



Volume 15 | Issue 4



RESEARCH
ARTICLE



OPEN
ACCESS



PEER
REVIEWED

Creating trust and distrust in internet voting: a Q-methodological study from Estonia

David Dueñas-Cid *Kozminski University*

Bogdan Romanov *University of Tartu*

DOI: <https://doi.org/10.14763/2026.4.2124>

Published: 1 October 2026

Received: 19 April 2025 **Accepted:** 19 May 2026

Funding: 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. The work of 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".

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Licence: This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. <https://creativecommons.org/licenses/by/3.0/de/deed.en>
Copyright remains with the author(s).

Citation: Dueñas-Cid, D., & Romanov, B. (2026). Creating trust and distrust in internet voting: a Q-methodological study from Estonia. *Internet Policy Review*, 15(4). <https://doi.org/10.14763/2026.4.2124>

Keywords: Trust, Distrust, Internet voting, Estonia, Democracy

Abstract: This article investigates how trust and distrust in internet voting are constructed in Estonia, the only country to have used nationwide internet voting in legally binding elections for two decades. Drawing on expert interviews and Q-methodology with Estonian citizens, the study maps how both expert and public discourses articulate confidence and scepticism toward internet voting. Three discourses emerge: 1) Institutional trust and practical optimism, highlighting habitual use, institutional reliability, and everyday convenience; 2) Concerns over transparency and accessibility, emphasising openness, communication, and inclusivity; and 3) Scepticism about security and human vulnerabilities, focusing on system opacity, the concentration of control, and human error. The analysis reveals an asymmetry between trust and distrust narratives: while trust discourses are well-developed and grounded in experience and institutional legitimacy, distrust discourses remain reactive and less differentiated, blending technical and political concerns. The findings suggest that in digitally advanced contexts, long-term exposure to functioning e-governance systems consolidates complex justifications for trust, whereas scepticism, though persistent, lacks structural articulation. The study contributes to broader debates on democratic legitimacy in digital elections, demonstrating that trust in internet voting depends as much on political culture and institutional transparency as on technological performance.

Introduction

Trust is a cornerstone of democratic governance, enabling citizens to accept vulnerability under conditions of uncertainty and to recognise the legitimacy of political institutions (Braithwaite, 1998; Hardin, 2002; Luhmann, 1979; Warren, 2018). Nowhere is this more critical than in the conduct of elections, which must be perceived as both fair and credible to ensure that outcomes are broadly accepted. As societies undergo rapid digital transformation, electoral processes have increasingly integrated technological solutions, raising new opportunities and challenges for democratic legitimacy (Castells, 2013; Norris, 2002).

The incorporation of technology into elections is not a recent phenomenon. Innovations such as electronic voter lists, ballot scanners, and voting machines have been widely deployed to improve efficiency and accuracy (Krimmer, 2012). More ambitious reforms, however, involve internet voting, which allows citizens to cast ballots remotely via digital platforms (Alvarez et al., 2009, 2011). Initially promoted to counter declining turnout, enhance accessibility, and modernise election administration, internet voting has generated significant scholarly and policy debate. While proponents emphasise its convenience and potential to increase participation among specific groups (Solvak & Vassil, 2018), critics highlight the heightened risks to security, transparency, and public trust (Carter & Campbell, 2011; Mahrer & Krimmer, 2005).

Trust remains central to these debates. Without sufficient levels of public confidence, the introduction of internet voting risks undermining rather than strengthening democratic legitimacy. Scholars have demonstrated that trust in electoral technologies extends beyond technical reliability to broader political and institu-

tional contexts, including confidence in electoral authorities, governments, and legal safeguards (Ehin & Solvak, 2021; Werbach, 2018). Distrust, in turn, does not necessarily represent the absence of trust but may function as a constructive force, demanding accountability and reinforcing vigilance over electoral processes (Six & Latusek, 2023). The coexistence of trust and distrust highlights the complexity of digital elections, where technical performance, institutional transparency, and political culture are deeply intertwined (Mayer et al., 1995).

Against this backdrop, the central research question guiding this study is: how are trust and distrust in Internet voting constructed, and what arguments shape their formation across technological and political dimensions? Addressing this question is particularly important in digitally advanced democracies such as Estonia, where internet voting has been embedded within broader e-governance infrastructures and used in legally binding elections for nearly two decades. Rather than examining hypothetical expectations surrounding internet voting, the Estonian case allows for the analysis of trust and distrust discourses shaped by long-term exposure, institutional familiarity, and practical experience with the system.

The article is structured as follows. The next section reviews the existing literature on trust, distrust, and electoral technologies, highlighting key theoretical and empirical debates. This is followed by a methodological discussion explaining the combination of expert interviews and Q-methodology used to capture both professional assessments and citizen perspectives. The subsequent sections present the analysis, identifying discourses of trust and distrust, and examining how they are embedded in broader institutional and sociotechnical contexts. The final section discusses the implications of these findings for democratic theory and electoral practice, emphasising the conditions under which internet voting can be perceived as legitimate and trustworthy.

Literature review

Technological innovation has permeated nearly every aspect of contemporary society, and democratic elections are no exception. Over the past decade, significant attention has been devoted to understanding how digital technologies are employed to shape and influence voter behaviour (Campante et al., 2018), especially following the Facebook/Cambridge Analytica scandal (Heawood, 2018), which revealed the extent to which personal data could be harvested and strategically deployed in political campaigns. Since then, terms such as fake news (Allcott & Gentzkow, 2017; Lazer et al., 2018), misinformation, and disinformation (Jerit & Zhao, 2020; Shu et al., 2020) have become part of the usual political vocabulary,

intensifying their presence during electoral processes. Far from being confined to isolated cases, these phenomena have manifested globally, with documented instances across diverse political systems and cultural contexts (Echeverría et al., 2024; Erlich & Garner, 2023; Lee, 2019; Pierri et al., 2020).

