Government Information Quarterly 42 (2025) 102068

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

State versus Technology: What drives trust in and usage of internet voting, institutional or technological trust?

Bogdan Romanov [a,*], David Duenas Cid [b], Peeter Leets [a]

[a] *Tartu University, Lossi 36, 51003, Estonia*
[b] *Kozminski University, Poland*

ARTICLE INFO

Keywords:
Trust
Internet voting
Political trust
Technological trust
Democracy
Estonia
Institutional trust

ABSTRACT

This study examines the combined influence of technological and institutional trust on citizens' perceptions of and engagement with Internet voting, addressing gaps in the literature on digital governance and trust. While prior research often treats these trust dimensions separately, this article explores their interplay within the context of Estonia, which has utilized Internet voting for two decades. By constructing composite indices for technological and institutional trust through factor analysis, the study offers a novel methodological approach to operationalizing trust in digital governance (within the article, digital governance and e-governance are used interchangeably) research in general and Internet voting in particular, based on post-electoral survey data.

Applying linear and logistic regression analyses, the study explicitly examines how these trust dimensions affect citizens' trust in Internet voting systems and their actual use of such technology. The findings reveal that institutional trust is significantly more influential than technological trust, consistently emerging as the primary driver for both trusting Internet voting and engaging in its usage. Technological trust, in contrast, demonstrates only marginal predictive strength, highlighting the greater importance citizens place on institutional legitimacy, transparency, and accountability. These results emphasize the compensatory nature of institutional trust, suggesting that robust institutional frameworks allow citizens to confidently engage with complex technological systems despite limited technical understanding. Consequently, this research enhances theoretical insights into trust dynamics within digital governance, particularly in contexts where political sensitivity and institutional credibility significantly impact technology adoption.

1. Introduction

In modern democracies, trust serves as the foundation for the legitimacy and stability of governance systems. The progressive increase in the complexity of modern societies made it necessary to expand the theoretical comprehension of trust mechanisms (Giddens, 1991; Sztompka, 1999), adopt new perspectives on the functioning of trust, including, unavoidably, technology as an important sociotechnical factor for understanding it (Beck, 1992) and with a growing influence in current digital societies (Duenas-Cid & Calzati, 2023). The relevance of trust becomes even more critical when technologies are adopted for democratic processes (Kneuer, 2016), particularly in highly digitalized societies like Estonia (Toots, 2019). In such contexts, ensuring trust in both technology and institutions is a central concern for policymakers and governance agendas (Wolf et al., 2011). This reliance on different forms of trust underscores the growing interdependence between technology and institutional governance in sustaining democratic engagement (e.g., Internet voting, participatory budgeting, Internet forums) and in the overall development of digital governance (Abdulkareem et al., 2022; Demirdoven et al., 2020; Horsburgh et al., 2011; Parent et al., 2005; Santa et al., 2019).

Conventionally, trust is defined as the willingness to become vulnerable to another party whose actions they cannot fully observe or control, based on the belief that this party will act reliably and in their best interest (Koller, 1988; Mayer et al., 1995). Zand (1972) highlighted that trust is demonstrated when individuals accept such vulnerability. The significance of trust for the understanding of humanness is complex and affects many different aspects of individual and social life. In particular, the research is interested in the interactive nature of trust when it relates to others (either individuals or institutions). Guided by the topic of study, the focus is on two specific forms of trust that closely interact with it (Abdala et al., 2025): trust in technology (technological

* Corresponding author at: Tartu University, Lossi 36-304, 51003 Tartu, Estonia.
E-mail addresses: bogdan.romanov@ut.ee (B. Romanov), dduenas@kozminski.edu.pl (D.D. Cid), peeter.leets@ut.ee (P. Leets).

https://doi.org/10.1016/j.giq.2025.102068
Received 8 May 2025; Received in revised form 10 July 2025; Accepted 29 August 2025
Available online 5 September 2025

trust) (Wang et al., 2023) and trust in political institutions (institutional trust) (D. H. McKnight et al., 2002), whose definitions will be further provided.

While dealing with trust plays an important role in the development of digital governance in general, this is arguably more important when related to the integration of technology into democracy. Technology allows for increased efficiency and accessibility but, while doing so, introduces new vulnerabilities (Dueñas-Cid, 2024) in a context that is already challenging due to the political relevance of power delegation (Norris & Nai, 2017). When technology is in place, citizens are required to place a "leap of faith" not only in the institutions administering elections but also in the technology enabling them (Beldad et al., 2012). The main issue underlying trust in technology stems from the relatively high threshold for the comprehension of the technology in question. For instance, Internet voting involves the concepts of data privacy, cryptography, and server maintenance, whose nuances are sophisticated and might not be clear to the citizens (Erb et al., 2023). Understanding how institutional and technological trust interact is crucial to explaining the uptake and credibility of the Internet voting system or similar technologies.

In other words, unlike conventional paper-based voting, where procedural transparency is observable and comprehensive (e.g., physical ballot boxes, on-site observers), Internet voting demands that citizens place faith in invisible processes: cryptographic systems, server security, digital authentication, and software integrity. As such, trust becomes the central currency through which the legitimacy of digital elections is maintained. Crucially, this trust must operate on two levels: (1) in the technology itself, and (2) in the institutions that design, oversee, and safeguard the voting process. In Estonia's context, where technological infrastructures are highly developed and routinely used, this study seeks to determine which type of trust, technological or institutional, ultimately drives trust in and usage of Internet voting.

Despite trust's importance, it remains an underexplored factor in studies on digital governance. A significant portion of existing research focuses on either technological aspects, such as usability and security, or institutional factors, such as policy frameworks and governance (Alvarez et al., 2021; Carter & Campbell, 2011; Luo et al., 2024; Zhu et al., 2021). Meanwhile, few studies examine the intricate relationship between trust in technology and trust in institutions or their combined influence on the actual usage of innovations like Internet voting (Abdala et al., 2025). Addressing this gap is essential to ensure that digital tools uphold the principles of transparency, accountability, and inclusivity that underpin democratic governance.

For these reasons, the present study explores the interplay between technological and institutional trust in the context of Internet voting, focusing on Estonia, home of an advanced digital governance ecosystem with experience in the use of Internet voting since 2005 (Vassil et al., 2016). The research question was formulated as follows: Which type of trust, institutional or technological, incentivizes people to trust and actually use Internet voting? By answering this research question, the paper will contribute to the broader discussion on how trust is sustained in digital democracy and the functioning of acceptance mechanisms. Additionally, the research explores trust in Internet voting and actual usage of the technology instead of the intention to use.

Besides its contribution to the academic discussion, this study has important practical implications for electoral management bodies and governmental institutions. Understanding whether usage of and trust in Internet voting relies more on institutional or technological trust will help these bodies strategically prioritize their agenda in aspects such as communication or transparency. While Internet voting is often analyzed within the domain of electoral studies, its institutionalization in Estonia reflects a broader agenda of digital public governance. As a flagship e-government service, Internet voting is not merely a voting method, but a policy instrument embedded in state efforts to digitize public administration, enhance civic engagement, and streamline service delivery.

The structure of the article is as follows: The conceptual framework section is devoted to the presentation of the literature-based associations between technological/institutional trusts and the usage of Internet voting technology. Additionally, the section will emphasize the literature gap and present the hypotheses tested in this article. The third section, titled Methodology, will address the topics of case selection, survey data collection, and preparation. The purpose of the Analysis part is twofold: the first half is devoted to the institutional and technological trust indices composition with the help of Exploratory and Confirmatory Factor Analyses, while the second half of the Analysis will test the hypotheses by including the composed factors into the linear and logistic regression models. The fifth section is dedicated to the Discussion of the results and their correspondence with the previous and ongoing academic discussions. The last part of the article, the Conclusion, will summarize the work done, list the limitations of the presented research, and highlight the prospects for further research.

2. Conceptual framework

2.1. State of the art

Trust is, at the same time, a property connected with an individual belief or perception (Mooradian et al., 2006; Murnighan et al., 2004), and a relational concept that projects this individual belief on an external actor and that stems from the interaction between them (Cook et al., 2005). In consequence, different forms of trust can be posited depending on the type of actor included in the equation, including interpersonal trust (when refers to trust between individuals), group trust (when involves trust between various groups of individuals), institutional (when related to interaction between individuals and institutions), organizational trust (when trust occurs between different organizations) or technological trust (when related to the interaction between individuals and technology) (Hardin, 2002; Simon, 2020). This interactive nature of trust allowed for describing it a necessary element lying behind human cooperation (Simmel, 2011), social (Putnam, 2001) or economic relations (Fukuyama, 1995); and it does so by serving as a mechanism to reduce the complexity of human interaction (by relying in trusted actors) and the uncertainty that interaction entails (by identifying specific risks that are easier to confront than uncertain scenarios) (Luhmann, 1979). The complexity of trust when related to the use of technology (Bodó, 2021) has been approached in several ways, focusing in the nature of trusting behaviors as underlying disposition driving action (Evans & Krueger, 2009), the communitarian influence on perceiving political efficacy and further trusting (Anderson, 2010), on the legal foundations of trust in new technologies and its uses (Werbach, 2018); or on the reaction to the humanness of human-computer interaction (Ciechanowski et al., 2019; Lankton et al., 2015). Still, many approaches to the topic adopt a rather simplistic definition of trust, in which trust is reduced to a binary dichotomy whose antecedents are often a small number of variables. This makes trust become a sort of joker construct that can be used both at the foundation of a process of technology adoption (Janssen et al., 2018) or as a logical outcome of a given process (Lippert & Davis, 2006), stemming from the very complexity of trust as a social construct and the difficulty in ascertaining how it is distributed (Duenas-Cid & Calzati, 2023). This paper aims to shed light on this issue by approaching the use of Internet voting, being conscious that this particular technology is not directly comparable to many other e-governance technologies, but also being aware that it serves as a critical political technology with very specific features from where to extract crucial learnings that can pave the way for other types of technology.

This study acknowledges the relevance of interpersonal and group trust in closely related fields, such as in relation to the usage of digital governance tools or the development of political behaviors (Himelboim & Sweetser, 2012; Latusek et al., 2025). Other research also highlighted the influence of personality (Sindermann et al., 2023) and politics (Ehin & Solvak, 2021) in building trust on Internet voting, the impact of trust

in the Internet or in other technologies (Carter & Campbell, 2011), the importance of closeness to the electoral management (Warkentin et al., 2018), the compulsiveness of electoral participation (Zada et al., 2016), or the perceived convenience (Carter & Campbell, 2012) as factors guiding the adoption of Internet voting. However, two elements have traditionally been at the cornerstone of trust research and Internet voting: political institutions (Carter & Campbell, 2011; Kozel & Dečman, 2022; Warkentin & Rose, 2002; Welch et al., 2005) and technology-related (Acemyan et al., 2022; Volkamer et al., 2011) issues.

Technological trust dependency can be explained by the complex technological nature of Internet voting and the high-security requirements for its implementation in an intensely politically charged environment, such as systems of delegation of power or other forms of decision-making (Kulyk et al., 2022). Institutional trust dependency is driven by four main elements (Dueñas-Cid, 2024) that put pressure on Institutions when delivering technology in elections: the political significance of elections, the need to deliver an optimal technological display in a very defined and short period of time not prone to delays, the structural complexity of electoral management and challenges that technology poses for its integration in elections. It does not come as a surprise, hence, that the topic attracted both researchers in political sciences and public administration, generally inclined towards giving relevance to institutional forms of trust (Carter & Belange, 2005), but also scholars coming from technical fields (security, cryptography, etc.) for whom the topic relates more to the creation of secure environments and, as a result, to the capacity to project trust on technology (Carter & Belange, 2005). This diversity of approaches is also visible in the implementation recommendations proposed by international institutions, where measures to create institutional or technological trust are presented together (Rodríguez-Pérez, 2022; Wolf et al., 2011). Research also proved that the borders between institutional and technological trust are blurred, and trust can transfer from one to the other (Schaupp & Carter, 2005), picturing them as interconnected dimensions of trust addressing distinct aspects of how citizens relate to it: trust in technology is rooted in the functionality and security of technology (H. McKnight et al., 2009) and trust in institutions is grounded in the legitimacy and integrity of the institutions (Simon, 2020) overseeing its implementation. The previous also means that technological failures might have an impact on institutional trust (Oostveen, 2010), while breaches in trust in institutions might also impact the trust citizens have in technologies (Babayan et al., 2021), and vice versa, justifying the complexity of making the decision to adopt voting technologies by the potential backlash on institutions if not properly adopted (Mahrer & Krimmer, 2005).

By defining these constructs and exploring their theoretical underpinnings, this section establishes the foundation for analyzing their roles in fostering trust and usage of Internet voting. In order to achieve that point, and assuming that the expressed specificities of Internet voting invite a more nuanced approach to the topic of trust, the study proposes a tailored conceptual definition of technological and institutional trust.

In this context, **technological trust** refers to citizens' trust in the reliability, security, and efficiency of Internet voting (Volkamer et al., 2011). This form of trust is often cultivated through consistent, positive interactions with dependable digital platforms and digital governance services, including Internet voting (Gefen et al., 2003, 2005; D. H. McKnight & Chervany, 2001; Pavlou, 2003). It emphasizes operational competence, particularly whether the technology functions as intended, protects user data, and ensures system security (Carter & Belange, 2005). Reliability, security, and privacy are crucial for all technologies, but especially for digital political technologies, such as Internet voting, because citizens' Internet votes might determine the outcome of the elections (Erb et al., 2023; Volkamer et al., 2011).

