Zo21]. Appendix A1 (see [EDCV]) provides an overview of these, including the research approach chosen by the authors and the area, the type of elections, and the voting method studied.

3.2 First Results on Type of E-Voting and Considered Context

Regarding the 13 papers which we identified, it is noteworthy that most papers included are user studies ($n=11$), except for Licht et al. [Li21], who conduct expert interviews to inform their research, and Lindemane & Kuzmina [LK17] conducting expert interviews. Nine out of the thirteen papers focus on European countries. Some countries are studied multiple times, for example, Estonia, which is examined three times ([ES21], [SK19], [So20]), and Canada ([BGG19], [GGB18]) and Switzerland ([FGR19], [SK18]), studied in two papers respectively. Almost every paper focuses on national or European parliament elections. However, Alsadi & Schneider [AS20] study the case of representative elections in the UK, and the two studies focusing on Canada research indigenous self-governance of First Nations in Canada. Looking at the voting type studied, except for two studies on general e-voting ([FGR19], [LK17]), all use i-voting systems as subject of their research. Regarding the notion of trust, we find that only three studies define the term trust. Ehin & Solvak [ES21] and Agbesi et al. [Ag22] refer to the trust definition of Mayer et al. [MDS95], as presented in section 2.2, whereas in Zollinger et al. [Zo19] trust is identified as a mental model of voters. Out of the eight qualitative studies ([Li21], [Zo21], [BGG19], [FGR19], [Zo19], [GGB18], [LK17], [Ag22]) included in this review, only four mention how trust was measured in their studies ([Zo21], [FGR19], [Zo19], [Ag22]) stating that the word and notion of trust was used by the participants of their studies. For the five quantitative studies

([ES21], [So20], [AS20], [SK19], [SK18]), trust was measured by three studies using a scale from 0-10 for “Do you trust the procedure of internet voting?” or similar questions, with 0 representing the lowest level of trust and 10 the highest ([ES21], [SK19], [SK18]), and one study reports their participants to use the term trust ([AS20]).

3.3 Process to Identify and Categorize Potential Factors in Influencing Trust

For further examination, the full text of the 13 papers was analyzed in detail to identify potential factors they study for voter trust in e-voting. The corresponding passages were recorded in an Excel spreadsheet, along with the source paper and pages, a factor name for the factor described in the passage, a unique factor ID for every factor-passage combination, and coding for the direction of influence on voter trust into positive, negative, or positive/negative. Factors described as enhancing voter trust in the corresponding text passage were coded as positive for this occurrence, those described as decreasing voter trust or increasing distrust were coded as negative, and occurrences for which the influence could swing either way or was unclear were coded as positive/negative. For example, the text passage ‘Five participants also mentioned it as a confidence or trust feature, like P11 mentioned that it “give(s) a little more confidence” [Zo21], was coded with the factor name “Verifiability (General)” and direction of influence positive (Ex1), whereas for the text passage ‘A verification impact was raised, mainly decreasing trust, e.g.,’ I don’t trust the application after verification, even if the tracking number is private” (P33), even though an opposite positive effect on trust was also mentioned by some users: “the second phase makes me feel secure” (P4)’ [Zo19] was coded with the same factor name but positive/negative regarding direction of influence (Ex2).

Coding was carried out inductively. Text passages containing a factor already described before were coded with the existing factor name. Where a novel factor was described, a new factor name was created, taking the wording of the text passage into account. The coding of text passages and factors was performed by a single coder. The identified factors were then inductively grouped thematically into distinct categories, with consultation and discussion between the authors.

4 Results

4.1 Overview of Individual Factors Influencing Voter Trust in E-Voting

The procedure described above led to 133 text passages with factors described as influencing voter trust in e-voting, of which 56 were coded as positive, 55 as negative, and 22 as positive/negative. Of these, 64 unique potential factors could be identified. Twenty-eight of these were only associated with text passages coded as positive, 22 only with text passages coded as negative, and 14 associated with text passages coded as positive/negative at least

once or as positive for one text passage and as negative for another. Continuing the example from section 3.3, the factor “Verifiability (General),” as being associated with a text passage coded as “positive/negative” at least once, is coded as exerting “positive/negative” influence on voter trust. Appendix A2 (see [EDCV]) shows an overview of all factors and their trust codings. The categorization of factors, as we described above, leads to five distinct categories. The categories and number of factors grouped into the respective categories can be observed in Tab. 2.

Category	Number of Factors
Socio-Political Sphere	11
Individual Sphere	9
Trust in other Technology/Institutions/People	12
Process Related	4
Technology Related	28
	64

Tab. 2: Overview of categories and number of factors in each category

4.2 Categorization of Potential Factors Studied for Voter Trust in E-Voting

The categories identified and factors they embrace are presented subsequently below. For each category, the identified factors are presented in a table alongside a description of the factor, its influence on trust (P=positive, N=negative, P/N=positive/negative), the literature it is based on (its numbering in the references), and whether the factor is explicitly empirically validated or not for each of its literature sources (in the occurrence of paper in source column; E=empirically validated, T=theoretically only, E/T=theoretically and empirically validated). Furthermore, it can be seen whether a factor has been reported for general e-voting (E), for i-voting (I), or both (E/I). Even though this literature review focuses on literature that empirically researches voter trust, there are factors brought up by the empirical literature we researched that are not empirically validated in the studies reviewed. However, so as not to lose any factors brought up by the literature reviewed, these are still reported and discussed alongside empirically validated ones but are accordingly only marked as being theoretically validated.

4.2.1 Socio-Political Sphere

This category encompasses factors tied to the voters’ social sphere, such as trusted elites or a voter’s social media bubble and factors linked to voters’ political sphere, such as a country’s political system, the political discourse, and the position of political parties. Although divided into two subcategories for better visualization, both spheres are intertwined and, thus, are discussed alongside each other in the literature. In total, this category contains

11 factors, which are coded 21 times and based on four source papers. The factors in both subcategories are only discussed for i-voting in the literature. Tab. 3 provides an overview of the factors grouped into the subcategory *Social Sphere*.