A common thread behind these examples is the central role of digital technologies in enabling, amplifying, or accelerating their impact (Morgan, 2018). This dynamic has not only altered political competition but also generated a generalised concern about the resilience of democratic institutions in the digital age, leading to a broader crisis of trust (Bodó, 2021), as traditional institutional and interpersonal logics were not prepared to deal with these phenomena.

Digital technologies have also been increasingly integrated into election management. For several years, public administrations have explored technological solutions to improve the efficiency, security, and overall manageability of electoral processes (Krimmer, 2012). Innovations such as ballot scanners, electronic voter lists, and other digital tools have emerged, but the innovation that has received the greatest scholarly attention is the use of electronic means for casting ballots. Electronic voting can be broadly divided into two categories: the use of voting machines in traditional polling stations, known as Direct Recording Electronic (DRE) systems, and digitally enabled remote voting systems, commonly referred to as internet voting. This paper focuses on the second, which generated high expectations in the early 2000s due to its expected potential to streamline the voting process and fight against declining voter turnout (Alvarez & Hall, 2004), although, over time, many of these expectations have not been fully realised, and the widespread adoption of internet voting has lagged behind initial projections. While multiple factors help explain this outcome (Licht et al., 2021), trust-related issues remain central to understanding both the slow adoption and the mixed results of internet voting initiatives (Carter & Campbell, 2011; Mahrer & Krimmer, 2005; Volkamer et al., 2011).

Applied research on internet voting from a social science perspective can generally be divided into two main strands, depending on the focus of inquiry. The first strand concentrates on future-oriented projections, examining voters' intentions to use internet voting in countries where the technology has not yet been deployed (Musial-Karg, 2017; Nemeslaki et al., 2016), assessing potential impacts of its adoption (Carter & Bélanger, 2012; Krimmer et al., 2019), or analysing outcomes from pilot studies (Council of Europe, 2010; Hoxha et al., 2024; Turnbull-Dugarte & Devine, 2023). The second strand focuses on analyses of actual implementation in countries where internet voting is or has been in use. Given the limited number

of such cases, the literature has largely concentrated on Switzerland (Germann & Serdült, 2017; Serdült et al., 2015; Serdült & Kryssanov, 2018), Canada (N. Goodman, Gabel, et al., 2018; N. Goodman, McGregor, et al., 2018; N. J. Goodman, 2014; N. Goodman & Smith, 2017), and Estonia (Krimmer, Volkamer, et al., 2021; Madise & Vinkel, 2014; Toots et al., 2016). Research conducted in these three contexts has been particularly influential in recalibrating initial expectations against empirical realities. Findings show, for example, that while voters who adopt internet voting rarely return to other voting methods (Solvak & Vassil, 2018) and that it can be more cost-efficient than traditional channels (Krimmer et al., 2021), turnout increases tend to be confined to specific groups (Germann, 2021; Germann & Serdült, 2017). Moreover, integrating internet voting requires significant institutional and procedural adaptations to ensure alignment with existing voting systems (Krivonosova, 2022). In both cases, trust appears to be a central element, given the wide attention it received by research, either in the past (Carter & Campbell, 2011; Spycher et al., 2011; Warkentin et al., 2018) and recently (Abdala et al., 2025; Ehin & Solvak, 2021; Romanov et al., 2025; Sindermann et al., 2023).

A compelling case can be made for selecting Estonia when studying trust in internet voting. We argue that reliable insights into how citizens evaluate such systems can be gained only in countries where internet voting has been implemented and widely used, rather than in those where it remains hypothetical. Estonia is unique in this respect: it became the first country to introduce legally binding internet voting in national elections in 2005, and by the 2023 parliamentary elections, more than half of the electorate cast their ballots online (N. Goodman & Pyman, 2016; Heiberg et al., 2020; Solvak et al., 2019; Vassil et al., 2016). This long-term, large-scale use provides citizens with direct, experience-based knowledge of the system, allowing researchers to move beyond naïve expectations or speculative concerns that dominate debates in countries without such experience (Alvarez et al., 2009; Krimmer et al., 2019). In short, the Estonian case offers a uniquely robust empirical ground for studying the dynamics of trust, as voters have had sufficient opportunities to form reflections grounded in practice rather than mere anticipation.

Trust has long been recognised as a cornerstone of social interaction, cooperation, and institutional legitimacy (McKnight & Chervany, 1996), yet it remains a multifaceted and difficult-to-pin-down concept (Hupcey et al., 2001). At its most basic, trust can be understood as the willingness to accept vulnerability in the face of risk, sustained by positive expectations about another party's behaviour (Marsh & Dibben, 2005; Murnighan et al., 2004). However, such a definition is insufficient to capture the complexity of trust in contemporary digital democracies (Duenas-Cid

& Calzati, 2023). Scholars have emphasised that trust is at once an individual property and a relational construct. On one hand, it reflects personal beliefs and perceptions (Mooradian et al., 2006; Murnighan et al., 2004); on the other, it projects these beliefs outward, taking shape in interactions between actors (Möllering, 2001; Simmel, 1964). As a result, different forms of trust can be considered depending on the type of actor involved: interpersonal trust (between individuals), group trust (among collectives), institutional trust (between individuals and institutions), organisational trust (across organisations), and technological trust (between individuals and technological systems) (Hardin, 2002; Simon, 2020).