In contrast, **institutional trust** reflects citizens' trust in the integrity, competence, and fairness of the political managers (Sztompka, 1999) and entities responsible for managing Internet voting technology, such as governments, regulatory bodies, or electoral commissions (Easton, 1975, p. 19; Mishler & Rose, 2001). Institutional trust is rooted in broader factors, including perceptions of transparency, accountability, and adherence to democratic norms (Levi & Stoker, 2000). It encompasses not only the ethical management of Internet voting systems but also the institutions' ability to uphold fairness and legitimacy in policymaking and implementation (Tyler & Huo, 2002), or their capacity to react to problems regarding Internet voting use (Dueñas-Cid, 2024).

Shifting the focus to the associations between trust and technology usage, technological trust was reported to play a pivotal role in influencing citizens' usage of Internet voting systems. Positive experiences with other secure digital platforms, such as online banking and shopping, significantly enhance citizens' trust in similar technologies (Rogers, 2003; Venkatesh et al., 2003; Zhang & Zhou, 2020; Zhou, 2011, p. 2). This is particularly crucial in Internet voting, where users must trust the system to process their votes accurately, securely, and anonymously while exploring the technology less frequently than once a year (M. Alomari et al., 2012).

Research shows that technological trust helps mitigate perceived risks and uncertainties, increasing citizens' willingness to engage with Internet voting platforms (Carter & Belange, 2005; D. H. McKnight & Chervany, 2001). However, barriers to adoption and usage persist when citizens doubt the system's ability to address challenges such as cybersecurity threats, data breaches, or technical failures (Lee & See, 2004; Shin, 2010). Trust in technology's robustness and design also plays a significant role in alleviating concerns about system vulnerabilities and ensuring operational integrity (Lin, 2011).

On the other hand, trust in institutions, such as electoral commissions and government agencies, influences perceptions of procedural fairness, transparency, and accountability (Beldad et al., 2012; Perez & Ross, 2020). When citizens perceive these institutions as trustworthy, they are more likely to believe that Internet voting systems are ethically managed and competently deployed (S. G. Grimmelikhuijsen & Meijer, 2014; Mishler & Rose, 2001), putting institutional trust as an important precondition for considering the usage of technology (Schaupp & Carter, 2005).

2.2. Research gap

Despite extensive research on trust in technology and institutional trust as individual constructs, limited studies have examined their combined impact on the usage of Internet voting systems (Abdala et al., 2025; Bélanger & Carter, 2008; Perez & Ross, 2020). Existing literature predominantly approaches the usage of Internet voting via the Technology Acceptance Model (TAM) or the Unified Theory of Acceptance and Use of Technology (UTAUT), which limits the pool of variables to the technology-related factors (Abu-Shanab, 2014; M. K. Alomari, 2016; Warkentin et al., 2018). On the other hand, some articles focus exclusively on the role of institutional trust in digital governance manifestations (Lu et al., 2019; Mensah, 2020; Sharma, 2020).

While the study acknowledges that these two elements (i.e., institutional and technological trust) are not sufficient to dissect sophisticated Internet voting usage to its core, their uneven impact in the response to this question is a significant contribution, because the interplay between technological and institutional trust remains underexplored. While the assumption that technological and institutional trust work in parallel is quite accepted in the academic community (Abdala et al., 2025; Bodó, 2021; Wong et al., 2023), how both forms of trust are weighted and how they impact the adoption and usage of technology still has several open questions. For instance, how does institutional trust mediate the relationship between technological trust and citizens' actual usage of Internet voting? Or, is the perceived risk of a certain technology making citizens rely more on institutional trust? Addressing these questions can illuminate critical factors shaping the adoption of Internet voting systems and highlight areas for further research. Such inquiries are crucial for understanding how to build

comprehensive trust in innovative digital platforms (S. G. Grimmelikhuijsen & Meijer, 2014; Tolbert & Mossberger, 2006).

The research by Abdala et al. (2025) is the closest to the present, comparing both types of trust within the same case of Estonia and with a similar timeframe covered. While the definition of institutional trust that the authors propose is very aligned with the one presented in the current text, in contrast, the definition of technological trust focuses more on aspects related to security and experience with similar technologies, while theirs is on the efficiency of the performance of Internet voting. Besides the difference in the terminology and conceptualization, the difference is observed in the operationalization of the core variables of institutional and technological trust, as well as the results – more on that in the discussion part. However, the coincidence in time of both types of research can be a good occasion to discuss results and engage in an academic discussion on the reasons potentially driving different results.

Hence, the current article fills in the gap by examining the combined impact of technological and institutional trust on the trust in and usage of Internet voting, since, in general, a limited number of studies address the role of trust in the intention to use government-initiated technologies, such as Internet voting (Wang et al., 2023). Studying these two types of trust in the technology in question extends beyond mere electoral behavior — it captures public confidence in how governments govern through technology.

Additionally, this interplay will be tested in the case of democracy with a high degree of digital governance diffusion, hence constituting an ideal context to assess if exposure to technology daily (i.e., online banking, digital prescriptions, etc.) and trust in it convert into technological trust in Internet voting. The final methodological contribution of this study lies in constructing composite indices for technological and institutional trust. These indices, developed through rigorous exploratory and confirmatory factor analyses, provide a robust and multidimensional representation of the underlying trust constructs. By employing a weighted method to aggregate trust components, the article offers a novel approach to operationalizing trust, which can serve as a template for future research in e-governance.

In other words, the research is based on the previous studies on Estonian digital governance and Internet voting (Ehin et al., 2022, p. 201; Ehin & Solvak, 2021; Vassil et al., 2016), which laid out the context that was converted into the control variables. The research design engages in discussion with the work by Warkentin et al. (2018), who scrutinized the trust in Internet voting via the TAM framework and interpersonal trust lens in America by bringing more complex measurements for the trust in technology and trust in the political institutions into the case of a democracy with a population exposed to the e-governance to a high extent.

Besides the contribution to the academic discussion, the results of this research will enlarge the existing knowledge on the practical usage of Internet voting in relation to trust. Although the case of Estonia is very specific and might not find an easy extrapolation in other contexts where Internet voting has not yet been implemented, the results stemming from the analysis of the Estonian reality will help to foresee how trust works in a mature digital democracy and can help to build realistic expectations in other administrations willing to implement such technology. The dynamics of trust once Internet voting is consolidated should be logically different than those occurring at the early stages of technology implementation.

2.3. Hypotheses

Building on the conceptual framework, this section identifies key areas where the literature remains underexplored and formulates testable hypotheses to address the abovementioned gaps. These hypotheses are grounded in the theoretical foundations outlined in sections 2.1 and 2.2 and aim to shed light on the distinct and combined roles of technological and institutional trust in the context of Internet voting.

H1. Higher levels of technological trust are positively associated with citizens' trust in the Internet voting system and its usage.

This hypothesis is grounded in the **specific trust transfer theory (Gefen et al., 2003, 2005)**, which states that repeated positive experiences with familiar technologies (e.g., online banking, e-commerce, digital identity systems) create expectations that other digital services, such as Internet voting, will perform reliably. Technological trust may spill over from daily-use services to more politically consequential ones in highly digitalized societies like Estonia, where digital government services are pervasive. Prior research confirms that such transfer effects increase perceived usability and reduce perceived risk in digital interactions (D. H. McKnight & Chervany, 2001; Venkatesh et al., 2003; Wang et al., 2023). Internet voting, while more complex and politically sensitive, shares many of the same infrastructures and user interactions as routine e-services (e.g., ID-based authentication), thus positioning it within this broader spectrum of technological trust.

H2. Higher levels of institutional trust are positively associated with citizens' trust in the Internet voting system and its usage.

While technological functionality is essential, trust in the institutions managing digital systems is often a more decisive factor in determining public acceptance of e-government tools (Bélanger & Carter, 2008; Tolbert & Mossberger, 2006). This form of trust is particularly salient in the context of Internet voting, where citizens must rely not only on code but on governance, on the assumption that state actors will not misuse the system and that safeguards are in place to protect democratic integrity. Empirical studies show that institutional trust can serve a compensatory function: even when technical knowledge is limited or technological trust is weak, confidence in state institutions can sustain public support for complex technologies (S. Grimmelikhuijsen et al., 2017; Homburg et al., 2022; Mishler & Rose, 2001).

H3. Institutional trust has a stronger positive association with the trust and usage of the Internet voting system compared to technological trust.

This hypothesis posits that institutional trust has a stronger impact on Internet voting usage than technological trust. According to Gefen et al. (2003), institutional trust encompasses broader concerns about accountability and legitimacy, while technological trust focuses on operational efficiency and security. Given that citizens prioritize institutional legitimacy when interacting with government services (Tolbert & Mossberger, 2006), institutional trust is expected to have a more significant influence on the usage of Internet voting systems (Hamacher et al., 2016; Ribeiro et al., 2016).

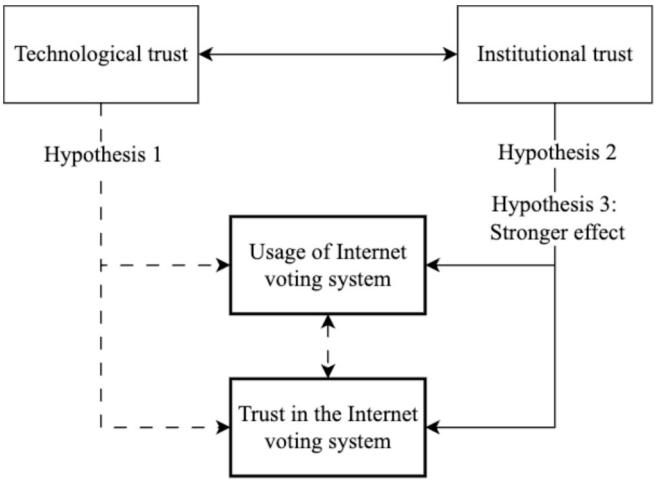

Fig. 1. Conceptual model of the hypothesized relationships between institutional and technological trust, trust in Internet voting, and the usage of Internet voting.

Fig. 1 depicts all core variables, technological and institutional trusts as "independent" variables, and usage of the Internet voting system and trust in the Internet voting system as two correlated dependent variables (for the correlation results, see Appendix C).

3. Research design

3.1. Case selection

Within the frame of data source definition, the necessary nuance requiring clarification is the answer to the question: Why is Estonia selected as the case for the analysis?

In general, Estonia serves as a critical case for the analysis of trust dynamics in the usage of Internet voting due to its status as a global pioneer in digital governance. Estonia, with its population of 1,330,068 (2021) and 1,365,732 people (2023) (*Population Figure | Statistikaamet*, 2025)[1], has been running Internet voting since 2005. Hence, Estonia became a benchmark for studying the integration of technology into democratic processes while providing a mature and well-documented context for exploring the interplay between technological and institutional trust (Ehin et al., 2022; Ehin & Solvak, 2021).

In terms of types of trust, Estonia's digital infrastructure is one of the most advanced globally, featuring e-governance platforms, digital identification systems, and robust cybersecurity frameworks (Espinosa & Pino, 2025; Kattel & Mergel, 2019). This emphasis on digital transformation was not merely a policy initiative but a state-building strategy following its independence from the Soviet Union in 1991. Facing limited resources, the government opted for digital-by-default reforms, resulting in early adoption of a national digital ID (2002), X-Road data exchange platform, Internet voting in 2005, and a range of other digital services (Espinosa & Pino, 2025; Kattel & Mergel, 2019). This technologically advanced environment offers an opportunity to assess the role of technological trust in an ecosystem where technological solutions are deeply embedded in citizens' everyday lives. Nevertheless, the sensitive nature of elections necessitates a parallel focus on institutional trust, as public trust in the entities managing the technology is critical for its legitimacy.

Additionally, Estonia's high levels of digital literacy (e.g., 62.6% of the Estonian population has at least basic digital skills in comparison to EU averages of 55.6% (*Estonia 2024 Digital Decade Country Report | Shaping Europe's Digital Future*, 2025)) and its population's frequent interaction with digital services further enhance the relevance of this case (Kralj, 2023). The high frequency of digital services usage and relatively higher share of ICT skills among the population are explained by the interoperability of services via the X-Road system, and the legal standing of digital signatures creates a governance ecosystem where digital interactions are standard practice, not exceptions. Citizens' familiarity with digital systems such as online banking, tax declarations, and health information services creates a fertile ground for understanding the transferability of trust from other technological domains to the context of Internet voting (Solvak et al., 2019). However, concerns surrounding cybersecurity risks, privacy breaches, and potential manipulation of the electoral process underscore the importance of institutional trust, particularly in the context of digital governance.

The final remark is about the hypothetical practical and theoretical contributions from treating Estonia as a critical case study in the context of institutional and technological trust. Estonia's long-term exposure to digital public services, robust cybersecurity infrastructure, and high baseline of digital literacy collectively create ideal conditions for technological trust in all technologies in general and Internet voting in particular. Paradoxically, if institutional trust is found to outweigh technological trust even in this context, it offers critical theoretical insight: namely, that institutional legitimacy remains the primary driver of public trust and technology adoption, regardless of digital sophistication and long-term exposure. This has powerful implications for other countries exploring Internet voting or broader digital governance reforms. First, it underscores that even well-engineered technologies cannot succeed without parallel investments in institutional transparency and accountability. Also, maybe trust in technology matters to the users during the early implementation stages, while as years pass, this effect might be diminishing. Second, it suggests that public trust in digital tools does not automatically emerge from technological familiarity or infrastructure alone; it must be anchored in the legitimacy of the institutions deploying them. Hence, Estonia's case provides both a cautionary and instructive example: while digital systems can become normalized, their democratic legitimacy hinges on citizens' trust in the political institutions behind them. For scholars, Estonia offers fertile ground for testing theories of trust spillover, digital habit formation, and institutional mediation. For practitioners, it highlights the need to pair technological deployment with robust public communication, procedural clarity, and long-term trust-building strategies, lessons applicable far beyond the Baltic region.