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Heuristics	Voters use heuristics as a shortcut for decision-making on complex technology.	P/N	[ES21]	[T]	[I]
Social Cue Taking	Voters rely on cues from their own social sphere when deciding on level of trust in e-voting.	P/N	[ES21]	[T]	[I]
Trusted Social Actors	Trusted social actors influence the approach towards and perception of e-voting of voters.	P/N	[ES21]	[T]	[I]
Social Media	Social media influences the approach towards and users' perception of e-voting.	P/N	[Li21]	[E/T]	[I]
Social Trust	General trust within society is important for adoption of voting technology. High levels of general trust increase the likelihood of trust in new voting technology and the authorities dealing with them.	P	[Ag22]	[E]	[I]

Tab. 3: Socio-political factors in the subcategory *Social Sphere*

Tab. 4 does the same for the subcategory *Political Sphere*. Please note that the factor "Heuristics" is shown in both tables for completeness, even though it is not part of any of the subcategories but resides on a higher level of abstraction.

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Heuristics	Voters use heuristics as a shortcut for decision-making on complex technology.	P/N	[ES21]	[T]	[I]
Political Cue Taking	Voters consider political actors' opinions and perceptions when deciding on trust in e-voting.	P/N	[Ag22], [ES21]	[T], [E/T]	[I]
Trusted Political Actors	Trusted political actors influence the approach towards and perception of e-voting of voters.	P/N	[Ag22], [ES21]	[E], [T]	[I]

Continued on next page

Tab. 4: Socio-political factors in the subcategory *Political Sphere*

Tab. 4 – continued from previous page

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Political Discourse	Current political discourse on e-voting influences voters' positions and attitudes toward e-voting.	P/N	[Ag22], [Li21]	[E], [E/T]	[I]
Perception of Administration	Positive public perception of administration of the election (e.g., being local).	P	[SK18]	[T]	[I]
Account for Political Culture	The voting system and functionality fit the political culture and voting procedure voters are used to, in the country the voting system is employed in.	P	[SK18]	[E]	[I]
Foreign Interference on Political Scene	The threat of malicious actors influencing the political landscape of a country.	N	[Ag22]	[E]	[I]

Tab. 4: Socio-political factors in the subcategory *Political Sphere*

4.2.2 Individual Sphere

The second category of factors entails factors that originate in the voters themselves, such as their education, experiences, knowledge, and perceptions. “Individual Sphere” contains nine factors that are coded ten times in total, and are distributed across six sources. We can observe that even though six sources discuss the factors, all of them only refer to i-voting. Tab. 5 provides an overview of these factors.

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Perception of Technology	The voter's negative perception of the technologies/e-voting system in use and their security.	N	[Li21]	[E]	[I]
Changed Voter Behavior	Change in voting behavior leads to insecurities and opposition to the novel technology.	N	[BGG19]	[E]	[I]
Voter Education	Voters' level of education and cognitive sophistication (measured by the type of highest educational degree).	P/N	[ES21]	[E]	[I]

Continued on next page

Tab. 5: Factors in the category “Individual Sphere”

Tab. 5 – continued from previous page

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Past Experience / Path Dependency	Voters' past experiences with e-voting or with related technologies.	P/N	[Li21]	[T]	[I]
Experiences with Electronical Services in the Public Sector	Positive and plenty of experience with other electronic services in the public sector.	P	[SK19]	[E]	[I]
Computer Literacy	Voters have sufficient computer literacy and skills.	P	[SK19]	[E]	[I]
Lack of knowledge in Internet Technologies	Voters lack knowledge of internet technologies that form the basis for e-voting solutions.	N	[Zo19]	[E]	[I]
Voting Electronically	Voters have actually voted electronically in elections.	P	[SK19]	[E]	[I]
Additional Information	Sufficient additional information is given to the voter to understand the system and base a judgment on.	P	[Zo21]	[E]	[I]

Tab. 5: Factors in the category "Individual Sphere"

4.2.3 Trust in other Technology/Institutions/People

The category "Trust in other Technology/Institutions/People" encompasses factors tied to voters' trust in related technologies, institutions, and people that may (not) be transferred to e-voting. The category holds 12 factors in three subcategories. These are coded 24 times and appear in 7 out of the 13 papers included in the literature review. We find that several factors, especially all factors of the *Trust in Technology* subcategory, are reported for general e-voting as well as i-voting in particular. Tab. 6 provides an overview of the factors in this category.

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Trust in Novel Technology (T)	Trust-Transference of trust in novel technology to e-voting.	P/N	[LK17]	[E]	[E/I]
Trust in Related Technology (T)	Trust in technologies related to e-voting (e.g., internet banking) and technology in general.	P	[FGR19], [Zo19]	[E], [E]	[E/I]
Correlation to Trust in Other Institutions (I)	Correlation of voters' trust in other institutions and their trust in e-voting.	P/N	[ES21]	[E]	[I]
Trust in Institutions (I)	Trust-transference of voters' trust in (state) institutions.	P	[Ag22], [FGR19], [Zo19]	[E], [E], [E]	[E/I]
Trust in Electoral System (I)	Trust in the current electoral system (involving various parties).	P	[Ag22]	[E]	[I]
Mistrust in Institutions (I)	Trust-transference of voters' mistrust in other institutions (that are in charge of the election) to e-voting.	N	[Li21]	[E]	[I]
Institutional Incompetence (I)	The election officials lack technical expertise when it comes to implementing voting technologies.	N	[Ag22]	[E]	[I]
Trust in Professionals (I)	Trust-transference of voter trust in professionals dealing with the technologies in use.	P	[Ag22], [FGR19]	[E], [E]	[E/I]
Trust in Media (I)	Trust in the media to expose corruption or cheating.	P	[Ag22]	[E]	[I]
Trust in Vendor (I)	Trust in the vendor of the election technology in use and knowledge of their affiliation and reputation.	P	[Ag22]	[E]	[I]
Mistrust in Vendor (I)	Mistrust in the vendor of the election technology in use, as they are involved with nation-states perceived as untrustworthy.	N	[Ag22]	[E]	[I]
Trust in Paper Voting (PV)	Trust-transference from trust in paper voting to using e-voting.	P	[So20]	[T]	[I]
*Subcategory: (T) = Trust in Technology, (I) = Trust in Institutions/People, (PV) = Trust in Paper Voting					