This interactive nature of trust underpins its role as a necessary element of human cooperation, civic life (Putnam, 2001), and economic exchange (Fukuyama, 1995). Trust reduces the complexity of human interaction (by relying on known actors) and helps manage uncertainty (by focusing on identifiable risks rather than diffuse ambiguities) (Luhmann, 1979), operating simultaneously as a social lubricant and a mechanism of simplification, enabling individuals to act in the face of unknowns.

Yet when applied to technology, trust reveals additional layers of complexity (Bodó, 2021; Bodó et al., 2025). Research has examined trust as a dispositional attitude guiding technological adoption (Evans & Krueger, 2009), as a communitarian product of perceived political efficacy (Anderson, 2010), as a legal safeguard embedded in governance frameworks (Werbach, 2018), or as a reaction to the “humanness” of human–computer interaction (Ciechanowski et al., 2019; Lankton et al., 2015). Despite this breadth, many approaches continue to treat trust as a binary construct explained by a handful of variables, rendering it an ambivalent concept that can be invoked either as a prerequisite for adoption (Janssen et al., 2018) or as its outcome (Lippert & Davis, 2006). This conceptual ambiguity is further reinforced by the frequent overlap between trust and neighbouring constructs, such as confidence and trustworthiness, which are often used interchangeably even though they refer to distinct aspects of social and technological relationships. Trustworthiness denotes the perceived characteristics of the trustee that signal competence, integrity, or benevolence (Levi & Stoker, 2000). By contrast, confidence refers to the trustor’s expectation or certainty that events will unfold as anticipated, grounded in prior knowledge, experience, or institutional routines (Giddens, 1991). The coexistence of these adjacent concepts blurs the concept of trust, complicating efforts to define its boundaries and identify its explanatory role in digital governance and technology adoption.

Building on this critique, Duenas-Cid & Calzati (2023) emphasise the mediated and asymmetric nature of trust and distrust. Trust is not simply an attribute of indi-

viduals or institutions but a relational property that emerges through knowledge asymmetries, expert mediation, and processes of familiarisation. It operates as both a bridge between ignorance and expertise and as a mechanism for transforming uncertainty into specific, navigable risks. In digital contexts, this mediation becomes sociotechnical: trust is not merely “in” technology but also “through” technology, shaped by interfaces, institutional embedding, and broader legitimacy structures. When applied to internet voting, this suggests that trust cannot be reduced to confidence in technical functionality alone. Instead, it involves overlapping forms, such as technological trust in system reliability, institutional trust in electoral authorities, organisational trust in system operators, and group trust in peer adoption patterns. All of them converge in shaping whether citizens accept or resist digitalised electoral participation.

Distrust, on the other hand, is understood in Duenas-Cid and Calzati’s (2023) framework as an asymmetrical opposite of trust: although they clearly occupy opposite ends of a common spectrum, they operate in different ways (Luhmann, 1979; Six & Latusek, 2023). Distrust may even play a constructive role, contributing indirectly to the creation of trust (Duenas-Cid, 2024; Duenas-Cid & Misev, 2024). As Sztompka (2003) notes, a “healthy balance” of trust and distrust is necessary for modern societies: excessive trust risks fragility and disempowerment, while excessive distrust corrodes legitimacy.

Within democratic systems, measured distrust should not necessarily be understood as a dysfunctional or undesirable phenomenon. Democratic institutions frequently incorporate mechanisms of oversight, monitoring, and accountability that reflect the productive role of citizen scrutiny toward public authorities (Rosanvalon & Goldhammer, 2008). Applied to internet voting, this means that distrust should not be dismissed as mere resistance or conservatism. Instead, it may contribute to demands for transparency, verifiability, and institutional safeguards. At the same time, distrust is not inherently beneficial. Excessive distrust may undermine institutional legitimacy and reduce citizens’ willingness to engage with public institutions and technological innovations, as demonstrated by the cases of electronic voting in Norway (Jordi et al., n.d.; Markussen et al., 2014) and the Netherlands (Duenas-Cid, 2024). Recent governance research further suggests that trust and distrust may coexist rather than function as simple opposites, shaping different forms of engagement with public systems (Verhoest et al., n.d.). Consequently, the democratic value of distrust lies not in its mere existence but in maintaining a balance between critical scrutiny and sufficient confidence to enable participation and institutional innovation.

The application of this framework to the analysis of internet voting allows for a construction of a complex approach to the understanding of internet voting, creating four ideal typologies encompassing the elements included in Duenas-Cid and Calzati's framework: 'trust in-', 'distrust in-', 'trust through-' and 'distrust through' internet voting. Based on this framework, we hypothesise that the four ideal types of dis/trust will be present in the outcomes of the Q-Methodology experiment.

TABLE 1. Typology of trust and distrust in internet voting based on the Duenas-Cid and Calzati (2023) framework.¹

Trust in Including technical and institutional elements that allow reliance on the system	Distrust in Including technical limitations (opacity, risks, etc.) and fear of manipulation
Trust through Including the potential for the improvement of democracy and trust transference from other institutional setups	Distrust through Including fear of the erosion of democracy and the need for accountability of the government.

Methods

This study employs a mixed-method design combining expert interviews and Q-methodology to examine how trust and distrust in internet voting are articulated in Estonia. The two approaches complement each other: expert interviews capture professional and institutional perspectives, while Q-methodology identifies shared viewpoints among citizens. Together, they provide an integrated understanding of how trust discourses are shaped by both policy actors and the public.