3.2. Data

In terms of the data collection, the University of Tartu, Estonia, regularly collects post-election individual-level survey data. Currently, data is available for eight elections from 2009 to 2023, with the last iteration taking place from March 12-19, 2023. These datasets were selected due to their comprehensive coverage of voter behaviors and attitudes regarding Internet voting and their temporal proximity, ensuring the relevance and representativeness of recent public opinions and behaviors in Estonia. A detailed description of the sampling, sample sizes, and interview modes of the surveys is presented in Appendix A.

The primary data for this study consists of responses from the two aforementioned post-election surveys. Each post-election survey used in this study comprises a nationally representative sample of approximately 1,000 respondents drawn from the Estonian voting-age population (approx. 1 million individuals (*Riigikogu Elections | Elections in Estonia*, 2025)). The surveys were conducted using stratified random sampling, ensuring proportional representation by key demographics such as age, gender, region, and language group. With a population of 1.37 million (as of 2025) and a voting-age population of around 1 million, a sample size of 1,000 yields a margin of error of approximately ±3 percentage points at a 95% confidence level. This makes the dataset robust for identifying statistically meaningful trends, especially in a small-population country with relatively low internal heterogeneity.

While the ideal research design would include all available data waves, the questions regarding the trust were reworded exclusively for the years 2021 and 2023. The variables collected in these surveys include both dependent and independent variables, as well as control variables.

The dependent variables include trust in Internet voting, measured on a scale from 0 ("Do not trust at all") to 10 ("Trust completely"), and Internet voting usage, a binary variable indicating whether respondents voted online (coded as 1) or used another voting mode (coded as 0).

The independent variables of institutional and technological trust

Table 1
Sets of independent variables and their hypothetical trust factor.

Technological trust	Institutional trust
Trust online banking	Trust government
Trust online purchases	Trust parliament
Trust declaring taxes online	Trust president
Trust submitting health information online	Trust courts
Trust applying for documents online	Trust elections (in general)
—	Trust e-state

[1] Population number at the beginning of 2025 is 1,369,995 (*Population Figure | Statistikaamet*, n.d.)

indices are based on the stand-alone ordinal indicators, similar to the trust in Internet voting variable from the survey, see Table 1 below.

Control variables used in the analysis include age, gender, education level, and computer literacy. Data transformations involved converting ordinal trust measures into binary categories for clearer interpretation in regression analysis, reversing scales for PC literacy to facilitate intuitive interpretation, and consistently managing missing data by replacing non-responses with NaN values. More information on the data transformation and descriptive statistics can be found in Appendix B.

4. Method

The methodological approach of this study involves two primary stages: constructing trust indices through factor analysis and evaluating hypotheses through regression analysis. Initially, Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) were conducted to develop reliable technological and institutional trust indices. EFA was employed to identify underlying patterns in survey responses, confirming the hypothesized two-factor structure representing technological and institutional trust dimensions. CFA subsequently validated these constructs, ensuring they adequately represented the theoretical concepts under examination.

Following the creation of these indices, linear and logistic regression models were utilized to empirically test hypotheses concerning relationships between trust dimensions and the dependent variables: trust in and actual usage of Internet voting. Linear regression analysis was conducted to examine the ordinal yet treated as continuous dependent variable, trust in Internet voting, whereas logistic regression was used to analyze the binary usage of Internet voting technology. Regression models were specifically chosen over alternative methods, such as qualitative analysis or purely descriptive statistics, due to their ability to quantify the strength and direction of relationships between variables and their robustness in controlling for potential confounding factors. The inherent complexity and nuanced nature of trust within technological and institutional frameworks necessitated methods to accurately distinguish and quantify their respective impacts.

5. Analysis

5.1. Confirmatory factor analysis

To streamline the presentation of the results, the technical steps of correlation analysis and Exploratory Factor Analysis are placed in Appendix C and Appendix D, respectively. The core takeaway based on the EFA's output and scree plot is that data has two distinct factors. After defining the number of factors, the next step is to confirm if the trust indicators are linked to the proposed factors. To examine the relationship between the observed variables and the two latent constructs, technological and institutional trust, a Confirmatory Factor Analysis is conducted. The CFA model aims to confirm whether the data supports the hypothesized associations between each variable and its respective factor. The analysis strongly aligns with the theoretical expectations, as demonstrated by the standardized loadings and significance levels, see Table 2.

These results indicate that all variables significantly load onto their respective factors, with p-values below 0.05, confirming that each observed variable is a meaningful indicator of its latent construct. For the model's fit assessment, see Appendix E.

Additionally, the covariance between the latent constructs of technological trust (TechTrust) and institutional trust (InstTrust) is estimated at 2.551 ($p < 0.01$), indicating a statistically significant and positive relationship. In standardized terms, this corresponds to a correlation coefficient of approximately 0.658, suggesting a moderate to strong association between the two dimensions of trust.

This result offers several important conceptual and empirical implications. First, it confirms that technological and institutional trust are empirically distinct yet interdependent constructs. The positive covariance suggests that individuals who express greater trust in technological systems (e.g., online banking, e-tax, digital ID services) are also more likely to express trust in institutional frameworks (e.g., government, courts, electoral bodies) responsible for overseeing or implementing these systems. Second, this interdependence aligns with theoretical perspectives in the trust literature. As suggested by Giddens (1990, 1991) and Luhmann (1979), trust in complex sociotechnical systems is rarely rooted in technical features alone; instead, it is often mediated by institutional assurances, norms of accountability, and perceived legitimacy. In the Estonian context, where digital infrastructure is deeply embedded in public administration and the state actively curates its image as a "digital state", trust in technology may, to a large extent, be contingent on the perceived integrity and competence of political institutions. Third, the strength of the covariance (as well as its significance) justifies the decision to model these two constructs separately rather than collapsing them into a single dimension. The CFA output indicates that each trust domain loads significantly onto its own factor, which supports the notion that citizens differentiate between trusting the technology itself and trusting the institutions deploying it, even if these two assessments are often positively aligned. Finally, the covariance may also be interpreted as evidence of spillover effects: institutional trust can act as a substitute or compensatory mechanism when individuals lack a full understanding of the technical workings of complex systems such as Internet voting. Conversely, familiarity with or confidence in the functionality of e-government platforms may enhance generalized perceptions of state competence and fairness, reinforcing institutional trust in return.

Table 2
The output of the CFA analysis, '∼' is for regression relationships, '∼∼' is for covariances. All loading' coefficients are rounded to three decimals.

Variable	Operation	Factor	Loading
Trust online banking	∼	TechTrust	1.000
Trust online purchase	∼	TechTrust	0.862*** (0.038)
Trust declaring taxes online	∼	TechTrust	0.991*** (0.026)
Trust submitting health information	∼	TechTrust	1.172*** (0.033)
Trust applying to documents	∼	TechTrust	1.108*** (0.029)
Trust government	∼	InstTrust	1.000
Trust parliament	∼	InstTrust	0.840*** (0.019)
Trust president	∼	InstTrust	0.911*** (0.021)
Trust courts	∼	InstTrust	0.777*** (0.020)
Trust elections	∼	InstTrust	0.933*** (0.020)
Trust e-state	∼	InstTrust	0.873*** (0.020)
Institutional trust	∼∼	InstTrust	6.960*** (0.322)
Institutional trust	∼∼	TechTrust	2.551*** (0.138)

Standard errors in parentheses. * p<.1, ** p<.05, ***p<.01.

5.2. Composing the indices

The final stage in the first part of the analysis is to create the indices themselves once it has been established that the data has two factors corresponding to the technological and institutional trusts with underlying trust-related indicators. Regarding the composition methods, the study computed weighted composite scores, which apply factor loadings as weights to each variable. Factor loadings, obtained from CFA, represent how each variable aligns with its respective latent factor. Variables with higher loadings have a stronger association with the

factor, contributing more to the composite score.

5.3. Regression analysis results with non-aggregated trust indicators

With the technological and institutional trust indices established through factor analyses and constructed using the weighted method, the next step involves testing their explanatory power in explaining trust in and practical usage of online voting systems. By incorporating these indices into regression models, this study examines the extent to which technological and institutional trust influence the dependent variables and evaluates the relative strength of their effects. The following analysis employs linear and logistic regression approaches to comprehensively assess the extracted hypotheses. Since the regression models did not meet all necessary theoretical assumptions[2], robust standard errors are added to all models.

Charts under Figs. 2 and 3 illustrate the coefficient plot outputs for Models 1 and 2, respectively, which incorporate standalone indicators of technological and institutional trust to assess their relationship with the dependent variables: trust in and usage of Internet voting systems. These models provide an initial exploration of the distinct effects of individual trust components on citizens' trust and the usage of Internet voting technology. The detailed outputs are in Appendix G, Table G1.

The results highlight a significant difference between technological and institutional trust indicators in predicting trust in and usage of Internet voting systems. Among the technological trust variables, none, including trust in online banking, online purchases, or declaring taxes, exhibit a statistically significant relationship with either dependent variable. This suggests that trust in digital technologies does not necessarily translate into trust in or usage of Internet voting.

In contrast, institutional trust variables show consistent and significant effects. Trust in government and trust in elections emerge as the most influential predictors. Trust in government demonstrates a strong positive association with trust in Internet voting ($\beta = 0.282$, $p < 0.01$) and also has a weaker yet significant influence on Internet voting usage ($\beta = 0.111$, $p < 0.05$). Trust in elections, however, displays the largest coefficients across both models, signifying its critical role in shaping citizens' trust ($\beta = 0.692$, $p < 0.01$) and their likelihood to adopt the system ($\beta = 0.141$, $p < 0.01$). Other institutional trust variables, such as trust in the president and trust in the e-state, also contribute positively and significantly to both outcomes, albeit with smaller coefficients. Notably, trust in parliament exhibits a negative association with trust in Internet voting ($\beta = -0.145$, $p < 0.01$), which warrants further investigation to understand its underlying causes.

The control variables provide additional context. PC literacy significantly predicts both trust in and usage of Internet voting, reinforcing the importance of digital competence in fostering usage. Gender is negatively associated with trust in Internet voting, indicating lower levels of trust among female respondents, although it does not significantly affect usage. Age, on the other hand, shows no significant relationship with either dependent variable, suggesting that generational differences do not influence trust and use of Internet voting. The education effect is negative yet statistically insignificant in both models.

5.4. Regression analysis results with weighted indices

The second and final part of the analysis is captured in Fig. 4, which presents the regression results for Models 3 and 4, incorporating weighted composite indicators for technological and institutional trust. These indices account for the relative contributions of each trust variable based on their factor loadings from the confirmatory factor analysis. By applying weights to the composite measures, these models offer a nuanced perspective on the role of technological and institutional trust in predicting trust in and the usage of Internet voting systems. The detailed regression output can be found in Appendix G, Table G2.

The results indicate that institutional trust continues to exhibit a substantial and statistically significant effect across both models. In Model 3, institutional trust demonstrates a strong positive relationship with trust in Internet voting ($\beta = 1.264$, $p < 0.01$). Similarly, in Model 4, institutional trust significantly predicts the likelihood of using Internet voting ($\beta = 0.3307$, $p < 0.01$). These findings reinforce the critical role of institutional trust in shaping citizens' perceptions of and actual engagement with Internet voting systems.

On the other hand, the composite indicator of technological trust does not significantly affect either dependent variable. In Model 3, the coefficient for technological trust is negative and statistically insignificant ($\beta = -0.002$), suggesting no meaningful relationship with trust in Internet voting. In Model 4, the effect of technological trust on Internet voting usage remains negligible and statistically insignificant ($\beta = -0.032$). This lack of statistical significance underscores the limited influence of aggregated technological trust on citizens' trust in or usage of Internet voting, even when combined into a composite index.

The control variables reveal patterns consistent with the findings in Figs. 1 and 2. PC literacy remains a significant predictor of both trust in and usage of Internet voting, highlighting the importance of digital competence in fostering positive attitudes and behaviors – higher PC skills lead to higher trust and the usage of Internet voting. Gender continues to demonstrate a negative relationship with trust in Internet voting, though its effect on usage is not significant. Again, age does not show a significant association with either dependent variable. Similar to Models 1 and 2, education remains statistically insignificant for both models.

5.5. Evaluation of hypotheses

The findings of this study provide critical insights into the interplay between technological and institutional trust in shaping citizens' trust in and usage of online voting systems. Drawing on the case of Estonia, a global leader in digital governance and Internet voting implementation, the analysis highlights the centrality of institutional trust in fostering trust in and usage of Internet voting, while technological trust plays a more limited role. These results contribute to the broader discourse on trust in digital governance by emphasizing the nuanced dynamics of public trust in digital electoral systems (Bélanger & Carter, 2008; D. H. McKnight et al., 2002).

The study is guided by three hypotheses, which address the relationship between trust dimensions and Internet voting:

H1. Higher levels of technological trust are positively associated with trust in online voting systems.