Tab. 6: Factors in the category "Trust in other Technology/Institutions/People"

4.2.4 Process Related

For the “Process Related” category, we find factors tied to the election proceedings, organization, vote counting, and election results. This category covers four factors in two subcategories. The factors are based on three source papers and coded four times. Tab. 7 provides an overview of the category.

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Transparency (P)	Transparency of the voting process (e.g., voters can observe every step of the voting process).	P	[FGR19]	[E]	[E]
Understandability of Election Proceedings (P)	Understandability of the voting process (e.g., voters understand every process step).	P	[Zo19]	[E]	[I]
Immediate Results (R)	Election results can be provided immediately.	P	[GGB18]	[T]	[I]
Simplifying Tabulation (R)	Election tabulation is simplified and can be performed automatically.	P	[GGB18]	[T]	[I]
*Subcategory: (P) = Election Proceeding, (R) = Election Result					

Tab. 7: Factors in the category “Process Related”

4.2.5 Technology Related

The largest category contains factors tied to the e-voting system, its technical implementation and understandability, security and data privacy propositions, and verifiability of votes. The category contains 28 factors in 5 subcategories. They are coded 74 times in total and based on 10 out of the 13 papers included in the review. Tab. 8 provides an overview of the first four subcategories, and Tab. 9 provides an overview of the subcategory *Security & Privacy*, which is presented separately due to its size.

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Lack of Trust in one Component (S)	A lack of voter trust in one system component undermines trust in the whole system.	N	[ES21]	T	[I]

Continued on next page

Tab. 8: Factors in the category “Technology Related” (with the subcategory *Security & Privacy* excluded)

Tab. 8 – continued from previous page

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
System Reliability in Verifiability (S)	Voters have a negative attitude towards reliability of the verifiability mechanism (e.g., because of missing additional information to base judgments on).	N	[Zo21]	[E]	[I]
Demonstration (S)	Demonstration of the system to the public and/or within institutions.	P	[Li21], [SK18]	[E], [E]	[I]
System Reliability (S)	Reliability of the system as a whole (e.g., in case of power cuts, failures or outages)	N	[Ag22]	[E]	[I]
Usability (S)	Ease of use and clearly stated rules/steps must be followed.	P	[Ag22]	[E]	[I]
Technical Failure (T)	Technical failures and problems accepting their occurrence by the voter.	N	[Ag22], [Li21], [FGR19]	[E], [E], [E]	[E/I]
Distributed Ledger Technology (T)	Immutability induced by usage of distributed ledger technology.	P	[AS20]	[T]	[I]
Complexity (T)	E-voting systems are complex to understand and use.	N	[Ag22], [Li21], [Zo21]	[E], [E], [T]	[I]
Complexity of Verifiability (T)	Verifiability methods are complex to understand, and voters question their necessity.	N	[Zo21]	[T]	[I]
Verifiability (General) (V)	Verifiability is a key feature of creating observability for voters and the general public.	P/N	[Ag22], [Zo21], [So20], [AS20], [Zo19], [SK18]	[E], [E], [E], [E/T], [E], [E]	[I]
Possibility to Verify (V)	Being able to verify one's vote without necessarily performing the verification.	P	[So20], [AS20], [SK19]	[E/T], [E], [E]	[I]
Traceability (V)	It is possible for voters to trace their vote and ensure it matches their intention.	P	[Ag22]	[E]	[I]
Implementation (V_A)	The specific implementation of verifiability methods.	N	[Zo21]	[E]	[I]
Novelty (V_A)	Verifiability methods are novel, new, and unknown to voters.	N	[Zo21]	[T]	[I]

Continued on next page

Tab. 8: Factors in the category “Technology Related” (with the subcategory *Security & Privacy* excluded)

Tab. 8 – continued from previous page

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Understandability Issues (U)	Voters do not or cannot fully understand the e-voting system.	N	[Ag22], [Li21]	[E/T], [E]	[I]
Lack of Understanding of Verification (U)	A lack of understanding of the verifiability method b use, its available features, and prerequisites.	N	[Zo21], [AS20], [Zo19]	[E], [T], [E]	[I]
*Subcategory: (S) = System Related, (T) = Technology Related, (V) = Verifiability, (V_A) = Verifiability Aspects, (U) = Understandability					

Tab. 8: Factors in the category “Technology Related” (with the subcategory *Security & Privacy* excluded)

For *Security & Privacy*, several factors are reported for e-voting and i-voting. For all other categories, however, only damage to the public was reported for both voting types.