Expert interviews

Sixteen semi-structured interviews were conducted between December 2022 and April 2023 with stakeholders involved in the development, monitoring, and public discussion of internet voting, including electoral officials, journalists, and technology providers². For more information on profiles, see Appendix B. Participants were selected purposively to represent diverse professional backgrounds. Interviews lasted approximately 55 minutes and focused on themes such as system security, transparency, and public confidence. Conversations were recorded with consent, transcribed verbatim via Otter.ai, and thematically coded to extract recurrent

1. While this typology guided Q-sample construction and initial coding, the empirical analysis (see Results, Discourses 1–2, and Discussion) found that citizen trust differentiates primarily along a habitual-vs-conditional basis within the trust in category, rather than splitting cleanly between Trust in and Trust through as hypothesised. Distrust, by contrast, showed no equivalent internal differentiation between Distrust in and Distrust through. See Discussion for full treatment.

2. The authors will provide the interview questionnaire upon the request.

statements about trust and distrust that informed the subsequent Q-sample construction.

Given that several interviewees were directly involved in the administration or public communication of internet voting, their perspectives may reflect institutional positions and professional commitments to the system. To mitigate this, participants were selected from diverse professional backgrounds, including journalists, technical specialists, and external observers involved in public debates surrounding internet voting. Nevertheless, the expert interviews should not be understood as neutral representations of all possible perspectives, but rather as institutional and professional framings through which trust and distrust in internet voting are articulated in Estonia.

Q-Methodology

To identify and analyse subjective viewpoints on trust in internet voting among a broader group of participants, we have employed on-site, in-person Q-methodological discourse analysis (Ramlo & Newman, 2011). This method allows us to evaluate the positions on the statement, extracted from expert interviews, regarding the factors of trust and distrust in internet voting. Adhering to the principles of Q-methodology (McKeown & Thomas, 2013; Watts & Stenner, 2012), this method integrates statistical analysis to identify factors and qualitative techniques to interpret patterns of subjective viewpoints on data. Unlike traditional quantitative factor analysis (Fabrigar et al., 2012) or purely qualitative discourse analysis (Schiffrin et al., 2008), Q-methodology identifies discourses through correlations among statements and groupings of individuals who agree with them.

To simplify the sorting process for participants, we have prepared a template. The template on which the respondents distributed the statements reflected the agreement scale, where -4 indicated complete agreement, +4 complete disagreement, and 0 indicated indifference and neutrality; see Figure 1 for an example. To allow participants to express their subjective positions freely, the 0-point scale was used as a neutral option rather than compelling them to select a position on a strictly symmetrical scale.

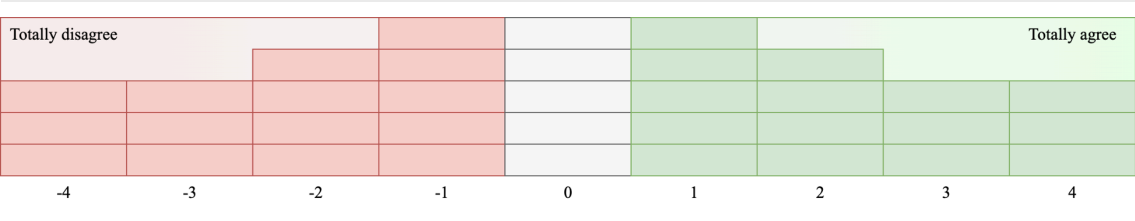


FIGURE 1: The symmetrical Q-methodology template was used to Q-sort 36 statements.

Q and R samples

According to the “manual” of Q-methodology (Watts & Stenner, 2012), we ensured that the number of statements exceeded the number of respondents in order to provide sufficient discursive diversity and avoid overly constraining the sorting process. In other words, our Q-sample comprised 36 claims about internet voting. The construction of the Q-sample was informed by the themes identified in the expert interviews. To form the Q-sample, we transcribed all 16 expert interviews, which yielded a range of statements and factors that might shape citizens’ trust or distrust in internet voting. However, the statements themselves were not direct reproductions of expert arguments, but rather derivatives of broader topics and recurring discussions surrounding internet voting. While themes such as transparency, institutional trust, and security risks were present in the interviews, they did not constitute the only dimensions included in the statement set. The final Q-sample intentionally incorporated heterogeneous and competing claims related to technological reliability, accessibility, political legitimacy, convenience, democratic participation, and institutional accountability. In line with Q-methodology, the statements defined the discursive space within which participants positioned themselves, while still allowing for the emergence of contrasting and internally differentiated viewpoints, which is why the additional post-assignment interviews were conducted. The complete list of statements is provided in Appendix C.

The pool of respondents included 26 English-speaking Estonian participants. In line with the principles of Q-methodology, the aim of respondent selection was not statistical representativeness, but the identification of shared viewpoints and discourse patterns across participants. Recruitment was delegated to the Norstat survey company based on two predefined criteria: firstly, participants had to be able to communicate in English in order to conduct the post-Q-sorting interviews regarding the reasoning behind the statement distribution with researchers in English; and secondly, the sample was designed to consist equally of participants who had previously used internet voting in Estonia and those who had not. The distinction referred specifically to prior use of internet voting and did not differen-

tiate between citizens who abstained from voting entirely and those who voted through alternative channels. Although the English proficiency requirement may have introduced a bias toward more internationally oriented or digitally confident respondents, the final sample still reflected a relatively broad age distribution, ranging from 22 to 67 years old. Beyond demographic characteristics and prior exposure to internet voting, no additional socioeconomic or recruitment-channel-level information was collected, which limits the ability to further contextualise the respondent pool. Nevertheless, the sample was considered sufficient for factor extraction and discourse interpretation while still allowing for diversity in attitudes and experiences related to internet voting. A detailed overview of the sample's demographic composition, including age, gender, prior exposure to internet voting, and alignment with the discourse, is provided in Appendix A.