The first hypothesis was falsified since independent indicators of technological trust operationalization, as well as the index for technological trust, were not statistically significant across all models. Yet additionally, its impact is relatively small and, hence, the variable does not present a significant predictive power for the trust in and actual usage of the technology in question. This suggests that while citizens may value technological functionality, their trust in online voting systems depends more heavily on other factors, particularly institutional trust.

H2. Higher levels of institutional trust are positively associated with trust in online voting systems.

The analysis fully supports the second hypothesis – institutional trust is consistently a significant predictor of trust in and the usage of online voting systems. Trust in government and electoral institutions, in particular, emerged as the strongest determinants of trust in Internet voting. Based on Models 3 and 4, the increase in institutional trust by one unit leads to a 1.26 increase in trust in Internet voting and an approximately 39,1% increase in odds of using the technology. This

[2] See Appendix F for diagnostic plots and assumption testing results for the linear and logistic models.

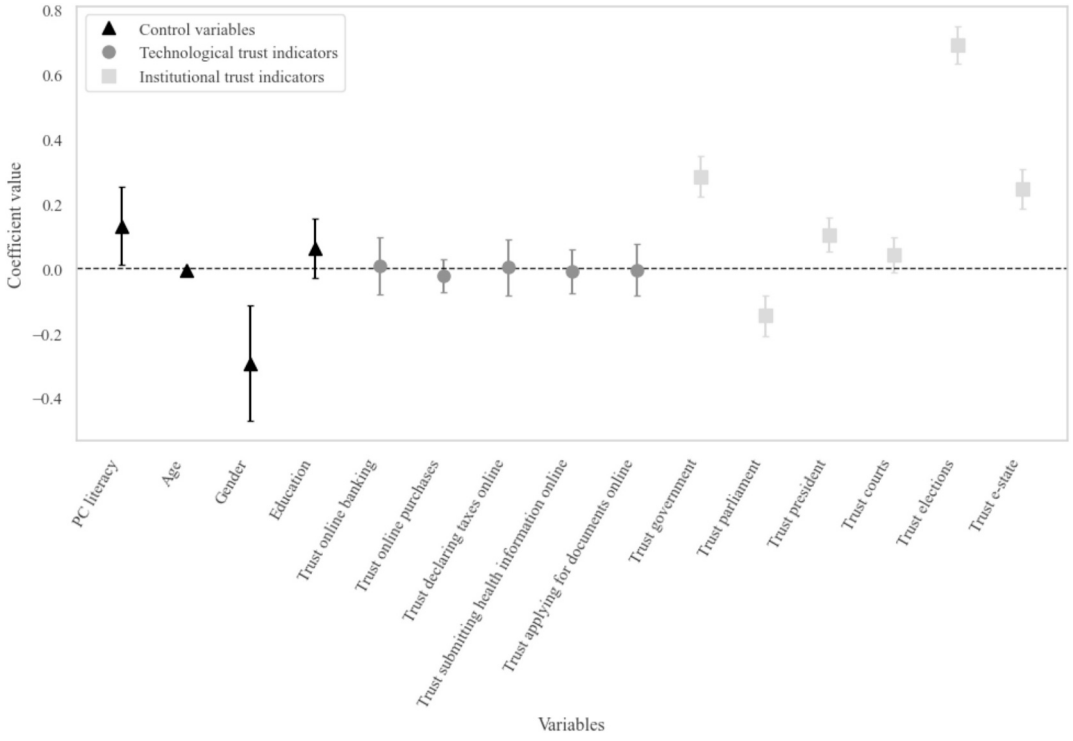

Fig. 2. Coefficient plots for Model 1, dependent variable: trust in Internet voting.

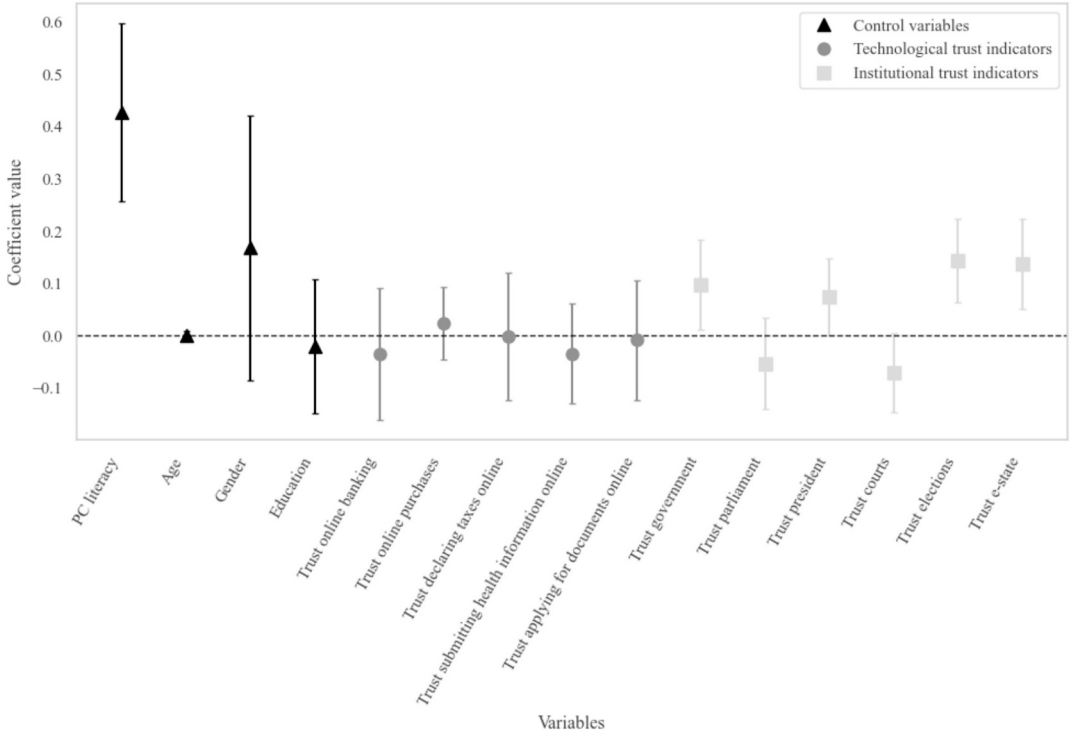

Fig. 3. Coefficient plots for Model 2, dependent variable: usage of Internet voting.

aligns with prior research emphasizing the role of institutional legitimacy and transparency in fostering public trust in digital governance.

H3. Institutional trust has a stronger positive association with the trust and usage of Internet voting system compared to technological trust.

The third assumption also finds support in the analysis; the regression analyses consistently demonstrate that institutional trust exerts a more significant influence on trust in and the usage of online voting. This aligns with previous studies emphasizing the importance of institutional legitimacy and transparency in shaping public attitudes toward digital governance (S. G. Grimmelikhuijsen & Meijer, 2014; Tolbert & Mossberger, 2006). Institutional trust provides citizens with

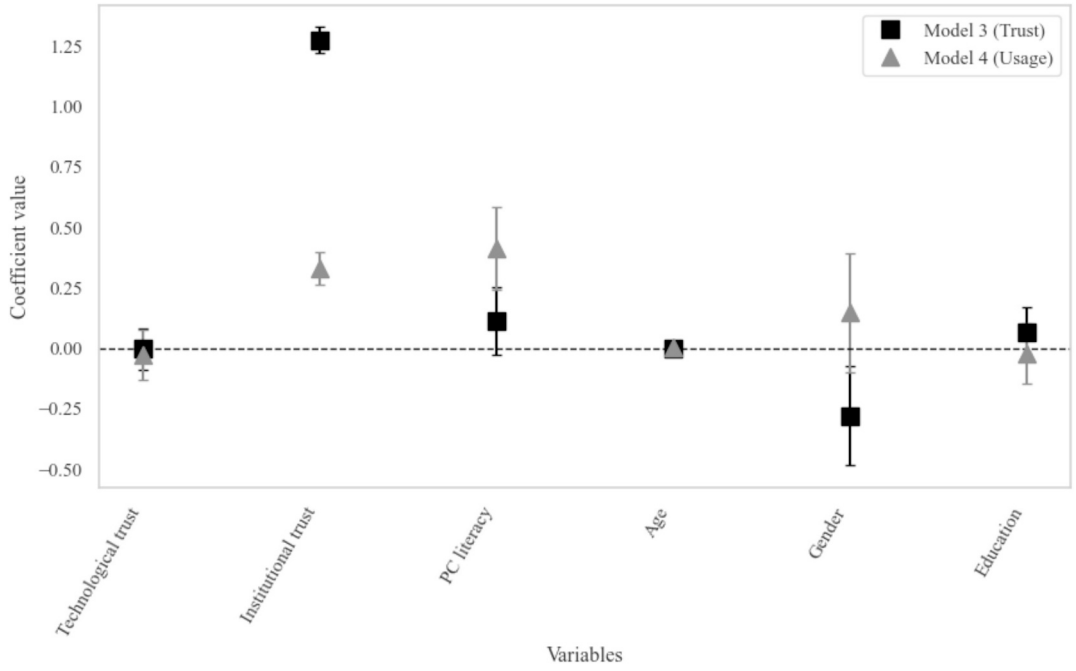

Fig. 4. Coefficient plot for models 3 and 4.

the assurance that electoral processes are fair and that any technological challenges will be addressed responsibly, thereby reinforcing the legitimacy of Internet voting. Also, these findings demonstrate the overriding importance of institutional legitimacy, as citizens rely on trust in the people and organizations managing the technology, especially in politically sensitive contexts like elections. The importance of institutional trust is vividly clear in the quantified effects of the associations, and the odds of using Internet voting increase by 39% (based on the Model 4 results) with the one-unit growth of trust in political institutions.

Conversely, technological trust demonstrates limited explanatory power; its effect on trust and usage remains statistically insignificant. This outcome reflects the specific role of technological trust in politically sensitive contexts, where citizens may perceive the stakes as too high to rely solely on the functionality of the technology. Instead, they appear to prioritize institutional trust, which addresses broader concerns of transparency, legitimacy, and accountability. This finding aligns with the concept that institutional trust acts as a foundational layer of trust, particularly in settings where the integrity of democratic processes is paramount. Thus, while technological trust contributes marginally to perceptions of online voting systems, the strength of institutional trust ultimately drives usage and public trust in the case of democracy with extended exposure to the particular technology.

6. Discussion

As was hinted in section 2.2 of the text, the findings allow the research to engage in discussion with the article by Abdala et al. (2025), where the colleagues reach different results – trust in technology being the one driving the usage of Internet voting, while institutional trust appears as the mediating variable. The authors bring the "multidimensional" notion of trust by introducing the distrust variable as well, which shall be encouraged since trust is always accompanied by distrust (Duenas-Cid & Calzati, 2023). However, the red thread within the current research is that trust is problematic to be captured by one question or variable. To solve this issue, this research approached both constructs using a multi-level composition of the variable in question. Trust, either in institutions or technology, is an agonistic construct that gathers different elements for its symbolic definition. The article posits that trust in government cannot be sufficient for the conceptualization and operationalization of "institutional trust", and trust in Internet voting is insufficient for "technological trust". For reference, see Fig. C1 in Appendix C with the correlation output: the 0.5 correlation between the trust in online voting and mode of voting (usage of Internet voting) already indicates that those are positively associated, and moreover, there is a strong correlation across the trust in online voting and sub-indicators of institutional trust (i.e., trust in government, parliament, elections, etc.).

Besides the previous point, the results are aligned with Abdala et al.'s idea that the unique context of Estonia likely plays a role in shaping trust-usage dynamics. As one of the most digitized societies globally, Estonia has normalized the use of secure digital platforms for daily activities, such as banking, tax declarations, and health services (Margetts et al., 2021); this was also illustrated by the absence of effect from age as a control variable. However, differently from them, the study demonstrates that a high degree of diffusion of digital systems may reduce the variability of technological trust, rendering it less influential in predicting online voting behavior and expanding the idea expressed by Solvak and Vassil (2018) that Internet voting creates habit: the generalized use of e-government technologies also generates habit and eases the usage of other technologies. However, the prominence of institutional trust underscores the critical role of perceived transparency and accountability in mitigating concerns about cybersecurity, privacy, and the misuse of technology. These findings might be applicable to Switzerland, that have re-introduced Internet voting trials in selected cantons – while work by Mendez and Serdült (2017) showed the effects of age and gender on trust, which was also typical for Estonia, these variables will lose their impact in the long-term and the "faithfulness" will be dependent on other trustors, such as political institutions.

Summarizing implications for the academic research and the engagement with the work by Abdala and colleagues, the findings underscore the importance of institutional trust as a central explanatory variable in technology adoption models in democratic digital governance. While many frameworks, such as TAM or UTAUT, emphasize technological features, the results suggest that public trust in the legitimacy, transparency, and accountability of managing institutions may be equally or more critical. This calls for a broader theoretical integration of institutional trust into future studies on digital government acceptance. Moreover, the use of multidimensional trust indices

validated through factor analysis demonstrates a valuable methodological advancement. The core recommendation for future research would be to move beyond single-item trust measures and employ similar composite approaches to enhance construct validity.

Despite the academic contribution to the discussion, the findings hold significant practical implications for election management bodies, electoral authorities, and policymakers involved in implementing and maintaining Internet voting systems. Given the decisive role of institutional trust, authorities should prioritize transparency, accountability, and procedural fairness to foster public trust (Ripamonti, 2024). Electoral institutions might benefit from active public engagement campaigns that transparently communicate system functionality, audit results, and responses to concerns. Additionally, efforts to enhance technological literacy among citizens should be complemented with sustained institutional credibility-building activities, as technological trust alone is insufficient to guarantee public acceptance of e-governance tools. These impacts extend to the overall e-governance research by shedding light on patterns of trust cross-fertilization between different technologies and how different forms of trust influence their usage.