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Data Privacy (P)	Voter data may be disclosed to private vendors selling e-voting technology.	N	[Ag22], [FGR19]	[E], [E]	[E/I]
Privacy Concerns in Verifiability (P)	The use of verifiability methods is viewed as a privacy breach by voters.	N	[Zo21]	[T]	[I]
Source Code Publication (S)	Publication of the source code or part of it to the public to engage with public and external experts.	P	[SK18]	[E]	[I]
Expert Audit (S)	Expert auditing of the e-voting system.	P	[Ag22], [SK18]	[E], [E]	[I]
Enhanced Voting Security (S)	Enhanced security of e-voting systems.	P	[Ag22], [AS20]	[E], [T]	[I]
Security Concerns (S)	Concerns regarding the security of e-voting systems (may include not only actual security breaches/risks but also perceived security).	P/N	[Ag22], [Li21], [FGR19], [Zo19]	[E], [E], [E], [E]	[E/I]
Security Risks (S)	Risks related to the security of systems.	P/N	[Ag22], [Zo21]	[E/T], [T]	[I]

Continued on next page

Tab. 9: Factors in the subcategory *Security & Privacy* of the category “Technology Related”

Tab. 9 – continued from previous page

Factor Name	Description	Influence	Source	Empirical vs. Theoretical	Voting Type
Security Breaches (S)	A breach in voting system security may allow attackers to tamper with or disclose data.	N	[Li21], [FGR19]	[E], [E]	[E/I]
Damage to Public (S)	Problems in an e-voting system's security may lead to harm to the public community in general.	N	[FGR19]	[E]	[E]
Vote Forging (S)	Forging of votes in any way.	N	[Ag22], [FGR19]	[E], [E]	[E/I]
Authentication (S)	Authentication to prevent unauthorized logins to the voting platform as a security assurance.	P	[Ag22]	[E]	[I]
Explainability of Security Propositions (S)	Election authorities provide a complete and understandable explanation of levels of security provided.	P	[Ag22]	[E]	[I]
*Subcategory: (P)=Privacy, (S)=Security					

Tab. 9: Factors in the subcategory *Security & Privacy* of the category “Technology Related”

5 Discussion

5.1 Potential Factors for “Socio-Political Sphere”

Forming judgments on novel technology is complex, and citizens use effort reduction strategies to help form an opinion, such as heuristic methods. Literature describes how citizens use cue-taking from trusted social or political actors as an heuristic that helps them decide on their opinion towards i-voting. “Because of the cognitive and temporal costs of rational reasoning, individuals look to other trusted social actors [. . .] for signals suggesting what to think or how to behave” [ES21].

Two sources providing social cues influencing voter opinions for trusting i-voting were determined: Trusted social actors [ES21] and social media [Li21]. However, there is no empirical data on either cue-taking from social actors or social media provided by the authors. Those cues voters rely on when forming judgments on i-voting may also come from political parties, as empirically studied in the case of Estonian i-voting by Ehin et al. [ES21]. They found a correlation between voters’ position and political leanings and parties they voted for: those voting for parties with a high trust position toward i-voting also have higher trust in i-voting and vice-versa. This relation is described as being vivid and mutable, so party supporters change their individual position if their chosen party’s position on trust in i-voting changes. This is especially interesting because it opens the door

to considering new elements for understanding trust-related issues since parties' position on electoral innovation might be based on their expectations of how it could affect their electoral prospects and hence, this potential fear of innovation might be transferred to a trust-related dimension.

Besides cue-taking, other elements influencing individual opinions regarding trust and distrust were uncovered: the political discourse [Li21], the fear of foreign interference in the political landscape [Ag22], and general social trust within society [Ag22]. Data on Swiss trust in e-voting suggests that an e-voting system's features must furthermore match the political culture of the country it is employed in to have the intended effect [SK18]. For example, the possibility to cast multiple votes as is used in Estonia and considered trust building there, did not increase Swiss trust in e-voting as it did not correspond to Swiss voting behavior.

5.2 Potential Factors for “Individual Sphere”

Voter trust is negatively impacted by voters' perception regarding the technology itself. The lack of comprehension of how complex voting systems work or fears and concerns regarding their security are listed among these factors [Li21]. However, a change in voter behavior may also induce distrust. This can be observed in the case of Canadian First Nations, which oppose any change for historical reasons, and accordingly are opposed to i-voting even though its use would allow them better self-administration [BGG19].

Similarly, voter education [ES21] and computer literacy [SK19] impact voter trust. Ehin et al. [ES21] discovered that during the earlier years of Estonian i-voting, lower levels of education were associated with higher trust, shifting in later elections to higher levels of education, generating added trust. However, a statistical interpretation and explanation of this reported effect is not possible based on the data used. Regarding computer literacy, on the other hand, a positive relationship was identified [SK19]. In accordance with the above, voter education levels appear not to be explicative variables for understanding trust-related positions, while computer literacy appears to be a good predictor for them.

Voter trust also appears to be influenced by past experiences voters had [Li21]. This so-called path dependency can be observed in all fields of the social sphere and, hence, for use in election systems. In the case of Estonia, for example, extensive experience voters have gained using electronic services in the public sector is also considered as increasing trust in i-voting [SK19].

5.3 Potential Factors for “Trust in other Technology/Institutions/People”

Previous levels of trust in elements relating to implementation of e-voting and i-voting appear to exhibit a positive correlation with further adoption of it. For example, voters with higher levels of trust in technology [Zo19] or who are used to related technologies, such as e-banking [FGR19], also tend to trust e-voting and i-voting solutions. Similarly, people

working in digitized environments or experiencing digitization processes are found to be more likely to adopt i-voting [Zo19].

Similar patterns for e-voting and i-voting are further described in relation to trusting other institutions. A positive correlation has been described between trust in i-voting and trust in political institutions, such as the parliament, government, or politicians [ES21, Zo19]. But this relation is limited to certain conditions, and for such a trust transference towards e-voting to succeed, the government must be sole guarantor of the system [FGR19]; and even then, there is no guarantee that trust established with political institutions is going to transfer to i-voting [Li21]. For i-voting, it is reported that the same relationship also works in the opposite direction; systems can only be as trustworthy as the people proposing and constructing them: e-voting technologies might not be accepted if voters do not trust election authorities [Li21].