To explore the subjective perceptions of the participants further, we have, first of all, introduced them to the overall idea of the project by also explaining the source from where statements originated; secondly, we involved the participants in the Q-sort process, within which they were expected to allocate the 36 statements across the template. Lastly, by asking the respondent to elaborate on their position on the Q-sorting result, why exactly was the statement placed in this category? The extremums were of the most interest; those would be columns +4, +3, -3, and -4, along with the statements attributed to these categories.

The Q-methodology was conducted with a slight delay, following the interviews in June 2023, due to the recruitment process. This delay allowed us to capture the Estonian parliamentary elections in March 2023, an experience the respondents could use as a vivid reference point.

Following Duenas-Cid and Calzati's (2023) typology, trust and distrust were treated not as unitary constructs but as composites of four analytically distinct orientations, which guided both Q-sample construction and post-hoc interpretation of factors:

1. **'Trust in'** internet voting was operationalised as agreement with statements referring to the technical reliability of the system, the competence of the institutions and personnel administering it, or confidence grounded in habitual, personal use – independent of any claim about the system's broader democratic consequences.
2. **'Distrust in'** internet voting was operationalised as agreement with statements referring to technical opacity, vulnerability to error or manipulation, or scepticism toward the competence or intentions of those operating the system.

3. **'Trust through'** internet voting was operationalised as agreement with statements linking the system to downstream democratic goods, participation, accessibility, institutional legitimacy, or political modernisation, regardless of the respondent's confidence in the underlying technology.
4. **'Distrust through'** internet voting was operationalised as agreement with statements expressing concern about the erosion of democratic accountability, the concentration of institutional power, or the weakening of electoral legitimacy as a consequence of digitalisation.

Each of the 36 statements comprising the Q-sample was classified against this fourfold scheme during sample construction, based on its dominant thematic orientation as derived from the expert interviews (see Appendix C for the full statement set and classification). This a priori classification allows for further reflection. First, the distribution between trust and distrust is balanced (20 trust statements, 16 distrust), but not in relation to in/through (26 in -12 through- the number exceeds 36, as a result of some statements combining both discourses). This bias stems from the previous interviews and the need to respect the arguments collected rather than forcing them to find a better balance between approaches. Second, it provided an analytic anchor for the qualitative interpretation of the three extracted factors: for each factor, we examined the distribution of its defining and distinguishing statements (Watts & Stenner, 2012) across the fourfold scheme, allowing us to assess the degree to which a given discourse aligned with a single ideal type or combined elements across categories. Discrepancies between the four-type classification of statements and the three-factor empirical solution, most notably the tendency of distrust-related statements to load together across the in and through categories, are addressed directly in the Results and Discussion as a substantive finding rather than as a methodological shortfall.

Factor analysis

After the onsite activity, the data were subjected to factor analysis to identify common patterns in participants' rankings. This analysis helped reveal shared viewpoints and distinguish between trust and distrust profiles based on their rankings of statements. In this research, we used KenQ software (Banasick, 2023), a specialised tool for Q-methodology, to perform the statistical analysis, including factor extraction and rotation.

The varimax rotation method was chosen for its ability to produce orthogonal (uncorrelated) factors. This approach is particularly effective in simplifying the data structure, as it maximises the variance explained by each factor. Varimax rotation ensures that statements load strongly on a single factor while minimising cross-

loadings on other factors, making it easier to assign participants to distinct discourses. This clarity is essential for studies like ours, which aim to delineate independent thought clusters and provide a structured understanding of diverse viewpoints. Unlike non-orthogonal rotation methods, such as centroid rotation, which are suited for exploring interconnected or overlapping perspectives, varimax rotation was selected to emphasise the independence of the identified factors. This decision ensured that the results provided a precise, interpretable distinction among the various discourses present in the data.

Finally, the factors identified through statistical analysis were interpreted qualitatively. The factors were constructed based on the manual thematic analysis, in which we identified factors using the received factor loadings and scores, the formulation of the statements, and the respondents' sorting justification. The respondents' backgrounds were also taken into account, particularly their prior experience with internet voting, or lack thereof.

Analysis results

The section in question is dedicated to the interpretation of the extracted discourses within the Q-methodology. Three factors were extracted from the analysis to explain the sources of trust and distrust in political technology and internet voting. The selection of three factors was based on two complementary criteria: the distribution of eigenvalues and the qualitative interpretability of the extracted discourses. As shown in Figure 2, the scree plot demonstrates a clear “elbow” after the third factor, indicating diminishing explanatory contribution from additional factors. Beyond this point, the extracted factors became less theoretically coherent and interpretively meaningful. Consequently, the three-factor solution was considered the most analytically robust and substantively interpretable configuration (see Table A1 in the Appendix).