7. Conclusion

This study addresses the research gap in the literature by examining the combined influence of technological and institutional trust on digital governance, specifically focusing on Internet voting in a democratic context. Through engaging with the current literature and formulating hypotheses, the research articulates the causal pathways linking trust dimensions to citizens' perceptions and behaviors regarding online voting. The study contributes methodologically by proposing a novel approach to the operationalization of technological and institutional trust through the creation of composite indices, which aggregate trust-related indicators via factor analysis. These indices were subsequently integrated into regression models to evaluate their relationships with trust in and usage of Internet voting.

The findings highlight the overriding role of institutional trust in shaping citizens' engagement with Internet voting systems. Institutional trust emerges as the stronger predictor of both trust in and usage of Internet voting, underscoring the importance of transparency, accountability, and trust in the institutions managing these systems. By contrast, technological trust demonstrates limited predictive power, suggesting that while citizens may value the functionality and reliability of digital systems, their ultimate trust hinges on the perceived integrity of the institutions overseeing the process. This distinction is particularly salient in politically sensitive contexts such as elections, where institutional trust can compensate for citizens' limited understanding of complex technologies.

7.1. Limitations

Despite its contributions, the study has several limitations that warrant consideration. First, the reliance on self-reported survey data may introduce biases such as social desirability effects, recall error, or respondent overconfidence in their own digital competence. Future research could complement this approach with experimental designs or behavioral data (e.g., digital trace or log-in data) to triangulate findings and validate reported behaviors.

Secondly, the issue of case specificity. Estonia, while analytically curious, represents a highly particular context: a small, digitally advanced, and politically stable country with nearly two decades of Internet voting experience and digital governance practices. Its high levels of digital literacy, trust in government, and habitual use of digital services place it at the frontier of global digital governance. As such, generalizing the findings to other countries (particularly those with less institutional trust, digital penetration, or democratic consolidation) should be done with caution.

Thirdly, although the study intentionally narrows the pool of trust in and usage of Internet voting determinants to two dimensions of trust, technological and institutional, additional variables, either trust-related or other indicators, may offer complementary insights. Incorporating distrust or skepticism explicitly could also provide a more nuanced understanding, as recent work has shown that trust and distrust do not necessarily form a single continuum but may coexist and interact.

Fourth limitation concerns potential endogeneity in the relationship between trust dimensions and Internet voting attitudes or behavior. While the study treats trust as an explanatory factor, it is plausible that trust is influenced by prior experiences with Internet voting or by unobserved variables such as political interest, ideology, or nationality. Future research could address this issue through instrumental variable approaches, panel data designs, or sensitivity analysis to better isolate causal pathways and account for reverse causality or simultaneity.

Finally, the study relies exclusively on quantitative data and quantitative methodology, derived from post-election surveys. While these provide valuable breadth, they necessarily trade off depth. The survey captures what people think about Internet voting, but not why they hold these views. In particular, the quantitative format cannot uncover the underlying motives, justifications, emotional undercurrents, or perceived risks that shape trust or distrust in Internet voting. Nor does it fully capture contextual variation, for example, how different social groups (e.g., based on nationality or age) experience or interpret institutional or technological performance. These limitations constrain the study's ability to explain the complex narrative dimensions of trust.

7.2. Further research

Building on the insights from this study, several promising avenues for future research emerge. Comparative studies across different political systems, particularly contrasting consolidated democracies with emerging digital democracies, could help test the generalizability of the findings and uncover context-specific trust dynamics. The next iteration of studies should investigate whether similar trust dynamics hold in less digitally mature or institutionally different environments, particularly where digital trust has not yet consolidated.

Additionally, future research should explore how institutional trust interacts with other psychological or social factors, such as political efficacy, civic engagement, or media exposure, in shaping trust in Internet voting. Another fruitful direction involves unpacking the mediating or moderating role of technological experience and digital literacy. Longitudinal and experimental designs can help identify not just correlations but causality and change over time.

Finally, future work should consider incorporating the perspectives of non-users and skeptics of Internet voting, whose views are often underrepresented yet critical for a comprehensive understanding of public trust in digital democracy. Researchers could also track emerging technologies like AI-based governance tools or state chatbots to assess whether institutional trust remains a dominant driver as technological novelty increase.

CRediT authorship contribution statement

Bogdan Romanov: Writing – review & editing, Writing – original draft, Visualization, Validation, Project administration, Methodology, Formal analysis, Data curation. **David Duenas Cid:** Writing – review & editing, Writing – original draft, Supervision, Methodology, Funding acquisition, Conceptualization. **Peeter Leets:** Methodology, Formal analysis, Data curation, Conceptualization.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work, the authors used Grammarly and ChatGPT in order to correct the grammatical errors/typos. After

using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

Funding

The work of Peeter Leets and Bogdan Romanov was supported by the Estonian Research Council under grant number PRG920 and by the European Union's Horizon 2020 Research and Innovation Program under grant agreement No 857622 "ERA Chair in EGovernance and Digital Public Services - ECePS".

The work of David Duenas-Cid has been funded by the Polish National Research Center's grant OPUS-20 - 2020/39/B/HS5/01661 and EU H2020 MSCA Program, grant agreement no. 101038055.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The authors are grateful for the feedback provided by Dr. Mihkel Solvak, Valeria Babayan, and Dr. Margarita Zavadskaya while reviewing the manuscript in question.

Appendix A. Details on the survey data collection

Table A1
Description of post-election surveys used in the study.

Post-election survey	Sampling method	Interview method	Number of respondents
2013 local	stratified random sample	CAPI	1042
2014 EP	stratified random sample	CAPI	1001
2015 parliamentary	stratified random sample	CAPI	1007
2017 local	stratified random sample	CATI	1000
2019 parliamentary	stratified random sample	CATI	1000
2019 EP	stratified random sample	CATI	1002
2021 local	stratified random sample	CATI(30%)/CAWI(70%)	1153
2023 parliamentary	stratified random sample	CATI(20%)/CAWI(80%)	1001

Note: CAPI – computer-assisted personal interview, CATI – computer-assisted telephone interview, CAWI – computer-assisted web interview.

All surveys are post-election, with fieldwork conducted 30 days after the election date. The surveys use stratified random samples and represent eligible voters in terms of age, gender, citizenship and language, settlement type, and region. The sampling frame was the Estonian Population Registry, which holds demographic data for the whole population and their phone and email addresses. Professional survey companies conducted the sampling and surveying. Table A1 lists the interview methods and number of respondents for all the surveys used in this study.

Appendix B. Data transformation

Table B1
Detailed information on the data transformation.

Variable name	Operationalization
Use of Internet voting	Transformed from categorical to binary: • 'voted in an advance polls by Internet and then revoted in polling station' was replaced with 1 • 'voted in an advance polls by Internet' was replaced with 1 • 'voted on the election day' was replaced with 0 • 'voted in an advance polls at polling station' was replaced with 0 • 'other' was replaced with 0
Mean	**Std. dev.** **Min** **25%** **50%** **75%** **Max**
0.579	0.499 0 0 1 1 1
PC Literacy	The variable is ordinal and ranges from 1 ('very good') to 5 ('no computer skills'), so the recoded variable was reverted: • 1 (very good) was replaced with 5 • 2 (good) was replaced with 4 • 3 (average) was replaced with 3 • 4 (basic) was replaced with 2 • 5 (no computer skills) was replaced with 1
Mean	**Std. dev.** **Min** **25%** **50%** **75%** **Max**
3.958	0.903 1 3 4 5 5
Gender	Initially, the variable was also binary with the following coding, 1 (male) and 2 (female), now the values are the following: • 'female' was replaced with 1 • 'male' was replaced with 0
Mean	**Std. dev.** **Min** **25%** **50%** **75%** **Max**
0.475	0.499 0 0 0 1 1
Education	The variable is ordinal and ranges from 1 to 4:

(*continued on next page*)

Table B1 (*continued*)

Variable name	Operationalization						
	• 'elementary/basic' is 1 • 'secondary education/gymnasium' is 2 • 'vocational secondary education' is 3 • 'higher' is 4						
Mean							**Std. dev.**
Min	**25%**	**50%**	**75%**		**Max**		
2.809	1.054	1	2	2	4		4
	The list of the sub-indicators is presented in Table 2, see below. All of them are ten of the indicators are ordinal variables from 10 ('trust completely') to 0 ('don't trust at all'). To ensure the data coherence, the string values were replaced in the following way:						
	• 'trust completely' was replaced with 10 • 'don't trust at all' was replaced with 0						
All sub-indicators of technological and institutional trusts							
Variable	**Mean**	**Std. dev.**	**Min**	**25%**	**50%**	**75%**	**Max**
Trust online banking	8.771	1.650	0.0	8.0	9.0	10.0	10.0
Trust online purchases	7.187	2.173	0.0	6.0	8.0	9.0	10.0
Trust declaring taxes online	8.906	1.640	0.0	8.0	10.0	10.0	10.0
Trust submitting health information online	8.346	2.072	0.0	8.0	9.0	10.0	10.0
Trust applying for documents online	8.562	1.829	0.0	8.0	9.0	10.0	10.0
Trust online voting	6.700	3.529	0.0	4.0	8.0	10.0	10.0
Trust government	5.889	2.944	0.0	4.0	7.0	8.0	10.0
Trust parliament	5.555	2.564	0.0	4.0	6.0	7.0	10.0
Trust president	7.342	2.807	0.0	6.0	8.0	9.0	10.0
Trust courts	6.733	2.601	0.0	5.0	7.0	9.0	10.0
Trust elections	7.271	2.756	0.0	6.0	8.0	9.0	10.0
Trust e state	7.372	2.639	0.0	6.0	8.0	9.0	10.0
	As for the technical errors and absence of answers from the respondents, they were converted as well:						
All variables	• 'DK', '97', '98' were replaced with NaN						
Variable	**Mean**	**Std. dev.**	**Min**	**25%**	**50%**	**75%**	**Max**
Age	48.529	16.804	17.0	35.0	48.0	61.0	89.0

Appendix C. Correlation output

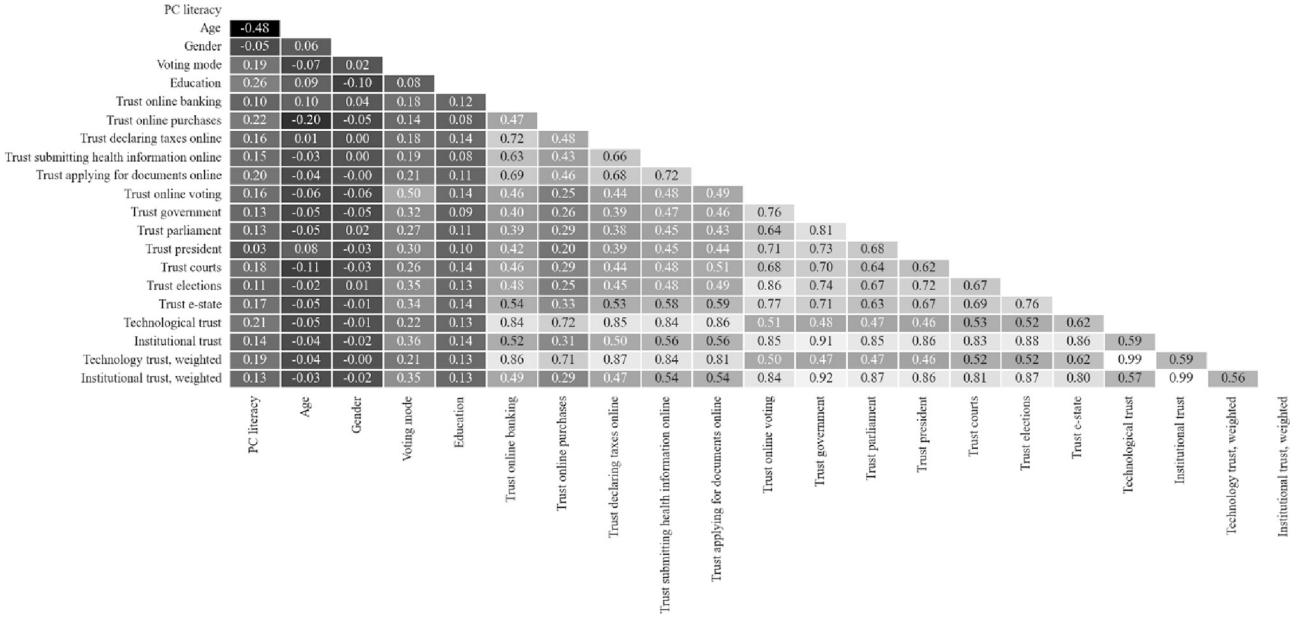

Fig. C1. The output of the correlation analysis (darker colors indicate a negative association, while lighter – positive).

Trust, in general, despite the trust object, is not age-dependent; there is no pattern in which older or younger people trust something more (the only hypothetical expectation is trust in online purchases). Trust in Internet voting is heavily correlated with trust in elections. Trust in Internet voting is associated with stand-alone trust in political institutions (correlation coefficients are higher than 0.64), while individual trust in political institutions is weakly associated with the indicators composing technological trust (correlation coefficients are less than 0.49).