Finally, trust transference is also observed from other voting channels. Besides the obvious differences between paper and e-voting and the various risks involved, trusting paper voting has been found to positively influence levels of trust concerning i-voting [So20]. In this case, we might infer that trusting institutions can transversally positively influence different voting channels, and therefore, the explanation for transferring trust from paper to e-voting might not be due to the system itself but due to previously existing levels of trust.

5.4 Potential Factors for “Process Related”

E-voting trust-related elements are described as extending beyond the technology itself, including elements relating to the process followed or employed for its implementation and management. For example, voters have increased trust in processes they understand [Zo19]. Simpler voting systems, such as traditional paper-based voting, are based on steps that are easy to understand and observe for every voter [FGR19, Zo19], although this is not reproduced in the same manner in e-voting or i-voting processes. Mistakes made by humans involved in this process are described as easier to accept than those made by software [FGR19]. Increasing transparency by sharing backstage processes of an e-voting election via, for example, live broadcasting may help mitigate these issues [FGR19]. While transparency was reported for general e-voting systems, understandability was highlighted for i-voting as a voting method, indicating that transparency of background processes alone may not be sufficient for voters to trust i-voting solutions, as they do not understand the steps necessary to take in order to vote or the processes behind these.

On the other hand, i-voting also delivers some simplification of processes that help build trust. The use of technology increases processual convenience, providing simplified ballot tabulation and immediate results and positively impacting trust in voting and election results, and between the government and citizens [GGB18].

5.5 Potential Factors for “Technology Related”

As this category covers many factors, it is divided into five subcategories, the first of which is *System-Related Aspects*, all of which factors are only described for i-voting. Serving as a general remark, it must be noted that lacking trust in a single system component can undermine the trust in the whole i-voting system [ES21]. On the other hand, demonstrating the system to the public before using it for elections is described as a method contributing to helping build trust in the new system [Li21, SK18], empirically observed in use of a demo website in Switzerland [SK18]. Demonstrations such as this may include not only demonstrations to voters but also rhetoric and competence demonstrations with a focus on institutions [Li21].

For the *Technical Aspects* subcategory, the literature suggests that technical failure is reported to be a factor negatively influencing trust in e-voting as well as i-voting solutions [Ag22, FGR19, Li21]. Aligned with this, system or software failures are difficult to accept by voters [FGR19]. Demonstrations of technology, once again, were proven effective to re-establish trust in systems that had previously experienced technical failures [Li21]. Regarding i-voting in particular, the complexity of voting systems contributes negatively to building trust [Ag22, Li21], especially when verification is in place [Zo21].

Privacy & Security aspects are important elements in relation to technical aspects of e-voting and i-voting. Looking at the privacy propositions e-voting and i-voting are associated with, there are concerns that private companies offering such voting solutions may obtain voters' personal data and voting preferences [Ag22, FGR19]. Moreover, for the case of i-voting, voters may view verifiability methods as privacy breaches [Zo21]. Regarding security, we find that enhancing an i-voting system's security is a factor positively influencing voter trust in the system [Ag22, AS20]. However, security is not an obvious element that average voters can understand immediately, and therefore, perceived security is more important than security actually provided. This perception and, consequently, trust are negatively influenced by security concerns voters may have [FGR19, Li21, Zo19], security risks they can perceive [Zo21], or security breaches occurring [FGR19, Li21]. Such negative effects on trust are reported for general e-voting as well as i-voting in particular. This is especially crucial, as e-voting systems may be available globally and can be attacked from anywhere in the world, affecting the entire nation and leading to fear of harm to the public setting [FGR19]. Publishing source codes and expert audits are considered as enhancement measures to increase levels of trust in i-voting solutions [SK18]. However, a survey conducted on i-voting usage in Switzerland revealed that expert audits were supported as trust-building measures, but not publication of source codes [SK18]. To increase levels of trust in and integrity of i-voting process, verifiability is one of the key trust features for i-voting systems [AS20]. It provides mechanisms for voters (individual verifiability) and the public (universal verifiability) to observe correct system behavior [AS20]. Its positive impact in increasing confidence in election results is supported by the findings of qualitative (e.g., [Zo21], [Zo19]) and quantitative studies (e.g., [So20], [AS20]). However, verification may also increase distrust, for example, because of privacy concerns or because voters cannot see its purpose [Zo19]. Interestingly, the possibility of verification has already increased trust in Estonian

studies, even if it was not actually used [So20, SK19]. For non-national representative elections, it was considered a bonus for a case study in England but deemed necessary for general elections [AS20].

A final subcategory is *Understandability*. We find that for i-voting, understandability issues lead to increasing security concerns and, thus, mistrust [Li21]. This is especially true for systems that also apply verifiability. A lack of understanding of verifiability, its purpose, and the way it works may lead to mistrust [AS20, Zo19], as verification is not natural for voters [Zo19] and may lead to their questioning the integrity of the election [AS20]. Additional information, evidence, and proofs [Zo21], as well as easy-to-perform mechanisms [Zo19], may help mitigate these problems. Understandability issues were not reported for general e-voting.

6 Conclusion

This work set out to answer the question of which factors are reported as potentially influencing voter trust in e-voting, performing a literature review of E-Vote-ID conference proceedings dating back to 2016. We identified 13 articles (see A1 in [EDCV] for an overview of these) with relevance for the matter of interest, from which we could identify 64 potential factors and their described direction of influence on voter trust in e-voting and i-voting. These factors were grouped into five distinct categories for further discussion, namely (1) “Socio-Political Sphere,” (2) “Individual Sphere,” (3) “Trust in Other Technology/Institutions/People,” (4) “Process Related,” and (5) “Technology Related.” Our findings and empirical literature identified can be used as a stepping stone for further research and assistance to understand how voter trust in e-voting can be established.