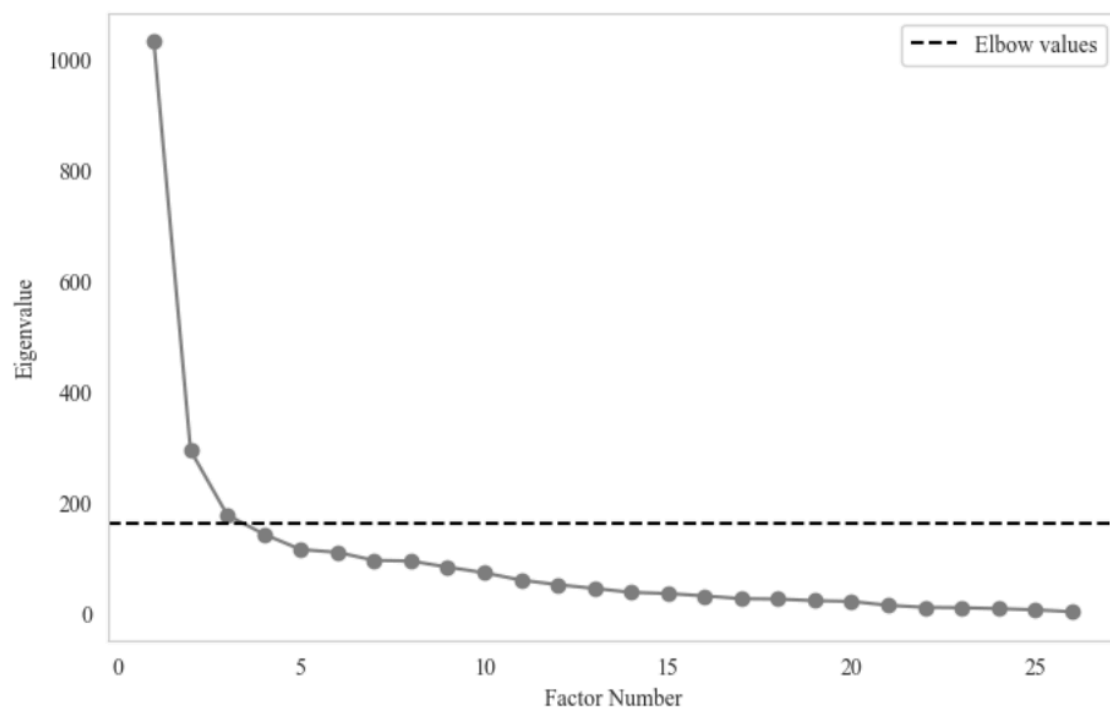


FIGURE 2: Scree plot (elbow method) used to determine the optimal number of factors for extraction based on eigenvalue distribution.

Further in the section, we analyse the factor scores of the statements attributed to each factor and provide an interpretation of the discourse on trust and distrust in internet voting. Still, the number of factors obtained (three) does not match the number of hypotheses previously detailed, opening the door to recalibrating them by discussing whether the different hypothetical distinctions between trust and distrust, or between in or through the system, are present in the discourses obtained. As the analysis demonstrates, the identified discourses do not map directly onto the four ideal-typical categories. Instead, several discourses combine elements of 'trust in/through' and 'distrust in/through' internet voting across both technical and political dimensions.

Discourse 1: Practical and pragmatic trust

This discourse expresses trust in internet voting as a functional and reliable extension of Estonia's digital state infrastructure. Participants aligned with this factor demonstrate a pragmatic optimism toward internet voting, rooted in their personal experiences, everyday digital practices, and a generally high level of institutional trust. While acknowledging potential risks, they emphasise that the system's consistent performance and integration into daily life outweigh concerns.

A defining element of this discourse is the emphasis on convenience, which is not

only viewed as a practical benefit but also as a facilitator of democratic participation. As one participant succinctly explained: *“It [internet voting] is more convenient, and I know a lot of people, so from personal experience, who see that it’s easier to vote online: first of all, you have a week where you can vote, and you can do it from everywhere.”* (P7).

“You can do it anywhere. It is not time or location specific... so it is more convenient” (P22).

Convenience is not abstract but grounded in personal experiences (related to the system’s spatial and temporal flexibility), observed behaviours, and peers’ lived experiences. Personal and social validation seem to reinforce perceptions of system reliability, while the ability to vote without logistical constraints makes internet voting appear more inclusive and efficient, especially to mobile or busy citizens.

For many, the shift to internet voting was part of a broader digital transition and reinforced by habit and cultural norms: *“It’s like doing bank transfers. They are regular. In most ways”* (P4).

“The more you do it, the more trust is generated, it’s how it works” (P7).

“We can do our declarations, taxes via the internet. I [was doing] them only on paper and it was painful. [Now] it’s very comfortable, and I can add something if I need, I can take it off if it isn’t anymore. So I can check all my data, all my real estate, my car, or something else with these systems.” (P26).

The habit of using digital technologies in other societal fields or in relation to Estonian e-government systems generates familiarity and trust. As digital practices become habitual, scepticism fades, and internet voting becomes a seamless extension of the e-governance experience. Institutional integration and consistent performance in other digital services feed into the legitimacy of internet voting. Trust in the broader e-state strengthens trust in its electoral tools.

Institutional trust underpins this pragmatic support. Respondents often referred to the reliability of public institutions and civil servants: *“I just say that I believe in the system that everybody [people who organised the whole election and people who provide the election platform] who’s doing their part knows what they are doing.”* (P23).

“People are using electronic banking and some other electronic services, so they definitely trust others as well. So it’s like a positive influence.” (P22).

The obtained responses reflect a belief in the competence and good intentions of election officials and civil servants. Discourses of trust are based not only on abstract design system principles but also on the presumed integrity of the people who run the system or on wider political infrastructures of trust. Internet voting is not viewed in isolation but as part of a larger trust network tied to public administration and governance, and affected by the spillover effect from political trust to technological trust, and vice versa.

Importantly, this trust is not blind. It is contingent on the system working well over time: *“It’s just with anything new, you start to question at first, but later, and then when you see that it works, and it works fine, then these kinds of fears go away, and people are more and more using these tools.” (P19)*

“...The new generation who grows up with that and they will already know that the system is working, the system has not failed, and they will go on with the [internet voting].” (P7).