Appendix D. Exploratory factor analysis details

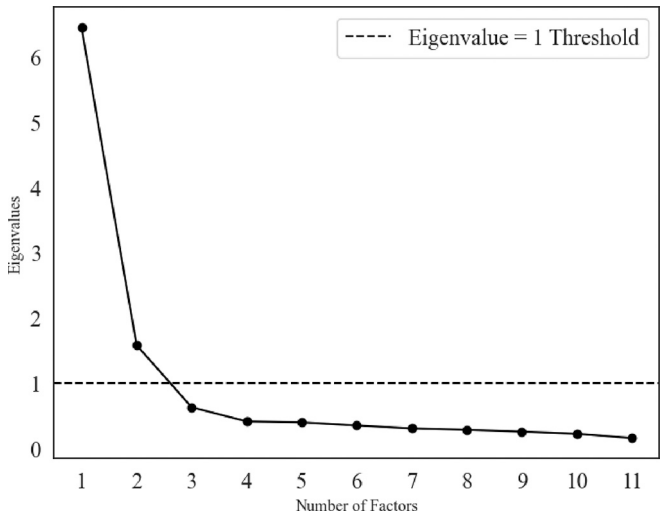

Fig. D1. Scree plot with the eigenvalues.

According to the elbow methods as well as the values of the eigenvalues, the data in question has two factors since in the range of eigenvalues, there are two values above the 1-threshold, and the visual representation indicates the "elbow" right exactly between 2 and 3 factors.

Appendix E. Confirmatory factor analysis details

Table E1
A technical assessment of the model's fit along with a qualitative interpretation. All coefficients and values are rounded to three decimals.

	Value of index
Degrees of Freedom (DoF)	43
Chi-Square (χ^2)	650.014, $p < 0.01$
Comparative Fit Index (CFI)	0.950
Goodness-of-Fit Index (GFI)	0.947
Adjusted Goodness-of-Fit Index (AGFI)	0.932
Normed Fit Index (NFI)	0.947
Tucker-Lewis Index (TLI)	0.936
Root Mean Square Error of Approximation (RMSEA)	0.097
Akaike Information Criterion (AIC)	45.119
Bayesian Information Criterion (BIC)	166.968

The model demonstrates an overall acceptable fit to the data, as indicated by indices such as the Comparative Fit Index (CFI = 0.950), Goodness-of-Fit Index (GFI = 0.947), and Adjusted Goodness-of-Fit Index (AGFI = 0.932), all of which meet or exceed commonly accepted thresholds of 0.95. However, the Root Mean Square Error of Approximation (RMSEA = 0.097) slightly exceeds the acceptable range, suggesting room for improvement in the model's approximation error. While the chi-square statistic ($\chi^2 = 650.014$, $p < 0.01$) indicates a significant difference between the observed and predicted covariance matrices, its sensitivity to sample size necessitates reliance on alternative indices. Overall, the model is a reasonable fit, though further refinements, such as reassessing factor loadings or exploring modification indices, could improve its alignment with the observed data.

Appendix F. Assessment of regression models quality

F.1. Linear model

Although multiple linear regression models were estimated in this study, assumption testing was conducted in detail for a model predicting trust in Internet voting with non-aggregated trust indices. All linear models share the same structure, use the same predictors, and rely on similar outcome variable scaling and distributions. Given this structural similarity, the assumptions examined (linearity, homoscedasticity, residual normality, and multicollinearity) are expected to apply similarly across the full set of models.

F.2. Linearity and heteroscedasticity

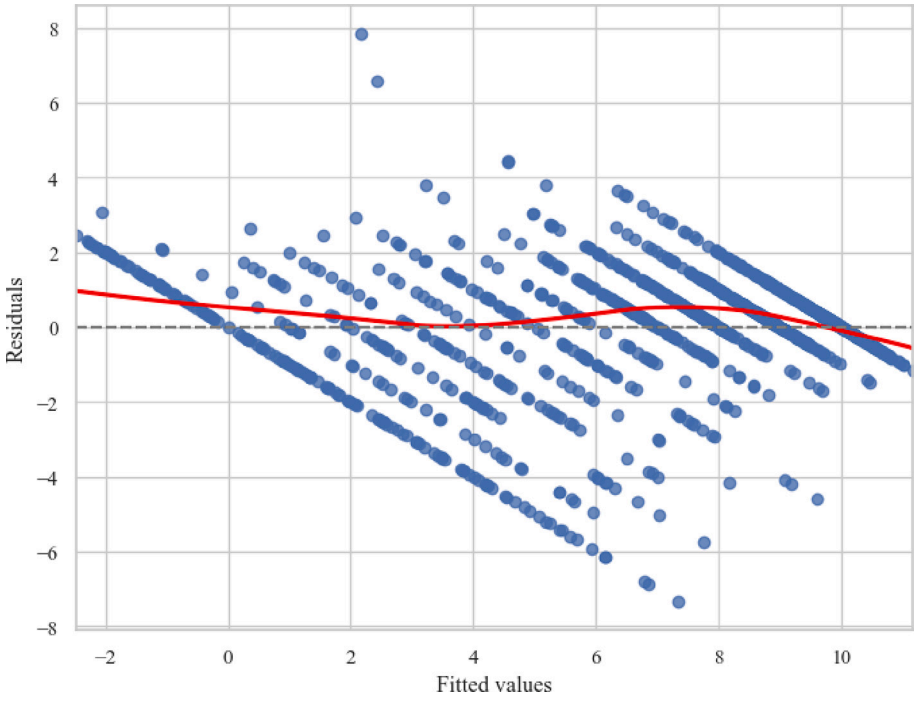

Fig. F1. Residuals vs Fitted (Linearity and Homoscedasticity).

A residuals-versus-fitted values plot revealed visible curvature and a fan-like spread, indicating violations of both the linearity and homoscedasticity assumptions. To formally assess heteroscedasticity, the Breusch–Pagan test was conducted, which returned highly significant results (F-statistic = 7.77, $p < 0.001$), confirming non-constant variance in the residuals.

F.3. Normality of residuals

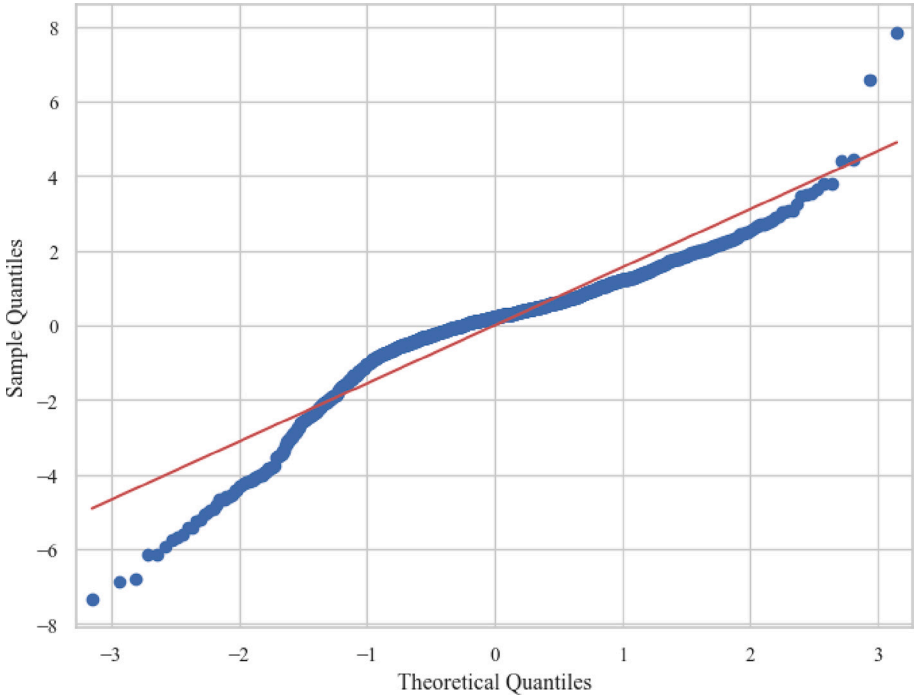

Fig. F2. Q-Q plot of residuals.

The Q–Q plot of residuals showed notable deviations from the reference line at both tails. The Shapiro–Wilk test further rejected the null hypothesis of normality ($p < 0.001$). These results suggest that the residuals are not normally distributed due to skewness.

F.4. Multicollinearity

Variance inflation factors (VIFs) were computed to assess multicollinearity among the predictors. All VIF values fell well below the commonly accepted threshold of 5, indicating no problematic multicollinearity. This is also supported by the correlation matrix output in Fig. C1.

Table F3
VIF values for the linear model.

Variable	VIF
const	75.935915
PC literacy	1.537340
Age	1.541769
Gender	1.046893
Education	1.186099
Trust online banking	2.735779
Trust online purchases	1.521666
Trust declaring taxes online	2.633847
Trust submitting health information online	2.511452
Trust applying for documents online	2.833295
Trust government	4.321448
Trust parliament	3.262801
Trust president	2.840591
Trust courts	2.535666
Trust elections	3.308281
Trust e-state	3.354862

F.5. Outliers

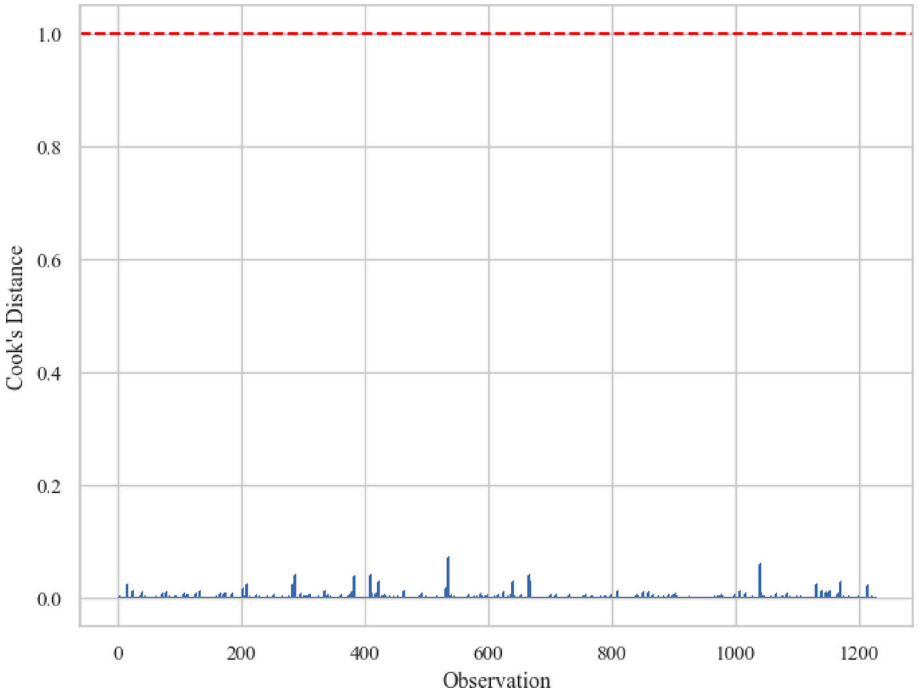

Fig. F4. Cook's distance for linear regression.

Cook's distance was calculated to detect overly influential cases. The distribution of values showed no instances exceeding the conventional cutoff of 1, suggesting that no individual observations disproportionately influenced the model estimates.

F.6. Logistic model

F.6.1. Linearity of the logit

A Box–Tidwell interaction term was used to test whether the continuous predictor Age exhibited a linear relationship with the logit of the dependent variable. The resulting interaction term (Age × log(Age)) was statistically insignificant ($p = 0.396$), indicating that the assumption of linearity in the logit was satisfied. The term was excluded from the final model specification.

F.6.2. Multicollinearity

Variance inflation factors (VIFs) were computed for all predictors. All values remained well below the commonly accepted threshold of 5 (maximum VIF = 4.33 for Trust in government), suggesting no problematic collinearity among explanatory variables.

Table F5
VIF values for the logistic model.

Variable	VIF
const	76.080704
PC literacy	1.536756
Age	1.543536
Gender	1.046908
Education	1.18493
Trust online banking	2.737111
Trust online purchases	1.522979
Trust declaring taxes online	2.634147
Trust submitting health information online	2.511967
Trust applying for documents online	2.830027
Trust government	4.334257
Trust parliament	3.268706
Trust president	2.825703
Trust courts	2.533883
Trust elections	3.306455
Trust e-state	3.351864

F.6.3. Outliers

Cook's distance was calculated to detect high-leverage or overly influential cases. No observations exceeded the conventional threshold of 1, and the vast majority exhibited negligible influence, confirming that model estimates were not distorted by individual outliers.