This work brings with it four major implications for research and practice. First, we present and discuss a large set of factors reported as influencing voter trust in e-voting and i-voting for different settings and countries. We believe these are potential factors worth considering, as their (direction of) impact may differ across different voting settings and/or countries. To the best of the authors’ knowledge, this is the first literature review of this kind, considering multiple countries and e-voting scenarios. The importance of our review’s findings has grown as research on e-voting in general has become more timely and important due to the COVID-19 pandemic (see, e.g., [KDCK21]) and as trust is a precondition for using novel technologies [ES21].

Second, a lack of empirical research on voter trust becomes apparent when regarding the distribution of papers covering the topic of voter trust in E-Vote-ID (see Fig. 2), which can be viewed as a reference for research in the field. Furthermore, this research is Europe-centric and focuses mainly on i-voting. Therefore, e-voting research lacks points of view, including non-European or developing countries, other e-voting methods, and voting scenarios not included in the review.

Third, the factors identified are categorized for further use in research and practice, building a stepping stone for future research in the field or a reference point for designing new e-voting solutions or the evaluation of existing systems. While we acknowledge that the

(direction of) impact of the potential factors identified may vary for different use cases, we argue that a large set of factors worth considering for e-voting solutions enables solutions perceived as being more trustworthy by voters. We also discuss the factors with regard to their respective voting type. Most factors have been studied prominently or only for i-voting. However, general e-voting and i-voting share factors regarding data privacy, security issues, and technical failure. Also, trust transference from trust in technology, institutions, and professionals can be observed for both voting types. On the other hand, differences seem to be present for the proceeding of the election, with trust in e-voting being influenced by the transparency of the proceedings but trust in i-voting by its understandability to the voter. The discrepancies in factors for e-voting and i-voting may be due to the relative majority of i-voting as studied voting method for the reviewed literature.

Fourth, current empirical research on voter trust seems to focus largely on the technical point of view, as we find that factors relating to the technology in use constitute almost half of factors determined, and 70% of articles in the review are associated with this category. Security topics and verifiability comprise the greatest number of factors within this category. Thus, we identify a need for more research in directions other than technology. For example, factors relating to the e-voting process or the voters themselves appear to have been insufficiently studied, and research on socio-political factors is mainly based on two studies ([ES21] and [Ag22]).

However, this work does not come without limitations, which open the door to further improvements and can be summarized as follows. For this work, only papers published in E-Vote-ID conference proceedings were used. Thus, interesting related work or studies from other journals and conferences are not included, along with factors that may be described there. Furthermore, the coding of articles was performed by only a single researcher. The absence of a second coder and co-coding discussion may lead to subjective bias concerning the text passages chosen and interpretation of these that leads to uncovering/naming the factors and direction of their influence. However, the categorization of factors found was performed in a discussion between the authors, decreasing subjective bias in this process step. Finally, there is only one axis used for capturing the direction of influence. However, there are more fine-grained views on trust in e-voting. For example, Duenas-Cid [DC22a, DC22b] consider trust and distrust on two different axes, each from “(Dis)Trust” to “Not to (Dis)Trust,” leading to a more fine-grained interpretation.

To leverage the work done in this article and overcome its limitations, we propose future research directions in the field of voter trust in e-voting. Building on this work, empirical studies of voter trust in e-voting could be conducted with or without focusing on specific factors or categories. Ideally, these studies would focus on categories considered underrepresented by this work (such as individual, socio-political, or process-related factors) and would be designed as cross-country studies to grasp effects shared by several countries and find differences between them. Such a call for cross-country considerations is also formulated for the European Union in [Tr16]. Studies like this would help to close the gap in empirical research on voter trust identified above. Furthermore, future work should investigate the differences in trust behaviour with regard to different voting methods (such as general e-voting, i-voting, etc.) in more detail or breadth. This could be, for example,

done by building on this study but including other outlets as well to increase the number of publications in the review.

7 Acknowledgments

The work of David Duenas-Cid has received funding from the Electrust (EU H2020 MSCA programme, grant agreement no. 101038055) and Dynamika (braku) zaufania w kreowaniu systemów głosowania internetowego (Narodowe Centrum Nauki, OPUS-20 competition, grant agreement no. 2020/39/B/HS5/01661) projects.

This work was supported by funding from the project “Engineering Secure Systems” of the Helmholtz Association (HGF) [topic 46.23.01 Methods for Engineering Secure Systems] and by KASTEL Security Research Lab.

References

- [Ag22] Agbesi, Samuel; Dalela, Asmita; Budurushi, Jurlind; Kulyk, Oksana: ”What Will Make Me Trust or Not Trust Will Depend Upon How Secure the Technology Is”: Factors Influencing Trust Perceptions of the Use of Election Technologies. In (Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Germann, Micha; Glondu, Stéphane; Hofer, Thomas; Krivonosova, Iuliia; Martin-Rozumilowicz, Beata; Rønne, Peter; Zollinger, Marie-Laure, eds): Seventh International Joint Conference on Electronic Voting (E-Vote-ID) 2022. University of Tartu Press, Tartu, Estonia, pp. 1–17, 2022.
- [AS20] Alsadi, Mohammed; Schneider, Steve: Verify My Vote: Voter Experience. In (Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Glondu, Stéphane; Krivonosova, Iuliia; Kulyk, Oksana; Küsters, Ralf; Martin-Rozumilowicz; Rønne, Peter; Solvak, Mihkel; Spycher Oliver, eds): Fifth International Joint Conference on Electronic Voting (E-Vote-ID 2020). TalTech Press, Tallinn, Estonia, pp. 280–295, 2020.
- [BGG19] Budd, Brian; Gabel, Chelsea; Goodman, Nicole: Online Voting in a First Nation in Canada: Implications for Participation and Governance. In (Krimmer, Robert; Volkamer, Melanie; Cortier, Veronique; Beckert, Bernhard; Küsters, Ralf; Serdült, Uwe; Duenas-Cid, David, eds): Electronic Voting, Lecture Notes in Computer Science, pp. 50–66. Springer International Publishing, Cham, 2019.
- [BMY20] Baskerville, Richard L.; Myers, Michael D.; Yoo, Youngjin: Digital First: The Ontological Reversal and New Challenges for Information Systems Research. *MIS Quarterly*, 44(2):509–523, 2020.
- [Bo21] Bodó, Balázs: Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society*, 23(9):2668–2690, 2021.
- [Bu18] Budurushi, Jurlind; Neumann, Stephan; Renaud, Karen; Volkamer, Melanie: Introduction to special issue on e-voting. *Journal of Information Security and Applications*, 38:122–123, 2018.