The durability of trust is framed as a consequence of the system’s track record. Continued success reinforces public confidence, suggesting a rational, experience-based evaluation, both of which echo the habitual nature of trust in internet voting, supported by trust in technology itself and associated political institutions. The hypothetical scenario of a system failure is also framed similarly: *“If the system fails, it will manipulate the trust factor for a few elections... but if they are working on a global amount and communicating that they have resolved the issues, then the trust will come back” (P7).*

Even as they acknowledge the potential for failure, transparency and responsiveness from political institutions are seen as key to rebuilding trust. The expectation is not infallibility, but rather responsible management and the technology’s consequential trustworthiness. The regular use of internet voting, hence, appears not only as a trust-maintaining mechanism but also as a trust-building mechanism.

Interestingly, the presence of a fallback option (i.e., paper voting) also reinforced trust. Several respondents mentioned that having alternatives contributed to their overall feeling of security: *“I think any voting cannot be 100% safe, so we have to ac-*

cept risk (...) but if internet voting is closed, I don't see any other reason... I should go back [to paper]" (P7). Knowing there is a backup plan makes people more comfortable with choosing the digital option, even if they do not plan to use the alternative. Differently, other trust-related elements are linked to the specific and unique properties of internet voting: *"The possibility to cancel things... we need to accept the risk anyway in organic processes"* (P22). In this case, trust connects with the broader philosophy of system design and public administration, acknowledging uncertainty, but relying on institutional adaptability and safeguards to manage it.

In accordance with the previous, the increasing usage of internet voting is not seen as a potentially dangerous scenario: *"Why should we vote on paper? I don't think it's a concern at all [the hypothetical scenario that more and more people are voting via the internet]"* (P26). The widespread use of internet voting, rather than being seen as a threat, is perceived as evidence of widespread approval and system maturity aligned with the general digitalisation of the country: *"I think we are evolving and going forward. Internet voting is going to be that way"* (P15).

This future-oriented stance reinforces the idea that internet voting is not just a present convenience, but a cornerstone of Estonia's political modernisation, as reflected by the response from P11 (who has the highest association with the institutional trust narrative): *"I think their [political actors] agenda is just to get more people to use the platform. And I think it helps them if they're being transparent about it, to build trust and get people to join them."*

In summary, this discourse reveals a form of technological trust anchored in institutional performance, collective habit, and consistent personal experiences. Trust is not rooted in the technicalities of cryptographic verification or system architecture, but rather in the reliability of Estonia's e-governance technology, institutional continuity, and everyday usability. This group perceives internet voting not as a radical innovation, but as a natural and dependable element of modern life in Estonia.

Discourse 2: Conditional trust and demands for verification

This discourse reflects a set of perspectives where participants engage critically with internet voting not as a technological failure, but as a system whose trustworthiness depends on visible safeguards, institutional transparency, and accessible communication. Unlike Discourse 1, where trust is grounded in habitual use and an accumulated, largely unquestioned track record, this discourse conditions trust on the availability of mechanisms that make the system's workings checkable

– audits, training, technical readiness, and clear communication when problems arise. Participants in this discourse do not reject the premise of trusting the system; rather, they resist the idea that trust should be extended on faith or as an acceptance of unavoidable risk. This distinction was directly visible in the composite Q-sort for this factor, which combined strong endorsement of statements affirming institutional competence, external audit, and cyberattack readiness, with a pointed rejection of the claim that “internet voting cannot be 100% secure and we need to accept the risk” – the single most distinguishing statement for this discourse. Where Discourse 1 accepts residual risk as the price of convenience, Discourse 2 treats blanket risk-acceptance as an insufficient basis for trust, demanding instead that trust be earned through demonstrable, checkable safeguards.

Trust in internet voting appears as the result of clarity, accountability, and public engagement: *“It could be better because right now we are discussing the parties who have their opinions, we discuss those opinions, but we don’t discuss the problem in depth. So I think that’s the problem. So it could be better... especially in journalism”* (P21). The political and partisan dominance of the discourse around internet voting hinders the possibility of a wider, informed, and balanced discussion with the citizenry.

Participants also raised concerns that transparency should extend beyond functional efficiency to include institutional communication and procedural accessibility: *“Here, I think compared with COVID, for me, when I made my first vaccination, I think I had enough information, and with the voting system, I still think that it should be really open and show everything. Because if they said that voting has some problem, okay, we have a problem, then they should fix it.”* (P24)

Some participants highlight a gap in public accessibility, not in terms of technical access, but in terms of confidence and clarity for all demographics: *“I think at the moment, not too many people [are] voting online, but there must be more. A lot of [people] don’t trust the system, especially the old people”* (P14). This gap is also reflected in the tension between the system’s usability and its understanding. P16 expressed, *“I know my parents are using internet voting,”* and later, when asked about the option to verify the vote, *“I didn’t think about it. I thought they gave a vote, so everything is okay with it”* (P16). This suggests a form of procedural opacity: even when the system appears functional and is widely used, it may not be fully understood, even by those who participate in it. The same participant further commented that *“I think [internet voting] is a piece of cake,”* but expressed a belief that *“Media is media. How much is the truth? It’s another case”* (P16), indicating some scepticism toward the information environment surrounding internet voting.

The value of public debate emerged as a contested point among participants in this discourse. P24 offers a sceptical reflection on its effectiveness in practice: *“But debate, there is always debate before elections. And it hasn't given any result”* (P24), pointing at the disillusionment with performative or cyclical discussions that fail to lead to meaningful change. Institutional trust goes beyond the existence of debates, but whether its outcomes are taken seriously and result in visible improvements or policy responsiveness. Thus, while this discourse broadly values transparency and dialogue, it also points to the limits of symbolic engagement and the need for debate to translate into tangible institutional accountability.