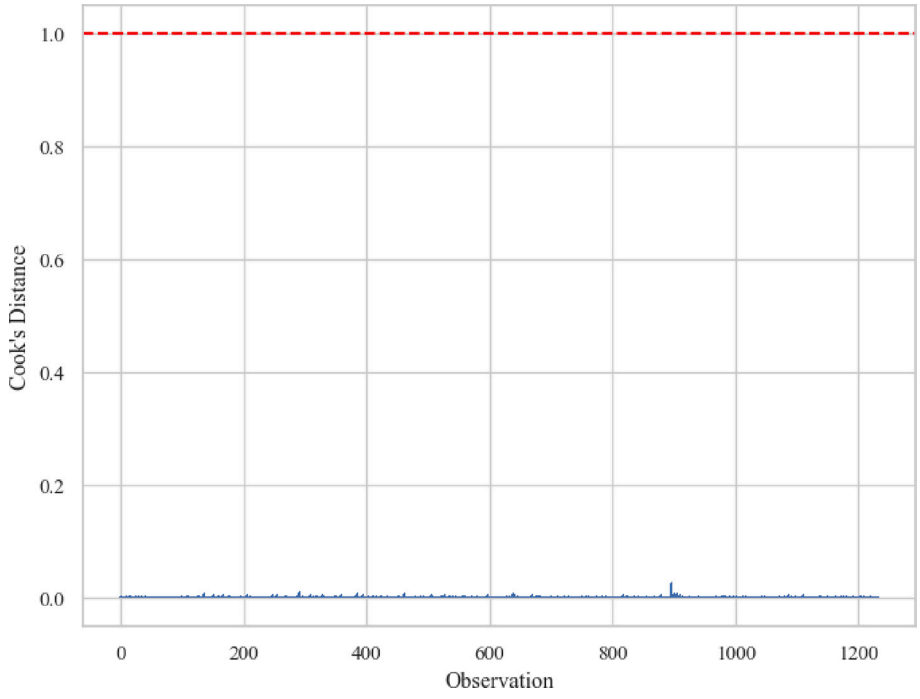

Fig. F6. Cook's distance for the logistic model.

F.6.4. Corrections

Given that the first two models demonstrated violations of key assumptions (heteroscedasticity and non-normality of residuals), heteroscedasticity-consistent robust standard errors (HC3) were applied uniformly across all linear and logistic models (it includes models 1-6). This ensures consistent and conservative inference across structurally similar models based on the same survey data and measurement instruments. This adjustment does not alter coefficient estimates but corrects standard errors and associated significance tests, thereby ensuring more reliable inference. Additionally, examined polynomial transformations for continuous variables to explore potential non-linear relationships but found that robust estimation was sufficient for addressing the identified violations.

Appendix G. Detailed regression outputs

Table G1
Models 1 and 2 regression output. All coefficients are rounded to three decimals. Robust standard errors (HC3) are reported in parentheses.

	Model 1: Trust in Internet Voting, OLS	Model 2: Internet Voting Usage, Logistic
const	-2.147***	-3.304***
	(0.463)	(0.569)
Trust online banking	0.008	-0.035
	(0.059)	(0.065)
Trust online purchases	-0.023	0.024
	(0.027)	(0.036)
Trust declaring taxes online	0.003	-0.001
	(0.065)	(0.062)
Trust submitting health information online	-0.01	-0.034
	(0.045)	(0.049)
Trust applying for documents online	-0.005	-0.008
	(0.055)	(0.059)
Trust government	0.284***	0.098**
	(0.046)	(0.044)
Trust parliament	-0.147***	-0.053
	(0.038)	(0.045)
Trust president	0.103***	0.074**
	(0.038)	(0.038)
Trust courts	0.041	-0.071*
	(0.035)	(0.039)
Trust elections	0.690***	0.144***
	(0.052)	(0.041)
Trust e-state	0.246***	0.137***
	(0.046)	(0.044)
PC literacy	0.131**	0.427***
	(0.067)	(0.087)
Age	-0.005	0
	(0.003)	(0.005)
Gender	-0.293***	0.168
	(0.093)	(0.13)
Education	0.061	-0.02
	(0.044)	(0.065)
R-squared/Pseudo R-squared	0.806	0.132
R-squared Adj.	0.803	—
No. Observations:	1227	1232

Robust standard errors are in parentheses. * p<.1, ** p<.05, ***p<.01.

Table G2
Models 3 and 4 regression output. All coefficients are rounded to three decimals. Robust standard errors (HC3) are reported in parentheses.

	Model 3: Trust in Internet Voting, OLS	Model 4: Internet Voting Usage, Logistic
const	-2.130***	-3.305***
	(0.494)	(0.552)
Technology trust, weighted	0.0021	-0.032
	(0.050)	(0.049)
Institutional trust, weighted	1.264***	0.331***
	(0.029)	(0.034)
PC literacy	0.114	0.413***
	(0.076)	(0.086)
Age	-0.003	0.001
	(0.004)	(0.004)
Gender	-0.272**	0.148
	(0.107)	(0.126)
Education	0.068	-0.023
	(0.053)	(0.064)
R-squared/Pseudo R-squared	0.737	0.1143
R-squared Adj.	0.736	—
No. Observations:	1227	1232

Standard errors are in parentheses. * p<.1, ** p<.05, ***p<.01.

References

Abdala, M. B., Plescia, C., Boyer, M. M., & Brunetti, A. L. (2025). Trust in government or in technology? What really drives internet voting. *Political Research Quarterly*. https://doi.org/10.1177/10659129251321424, 10659129251321424.

Abdulkareem, A. K., Abdulkareem, Z. J., Ishola, A. A., & Akindele, I. T. (2022). Does e-government impact e-participation? The influence of trust in e-government. *International Review of Public Administration, 27*(2), 91–110. https://doi.org/10.1080/12294659.2022.2071540

Abu-Shanab, E. (2014). Antecedents of trust in e-government services: An empirical test in Jordan. *Transforming Government: People, Process and Policy, 8*(4), 480–499. https://doi.org/10.1108/TG-08-2013-0027

Acemyan, C. Z., Kortum, P., & Oswald, F. L. (2022). The trust in voting systems (TVS) measure. *International Journal of Technology and Human Interaction, 18*(1), 1–23. https://doi.org/10.4018/IJTHI.293196

Alomari, M. K. (2016). E-voting adoption in a developing country. *Transforming Government: People, Process and Policy, 10*(4), 526–547. https://doi.org/10.1108/TG-11-2015-0046

Alomari, M., Woods, P., & Sandhu, K. (2012). Predictors for e-government adoption in Jordan. *Information Technology & People, 25*(2), 207–234. https://doi.org/10.1108/09593841211232712

Alvarez, R. M., Cao, J., & Li, Y. (2021). Voting experiences, perceptions of fraud, and voter confidence. *Social Science Quarterly, 102*(4), 1225–1238. https://doi.org/10.1111/ssqu.12940

Anderson, M. R. (2010). Community psychology, political efficacy, and trust. *Political Psychology, 31*(1), 59–84. https://doi.org/10.1111/j.1467-9221.2009.00734.x

Babayan, V., Marques, I., Mironyuk, M., & Turobov, A. (2021). *Public trust in internet voting systems: Evidence from Russian Public Opinion (SSRN Scholarly Paper 3976188)*. https://doi.org/10.2139/ssrn.3976188

Beck, U. (1992). *Risk society: Towards a new modernity*. SAGE Publications.

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems, 17*(2), 165–176. https://doi.org/10.1016/j.jsis.2007.12.002

Beldad, A., van der Geest, T., de Jong, M., & Steehouder, M. (2012). Shall I tell you Where I Live and Who I Am? Factors influencing the behavioral intention to disclose personal data for online government transactions. *International Journal of Human Computer Interaction, 28*(3), 163–177. https://doi.org/10.1080/10447318.2011.572331

Bodó, B. (2021). Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society, 23*(9), 2668–2690. https://doi.org/10.1177/1461444820939922

Carter, L., & Belange, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal, 15*(1), 5–25.

Carter, L., & Campbell, R. (2011). The impact of trust and relative advantage on internet voting diffusion. *Journal of Theoretical and Applied Electronic Commerce Research, 6*(3), 7–8. https://doi.org/10.4067/S0718-18762011000300004

Carter, L., & Campbell, R. (2012). Internet voting usefulness: An empirical analysis of trust, convenience and accessibility. *Journal of Organizational and End User Computing (JOEUC), 24*(3), 1–17. https://doi.org/10.4018/joeuc.2012070101

Ciechanowski, L., Przegalinska, A., Magnuski, M., & Gloor, P. (2019). In the shades of the uncanny valley: An experimental study of human–chatbot interaction. *Future Generation Computer Systems, 92*, 539–548. https://doi.org/10.1016/j.future.2018.01.055

Cook, K. S., Hardin, R., & Levi, M. (2005). *Cooperation Without Trust?* Russell Sage Foundation.

Demirdoven, B., Cubuk, E. B. S., & Karkin, N. (2020). Establishing relational trust in e-Participation: A systematic literature review to propose a model. In *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance* (pp. 341–348). https://doi.org/10.1145/3428502.3428549

Dueñas-Cid, D. (2024). *Trust and Distrust in electoral technologies: What can we learn from the failure of electronic voting in the Netherlands (2006/07)* (pp. 669–677). https://doi.org/10.1145/3657054.3657262

Duenas-Cid, D., & Calzati, S. (2023). Dis/Trust and data-driven technologies. *Internet Policy Review, 12*(4). https://doi.org/10.14763/2023.4.1727

Easton, D. (1975). A Re-assessment of the concept of political support. *British Journal of Political Science, 5*(4), 435–457. https://doi.org/10.1017/S0007123400008309

Ehin, P., & Solvak, M. (2021). Party cues and trust in remote internet voting: Data from Estonia 2005–2019. In R. Krimmer, M. Volkamer, D. Duenas-Cid, O. Kulyk, P. Rønne, M. Solvak, & M. Germann (Eds.), *Electronic voting* (pp. 75–90). Springer International Publishing. https://doi.org/10.1007/978-3-030-86942-7_6.

Ehin, P., Solvak, M., Willemson, J., & Vinkel, P. (2022). Internet voting in Estonia 2005–2019: Evidence from eleven elections. *Government Information Quarterly, 39*(4), Article 101718. https://doi.org/10.1016/j.giq.2022.101718

Erb, Y., Duenas-Cid, D., & Volkamer, M. (2023). *Identifying Factors Studied for Voter Trust in E-Voting—Review of Literature*. https://doi.org/10.18420/E-VOTE-ID2023_05

Espinosa, V. I., & Pino, A. (2025). E-government as a development strategy: The case of Estonia. *International Journal of Public Administration, 48*(2), 86–99. https://doi.org/10.1080/01900692.2024.2316128

Estonia 2024 Digital Decade Country Report | Shaping Europe's digital future. Retrieved July 10, 2025, from https://digital-strategy.ec.europa.eu/en/factpages/estonia-2024-digital-decade-country-report, (2025).

Evans, A. M., & Krueger, J. I. (2009). The psychology (and economics) of trust. *Social and Personality Psychology Compass, 3*(6), 1003–1017. https://doi.org/10.1111/j.1751-9004.2009.00232.x

Fukuyama, F. (1995). *Trust: The Social Virtues and the Creation of Prosperity*. Free Press.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Inexperience and experience with online stores: The importance of tam and trust. *IEEE Transactions on Engineering Management, 50*(3), 307–321. https://doi.org/10.1109/TEM.2003.817277

Gefen, D., Rose, G. M., Warkentin, M., & Pavlou, P. A. (2005). *Cultural diversity and trust in IT adoption* (p. 25).

Giddens, A. (1990). *The Consequences of Modernity*. Stanford University Press.

Giddens, A. (1991). *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Stanford University Press.

Grimmelikhuijsen, S. G., & Meijer, A. J. (2014). Effects of transparency on the perceived trustworthiness of a government organization: Evidence from an online experiment. *Journal of Public Administration Research and Theory, 24*(1), 137–157. https://doi.org/10.1093/jopart/mus048

Grimmelikhuijsen, S., Jilke, S., Olsen, A. L., & Tummers, L. (2017). Behavioral public administration: combining insights from public administration and psychology. *Public Administration Review, 77*(1), 45–56. https://doi.org/10.1111/puar.12609

Hamacher, A., Bianchi-Berthouze, N., Pipe, A. G., & Eder, K. (2016). Believing in BERT: Using expressive communication to enhance trust and counteract operational error in physical Human-robot interaction. In *2016 25th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN)* (pp. 493–500). https://doi.org/10.1109/ROMAN.2016.7745163

Hardin, R. (2002). *Trust and Trustworthiness*. Russell Sage Foundation.

Himelboim, I., Lariscy, R. W., Tinkham, S. F., & Sweetser, K. D. (2012). Social media and online political communication: The role of interpersonal informational trust and openness. *Journal of Broadcasting & Electronic Media, 56*(1), 92–115. https://doi.org/10.1080/08838151.2011.648682

Homburg, V., Moody, R., Yang, Q., & Bekkers, V. (2022). Adopting microblogging solutions for interaction with government: Survey results from Hunan province, China. *International Review of Administrative Sciences, 88*(1), 76–94. https://doi.org/10.1177/0020852319887480

Horsburgh, S., Goldfinch, S., & Gauld, R. (2011). Is public trust in government associated with trust in e-government? *Social Science Computer Review, 29*(2), 232–241. https://doi.org/10.1177/0894439310368130

Janssen, M., Rana, N. P., Slade, E. L., & Dwivedi, Y. K. (2018). Trustworthiness of digital government services: Deriving a comprehensive theory through interpretive structural modelling. *Public Management Review, 20*(5), 647–671. https://doi.org/10.1080/14719037.2017.1305689

Kattel, R., & Mergel, I. (2019). Estonia's digital transformation: Mission Mystique and the hiding hand. In P. Hart, & M. Compton (Eds.), *Great Policy Successes*. Oxford University Press. https://doi.org/10.1093/oso/9780198843719.003.0008.