- [DC22a] Duenas-Cid, David: A theoretical framework for understanding trust and distrust in internet voting. In (Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Germann, Micha; Glondu, Stéphane; Hofer, Thomas; Krivososova, Iuliia; Martin-Rozumilowicz, Beata; Rønne, Peter; Zollinger, Marie-Laure, eds): Seventh International Joint Conference on Electronic Voting (E-Vote-ID) 2022. University of Tartu Press, Tartu, Estonia, pp. 57–62, 2022.
- [DC22b] Duenas-Cid, David: The sociotechnical construction of trust and distrust in electronic voting: The case of the Netherlands [Presentation], 25.05.2022.
- [dFM17] de Freitas, Jorge Lheureux; Macadar, Marie Anne: The Brazilian Electronic Voting System: evolution and challenges. In (Krimmer, Robert; Volkamer, Melanie; Braun-Binder, Nadja; Loeber, Leontine; Maurer, Ardita Driza; Pereira Olivier; Duenas-Cid, David; Roenne, Peter; Kersting, Norbert; Schürmann, Carsten; Kulyk, Oksana; Vinkel, Priit, eds): Second Joint International Conference on Electronic Voting (E-Vote-ID 2017). TUT Press, Tallinn, Estonia, pp. 59–71, 2017.
- [EDCV] Erb, Yannick; Duenas-Cid, David; Volkamer, Melanie: Appendix A. https://secuso.ai.fb.kit.edu/downloads/documents/EVoting_Trust_Paper_Appendix_A.pdf. Accessed: 2023-09-14.
- [En] Enterprise Estonia: e-Governance - e-Democracy & open data. <https://e-estonia.com/solutions/e-governance/e-democracy/>. Accessed: 2022-08-17.
- [ES21] Ehin, Piret; Solvak, Mihkel: Party Cues and Trust in Remote Internet Voting: Data from Estonia 2005–2019. In (Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Kulyk, Oksana; Rønne, Peter; Solvak, Mihkel; Germann, Micha, eds): Electronic Voting, Lecture Notes in Computer Science, pp. 75–90. Springer International Publishing, Cham, 2021.
- [FGR19] Fragnière, Emmanuel; Grèzes, Sandra; Ramseyer, Randolph: How do the Swiss Perceive Electronic Voting? Social Insights from an Exploratory Qualitative Research. In (Krimmer, Robert; Volkamer, Melanie; Cortier, Veronique; Beckert, Bernhard; Küsters, Ralf; Serdült, Uwe; Duenas-Cid, David, eds): Electronic Voting, Lecture Notes in Computer Science, pp. 100–115. Springer International Publishing, Cham, 2019.
- [GGB18] Goodman, Nicole; Gabel, Chelsea; Budd, Brian: Online Voting in Indigenous Communities: Lessons from Canada. In (Krimmer, Robert; Volkamer, Melanie; Cortier, Veronique; Goré, Rajeev; Hapsara, Manik; Serdült, Uwe; Duenas-Cid, David, eds): Electronic Voting, Lecture Notes in Computer Science, pp. 67–83. Springer International Publishing, Cham, 2018.
- [Gi91] Giddens, Anthony: The consequences of modernity. Polity Press, Cambridge, 1991.
- [Gi16] Gibson, J. Paul; Krimmer, Robert; Teague, Vanessa; Pomares, Julia: A Review of E-voting: The Past, Present and Future. *Annals of Telecommunications*, 71(7-8):279–286, 2016.
- [GMR96] Gates, Bill; Myhrvold, Nathan; Rinearson, Peter: The Road Ahead. Penguin Books, Harmondsworth, Middlesex, UK, 2 edition, 1996.
- [Hu17] Hurlburt, George: How much to Trust Artificial Intelligence? *IT Professional*, 19(4):7–11, 2017.