Kneuer, M. (2016). E-democracy: A new challenge for measuring democracy. *International Political Science Review, 37*(5), 666–678. https://doi.org/10.1177/0192512116657677

Koller, M. (1988). Risk as a determinant of trust. *Basic and Applied Social Psychology, 9*(4), 265–276. https://doi.org/10.1207/s15324834basp0904_2

Kozel, E., & Dečman, M. (2022). The Impact of Trust in Government – Young Voters' Behavioral Intention to Use I-voting in Slovenia. *NISPAcee Journal of Public Administration and Policy, 15*(1), 61–87. https://doi.org/10.2478/nispa-2022-0004

Kralj, L. (2023). *Estonia: A snapshot of digital skills | Digital Skills and Jobs Platform*. https://digital-skills-jobs.europa.eu/en/latest/briefs/estonia-snapshot-digital-skills.

Kulyk, O., Budurushi, J., Dalela, A., & Agbesi, S. (2022). *"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*. http://hdl.handle.net/10062/84312.

Lankton, N., McKnight, D., & Tripp, J. (2015). Technology, humanness, and trust: Rethinking trust in technology. *Journal of the Association for Information Systems, 16*(10). https://doi.org/10.17705/1jais.00411

Latusek, D., Hamm, J. A., de Beeck, S. O., Ropp, J., Six, F., van Zimmeren, E., & Verhoest, K. (2025). *1: Trust in public governance: Scoping the field*. https://www.elgaronline.com/edcollchap/book/9781802201406/chapter1.xml.

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors, 31*.

Levi, M., & Stoker, L. (2000). Political trust and trustworthiness. *Annual Review of Political Science, 3*(2000), 475–507. https://doi.org/10.1146/annurev.polisci.3.1.475

Lin, H.-F. (2011). An empirical investigation of mobile banking adoption: The effect of innovation attributes and knowledge-based trust. *International Journal of Information Management, 31*(3), 252–260. https://doi.org/10.1016/j.ijinfomgt.2010.07.006

Lippert, S. K., & Davis, M. (2006). A conceptual model integrating trust into planned change activities to enhance technology adoption behavior. *Journal of Information Science, 32*(5), 434–448.

Lu, J., Qi, L., & Yu, X. (2019). Political trust in the internet context: A comparative study in 36 countries. *Government Information Quarterly, 36*(4), Article 101386. https://doi.org/10.1016/j.giq.2019.06.003

Luhmann, N. (1979). *Trust and power: Two works*. Wiley.

Luo, C., Hasan, N. A. M., & Zamri Bin Ahmad, A. M. (2024). Exploring satisfaction and trust as key drivers of e-government continuance intention: Evidence from China for sustainable digital governance. *Sustainability, 16*(24). https://doi.org/10.3390/su162411068. Article 24.

Mahrer, H., & Krimmer, R. (2005). Towards the enhancement of e-democracy: Identifying the notion of the 'middleman paradox.'. *Information Systems Journal, 15*(1), 27–42. https://doi.org/10.1111/j.1365-2575.2005.00184.x

Margetts, H., Lehdonvirta, V., González-Bailón, S., Hutchinson, J., Bright, J., Nash, V., & Sutcliffe, D. (2021). The Internet and public policy: Future directions. *Policy & Internet, 13*(2), 162–184. https://doi.org/10.1002/poi3.263

Mayer, R. C., Davis, J. H., & Schoorman, D. (1995). *An integrative model of organizational trust*.

McKnight, D. H., & Chervany, N. L. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce, 6*(2), 35–59. https://doi.org/10.1080/10864415.2001.11044235

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81

McKnight, H., Carter, M., & Clay, P. (2009). Trust in technology: Development of a set of constructs and measures. In *DIGIT 2009 Proceedings*. https://aisel.aisnet.org/digit2009/10.

Mendez, F., & Serdült, U. (2017). What drives fidelity to internet voting? Evidence from the roll–out of internet voting in Switzerland. *Government Information Quarterly, 34*(3), 511–523. https://doi.org/10.1016/j.giq.2017.05.005

Mensah, I. K. (2020). The impact of political trust on e-government services adoption. *International Journal of Technology Diffusion (IJTD), 11*(4), 27–47. https://doi.org/10.4018/IJTD.2020100102

Mishler, W., & Rose, R. (2001). What are the origins of political trust? Testing institutional and cultural theories in post-communist societies. *Comparative Political Studies, 34*(1), 30–62. https://doi.org/10.1177/0010414001034001002
Mooradian, T., Renzl, B., & Matzler, K. (2006). Who trusts? Personality, trust and knowledge sharing. *Management Learning, 37*(4), 523–540. https://doi.org/10.1177/1350507606073424
Murnighan, J. K., Malhotra, D., & Weber, J. M. (2004). Paradoxes of trust: Empirical and theoretical departures from a traditional model. In *Trust and distrust in organizations: Dilemmas and approaches* (pp. 293–326). Russell Sage Foundation. https://psycnet.apa.org/record/2004-16590-012.
Norris, P., & Nai, A. (Eds.). (2017). *Election Watchdogs: Transparency, accountability and integrity*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190677800.001.0001.
Oostveen, A.-M. (2010). Outsourcing democracy: Losing control of e-voting in the Netherlands. *Policy & Internet, 2*(4), 201–220. https://doi.org/10.2202/1944-2866.1065
Parent, M., Vandebeek, C. A., & Gemino, A. C. (2005). Building citizen trust through e-government. *Government Information Quarterly, 22*(4), 720–736. https://doi.org/10.1016/j.giq.2005.10.001
Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275
Perez, V., & Ross, J. M. (2020). Federalism and polycentric government in a pandemic. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3570726
Population Figure. (2025). Statistikaamet. Retrieved July 10, 2025, from https://stat.ee/en/find-statistics/statistics-theme/population/population-figure.
Putnam, R. (2001). *Bowling alone: The collapse and revival of American community*. Simon and Schuster.
Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should i trust you?" Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 1135–1144).
Riigikogu Elections. (2025). Elections in Estonia. Retrieved July 10, 2025, from https://www.valimised.ee/en/archive/riigikogu-parliament-elections/riigikogu-elections.
Ripamonti, J. P. (2024). Does being informed about government transparency boost trust? Exploring an overlooked mechanism. *Government Information Quarterly, 41*(3), Article 101960. https://doi.org/10.1016/j.giq.2024.101960
Rodríguez-Pérez, A. (2022). The Council of Europe's CM/Rec(2017)5 on e-voting and Secret Suffrage: Time for yet another update? In R. Krimmer, M. Volkamer, D. Duenas-Cid, P. Rønne, & M. Germann (Eds.), *Electronic voting* (pp. 90–105). Springer International Publishing. https://doi.org/10.1007/978-3-031-15911-4_6.
Rogers, E. M. (2003). *Diffusion of Innovations* (5th ed.). Simon and Schuster.
Santa, R., MacDonald, J. B., & Ferrer, M. (2019). The role of trust in *e*-Government effectiveness, operational effectiveness and user satisfaction: Lessons from Saudi Arabia in e-G2B. *Government Information Quarterly, 36*(1), 39–50. https://doi.org/10.1016/j.giq.2018.10.007
Schaupp, C. L., & Carter, L. (2005). E-voting: From apathy to adoption. *Journal of Enterprise Information Management, 18*(5), 586–601. https://doi.org/10.1108/17410390510624025
Sharma, S. (2020). Can't change my political disaffection! The role of political disaffection, trust, and resistance to change in internet voting. *Digital Policy, Regulation and Governance, 22*(2), 71–91. https://doi.org/10.1108/DPRG-07-2019-0049
Shin, D.-H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers, 22*(5), 428–438. https://doi.org/10.1016/j.intcom.2010.05.001
Simmel, G. (2011). *The philosophy of money*. Routledge. https://doi.org/10.4324/9780203828298
Simon, J. (2020). *The Routledge handbook of trust and philosophy*. Routledge.
Sindermann, C., Rozgonjuk, D., Solvak, M., Realo, A., & Vassil, K. (2023). Internet voting: The role of personality traits and trust across three parliamentary elections in Estonia. *Current Psychology, 42*(30), 26555–26569. https://doi.org/10.1007/s12144-022-03644-4
Solvak, M., & Vassil, K. (2018). Could internet voting halt declining electoral turnout? New evidence that E-voting is habit forming: Internet voting and habit formation. *Policy & Internet, 10*(1), 4–21. https://doi.org/10.1002/poi3.160
Solvak, M., Unt, T., Rozgonjuk, D., Võrk, A., Veskimäe, M., & Vassil, K. (2019). E-governance diffusion: Population level e-service adoption rates and usage patterns. *Telematics and Informatics, 36*, 39–54. https://doi.org/10.1016/j.tele.2018.11.005
Sztompka, P. (1999). *Trust: A sociological theory*. Cambridge University Press.
Tolbert, C. J., & Mossberger, K. (2006). The effects of E-government on trust and confidence in government. *Public Administration Review, 66*(3), 354–369. https://doi.org/10.1111/j.1540-6210.2006.00594.x
Toots, M. (2019). Why E-participation systems fail: The case of Estonia's Osale.ee. *Government Information Quarterly, 36*(3), 546–559. https://doi.org/10.1016/j.giq.2019.02.002
Tyler, T. R., & Huo, Y. J. (2002). *Trust in the law: Encouraging public cooperation with the police and courts. xvi* p. 248). Russell Sage Foundation.
Vassil, K., Solvak, M., Vinkel, P., Trechsel, A. H., & Alvarez, R. M. (2016). The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015. *Government Information Quarterly, 33*(3), 453–459. https://doi.org/10.1016/j.giq.2016.06.007
Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478.
Volkamer, M., Spycher, O., & Dubuis, E. (2011). Measures to establish trust in internet voting. In *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance* (pp. 1–10). https://doi.org/10.1145/2072069.2072071
Wang, Y.-F., Chen, Y.-C., & Chien, S.-Y. (2023). Citizens' intention to follow recommendations from a government-supported AI-enabled system. *Public Policy and Administration*. https://doi.org/10.1177/09520767231176126, 09520767231176126.
Warkentin, M., Gefen, D., Pavlou, P. A., & Rose, G. M. (2002). Encouraging citizen adoption of e-government by building trust. *Electronic Markets, 12*(3), 157–162. https://doi.org/10.1080/101967802320245929
Warkentin, M., Sharma, S., Gefen, D., Rose, G. M., & Pavlou, P. (2018). Social identity and trust in internet-based voting adoption. *Government Information Quarterly, 35*(2), 195–209. https://doi.org/10.1016/j.giq.2018.03.007
Welch, E. W., Hinnant, C. C., & Moon, M. J. (2005). Linking citizen satisfaction with E-government and trust in government. *Journal of Public Administration Research and Theory, 15*(3), 371–391. https://doi.org/10.1093/jopart/mui021
Werbach, K. (2018). Trust, but Verify: Why the blockchain needs the law. *Berkeley Technology Law Journal, 33*(2), 487–550.
Wolf, P., Nackerdien, R., & Tuccinardi, D. (2011). *Introducing electronic voting: Essential considerations*. International Institute for Democracy and Electoral Assistance (With International Institute for Democracy and Electoral Assistance).
Wong, L.-W., Tan, G. W.-H., Ooi, K.-B., & Dwivedi, Y. (2023). The role of institutional and self in the formation of trust in artificial intelligence technologies. *Internet Research, 34*(2), 343–370. https://doi.org/10.1108/INTR-07-2021-0446
Zada, P., Falzon, G., & Kwan, P. (2016). Perceptions of the Australian public towards mobile internet e-voting: Risks, choice and trust. *Electronic Journal of E-Government, 14*(1). Article 1.
Zand, D. E. (1972). Trust and managerial problem solving. *Administrative Science Quarterly, 17*(2), 229–239. https://doi.org/10.2307/2393957
Zhang, P., & Zhou, M. (2020). Security and trust in blockchains: Architecture, key technologies, and open issues. *IEEE Transactions on Computational Social Systems, 7*(3), 790–801. https://doi.org/10.1109/TCSS.2020.2990103
Zhou, T. (2011). Understanding online community user participation: A social influence perspective. *Internet Research, 21*(1), 67–81. https://doi.org/10.1108/10662241111104884
Zhu, Y.-Q., Azizah, A. H., & Hsiao, B. (2021). Examining multi-dimensional trust of technology in citizens' adoption of e-voting in developing countries. *Information Development, 37*(2), 193–208. https://doi.org/10.1177/0266666920902819

Bogdan Romanov is a Junior Research Fellow and Ph.D. candidate at the Johan Skytte Institute of Political Studies, University of Tartu (2021-present). His research focuses on digital governance, e-participation, and online voting, with particular attention to its adoption under various political contexts, including electoral autocracies. Bogdan holds an MA in Democracy and Governance from the University of Tartu (2021), where his thesis explored health policy responses. Previously, he worked as a data analyst in the financial sector.

David Dueñas-Cid is an Associate Professor and Director of the Pubic Sector Data-Driven Research Program at Kozminski University. His research expertise includes electronic democracy, internet voting, and trust dynamics in digital governance. Previously, he held research positions at Tallinn University of Technology, Universitat Rovira i Virgili, and Tallinn University of Technology. He obtained his PhD on social movement politicization and currently leads research on trust and distrust in internet voting, funded by the H2020 Marie Skłodowska-Curie Actions and the Polish National Science Centre. He chairs extensive international collaborations.

Peeter Leets is currently a Developer at the University of Tartu's Johan Skytte Institute of Political Studies, a position he has held since July 2023. Previously, he worked as an Analyst at the same institute. Peeter earned his Master's degree in 2022, focusing on augmenting public sector decision-making with expert knowledge. His academic journey includes a Master's in Democracy and Government in the Digital Age (2022) and a Bachelor's in Political Science (2020), both from the University of Tartu. His research interests involve data-driven decision support systems in the public sector.