- [In] International Institute for Democratic and Electoral Assistance: ICTS in Elections Database. <https://www.idea.int/data-tools/data/icts-elections>. Accessed: 2022-08-17.
- [KDCK21] Krimmer, Robert; Duenas-Cid, David; Krivososova, Iuliia: Debate: Safeguarding Democracy During Pandemics. Social Distancing, Postal, or Internet Voting— the Good, the Bad or the Ugly? *Public Money & Management*, 41(1):8–10, 2021.
- [Li21] Licht, Nathan; Duenas-Cid, David; Krivososova, Iuliia; Krimmer, Robert: To i-vote or Not to i-vote: Drivers and Barriers to the Implementation of Internet Voting. In (Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Kulyk, Oksana; Rønne, Peter; Solvak, Mihkel; Germann, Micha, eds): *Electronic Voting, Lecture Notes in Computer Science*, pp. 91–105. Springer International Publishing, Cham, 2021.
- [LK17] Lindemane, Marija; Kuzmina, Jekaterina: Outstripping of the eVoting Evolution. In (Krimmer, Robert; Volkamer, Melanie; Braun-Binder, Nadja; Loeber, Leontine; Maurer, Ardita Driza; Pereira Olivier; Duenas-Cid, David; Roenne, Peter; Kersting, Norbert; Schürmann, Carsten; Kulyk, Oksana; Vinkel, Priit, eds): *Second Joint International Conference on Electronic Voting (E-Vote-ID 2017)*. TUT Press, Tallinn, Estonia, 2017.
- [Lu79] Luhmann, Niklas: *Trust and Power*. Wiley-Blackwell, Chichester, 1979.
- [Mc11] Mcknight, D. Harrison; Carter, Michelle; Thatcher, Jason Bennett; Clay, Paul F.: Trust in a Specific Technology. *ACM Transactions on Management Information Systems*, 2(2):1–25, 2011.
- [MDS95] Mayer, Roger C.; Davis, James H.; Schoorman, F. David: An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20(3):709, 1995.
- [Ox] Oxford Academic Dictionary: trust - noun. <https://www.oxfordlearnersdictionaries.com/definition/academic/trust1?q=trust>. Accessed: 2023-09-11.
- [Pa21] Page, Matthew J.; McKenzie, Joanne E.; Bossuyt, Patrick M.; Boutron, Isabelle; Hoffmann, Tammy C.; Mulrow, Cynthia D.; Shamseer, Larissa; Tetzlaff, Jennifer M.; Akl, Elie A.; Brennan, Sue E.; Chou, Roger; Glanville, Julie; Grimshaw, Jeremy M.; Hróbjartsson, Asbjørn; Lalu, Manoj M.; Li, Tianjing; Loder, Elizabeth W.; Mayo-Wilson, Evan; McDonald, Steve; McGuinness, Luke A.; Stewart, Lesley A.; Thomas, James; Tricco, Andrea C.; Welch, Vivian A.; Whiting, Penny; Moher, David: The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ (Clinical research ed.)*, 372:n71, 2021.
- [SC21] Swisher, Kara; Cook, Tim: Apple’s C.E.O. Is Making Very Different Choices From Mark Zuckerberg. <https://www.nytimes.com/2021/04/05/opinion/apples-ceo-is-making-very-different-choices-from-mark-zuckerberg.html?>, 05.04.2021. Accessed: 2022-08-18.
- [SK18] Serdült, Uwe; Kryssanov, Victor: Internet Voting User Rates and Trust in Switzerland. In (Krimmer, Robert; Volkamer, Melanie; Cortier, Véronique; Duenas-Cid, David; Goré, Rajeev; Hapsara, Manik; Koenig, Reto; Martin Steven; McDermott, Ronan; Roenne Peter; Serdült, Uwe; Truderung, Tomasz, eds): *Third International Joint Conference on Electronic Voting (E-Vote-ID 2018)*. TalTech Press, 2018.

- [SK19] Solvak, Mihkel; Krimmer, Robert: The Curse of Knowledge? Does Having More Technology Skills Lead to Less Trust Towards iVoting? In (Krimmer, Robert; Volkamer, Melanie; Beckert, Bernhard; Cortier, Véronique; Maurer, Ardita Driza; Duenas-Cid, David; Helbach Jörg; Koenig, Reto; Krivososova, Iuliia; Küsters, Ralf; Rønne, Peter; Serdült, Uwe; Spycher Oliver, eds): Fourth Joint International Conference on Electronic Voting (E-Vote-ID 2019). TalTech Press, Tallinn, Estonia, pp. 204–207, 2019.
- [So20] Solvak, Mihkel: Does Vote Verification Work: Usage and Impact of Confidence Building Technology in Internet Voting. In (Krimmer, Robert; Volkamer, Melanie; Beckert, Bernhard; Küsters, Ralf; Kulyk, Oksana; Duenas-Cid, David; Solvak, Mihkel, eds): Electronic Voting, Lecture Notes in Computer Science, pp. 213–228. Springer International Publishing, Cham, 2020.
- [SSP20] Sanger, David E.; Stevens, Matt; Perlroth, Nicole: Election Officials Directly Contradict Trump on Voting System Fraud. <https://www.nytimes.com/2020/11/12/us/politics/election-officials-contradict-trump.html>, 2020. Accessed: 2022-08-17.
- [Sz03] Sztompka, Piotr: Trust: A sociological theory. Cambridge University Press, Cambridge, 2003.
- [Tr16] Trechsel, Alexander H.; Kucherenko, Vasyl; Silva, Frederico; Gasser, Urs: Potential and Challenges of E-Voting in the European Union. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/556948/IPOL_STU%282016%29556948_EN.pdf, 2016. Accessed: 2022-09-06.
- [UL20] Ulmer, Alexandra; Layne, Nathan: Trump Allies Breach U.S. Voting Systems in Search of 2020 Fraud 'Evidence': A Reuters Special Report. <https://www.reuters.com/investigates/special-report/usa-election-breaches/>, 2020. Accessed: 2022-08-18.
- [Zo19] Zollinger, Marie-Laure; Distler, Verena; Rønne, Peter; Ryan, Peter Y. A.; Lallemand, Carine; Koenig, Vincent: User Experience Design for E-Voting: How Mental Models Align with Security Mechanisms. In (Krimmer, Robert; Volkamer, Melanie; Beckert, Bernhard; Cortier, Véronique; Maurer, Ardita Driza; Duenas-Cid, David; Helbach Jörg; Koenig, Reto; Krivososova, Iuliia; Küsters, Ralf; Rønne, Peter; Serdült, Uwe; Spycher Oliver, eds): Fourth Joint International Conference on Electronic Voting (E-Vote-ID 2019). TalTech Press, Tallinn, Estonia, pp. 187–202, 2019.
- [Zo21] Zollinger, Marie-Laure; Estaji, Ehsan; Ryan, Peter Y. A.; Marky, Karola: “Just for the Sake of Transparency”: Exploring Voter Mental Models of Verifiability. In (Krimmer, Robert; Volkamer, Melanie; Duenas-Cid, David; Kulyk, Oksana; Rønne, Peter; Solvak, Mihkel; Germann, Micha, eds): Electronic Voting, Lecture Notes in Computer Science, pp. 155–170. Springer International Publishing, Cham, 2021.