Concerns over inclusivity and access were also present in reflections on technical outreach and awareness, highlighting the lack of public knowledge of election observation workshops: *“I haven't heard about it at all... I do trust the elections, but I haven't heard about it. So imagine what older people feel or other people who are maybe a bit less educated”* (P21). This suggests a disconnection between institutional offerings and public awareness, indicating that even well-functioning systems may fall short if their operations are not clearly and widely communicated. (Kattel & Mergel, 2019; Leppiman et al., 2021)

Trust, while relying on many different sources, does not necessarily stem from the informed understanding of the system: *“It's easy. And I trust the internet voting. I don't know why, but I trust it”* (P9). The relation between trust and practice, already highlighted in previous research (Solvak & Vassil, 2018), also appears as an important element in the real capacity to understand the functioning of the system.

Overall, this discourse highlights the importance of effective communication, inclusivity, and institutional transparency, but its underlying logic remains a form of trust in the system – a conditional variant, resting on the visibility and verifiability of technical and institutional safeguards, rather than on habituation or accumulated experience alone. Trust, in this discourse, is contingent before it is automatic: it is extended to the extent that institutions demonstrate competence and communicate openly, not merely because the system has not yet failed. While participants voice clear concerns about accessibility and public understanding, these concerns function as conditions attached to trust rather than as a rejection of it, distinguishing this discourse from the more thoroughgoing scepticism articulated in Discourse 3.

Discourse 3: Scepticism about security and human vulnerabilities

The third and final discourse takes all concerns pinpointed in the second narrative

and pushes them to their extremes. Participants consistently emphasise the system's vulnerability to both technical and human error, the potential for manipulation, and the need to maintain or develop credible alternatives. For them, trust in internet voting cannot be separated from the recognition that all systems, especially those handling sensitive political processes, carry inherent risks that must be transparently acknowledged and actively mitigated.

Participants in this discourse adopt what might be called a limited distrust. They view the digital infrastructure of voting as complex and potentially opaque, and their concerns often stem from a lack of transparency or understanding of how the system operates. P10, for instance, describes that he does not trust the technology he utilises for the internet voting, such as a mobile phone for the voting verification: *"I don't really know what is going on inside my phone... it feels like it's safe, but I cannot detect if someone is using my phone or something"* (P10). This feeling is shared by other respondents in this group, distinguishing between the creation of trust in digital systems and their actual understanding or verifiability.

Distrust is also pointed towards institutions due to the concentration of control in the hands of a small number of technical and institutional actors. P1 highlights this tension explicitly, noting that *"there was a scandal where somebody gathered the ID cards of all the elderly people and just cast the vote"* (P1, P10³, P20⁴) – a case that pointed to both social vulnerability and the potential for system misuse and voter coercion. For P1, trust in the voting system was eroded not only by such incidents but also by the perceived general lack of response from authorities to public concerns. It is a reflection that *"the communication regarding [internet voting] has been very poor"* (P1), which underscores the idea that risk is amplified when it is not openly discussed. The embedded problem of internet voting with the digital identification card and "identity theft" was repeated by P18: *"However, with electronic voting, it becomes more of an issue because you know, as I mentioned previously, is that you cannot verify with 100% confidence that it is indeed the owner of the ID card that is voting."* (P18)

Institutional distrust was further supported by P18, who projected his distrust in the Election Management Body, when asked about the concentration of power and

3. *"Yes, again, this is because we have a problem with this, when there was a news also about it in some where they put the old people in the residence or something all together, and then they have access of their ID cards there."* (P10)
4. *"I don't, I don't believe that. If we see that political, government people on so one, they are sitting and also very many people are voting via internet, as in the passionate and old people houses. And usually all their ID cards are used."* (P20)

election result manipulation: *“It’s quite a small group and based in Tallinn, and a big argument against electronic voting is the fact that if you wanted to manipulate, then, as opposed to paper voting, where you need a very big group of people to manipulate elections in a meaningful way. In this case, electronic voting, the sort of circle of people that you would need to convince or buy out or, you know, swearing to silence that is much smaller”* (P18). This perspective reflects a broader anxiety not primarily about the technology itself, but about the trustworthiness of the small number of people who operate and control it – whether they can be convinced, bought, or silenced. This concern echoes a wider pattern in research on trust and digitalisation in Estonia: Männiste and Masso (2018) find that Estonians’ privacy concerns are shaped less by perceptions of technology as such than by trust in the institutions and individuals who administer digital systems, with those who feel institutions have overstepped reporting systematically lower institutional trust. Similarly, Hardy (2024), examining Estonia’s cross-border e-governance infrastructure (X-Road), argues that the central challenges of scaling such systems are not technical but concern control, sovereignty, and who holds authority over shared infrastructure. P18’s concern is best understood not as a claim about centralised architecture creating vulnerability in the abstract, but as a claim about the limited number of people who must be trusted to resist manipulation – a distinctly human, rather than purely structural, form of institutional distrust. Also, the participant draws a contrast between the distributed nature of traditional voting, which relies on many actors across multiple locations, and the perceived consolidation of central control in internet voting. By invoking the image of a small, closed group operating from Tallinn, P18 implies that the conditions for manipulation are not only technically feasible but also institutionally plausible, given a lack of oversight and transparency. This concern situates the discussion of trust in what might be classified as a political domain, where the issue is not just whether the system works, but who controls it and how resistant it is to fraudulent influence.

This critical perspective was deepened by P10, who further questioned the opacity surrounding the actors behind the voting technology: *“Because we as Estonians, I mean, maybe somebody does, but at least as a citizen level or just a normal person, we don’t know too much about these companies that are making these programs, and who are the people behind it? And are they hired by who, I guess, has done in government, but at which level? Who pulls the strings, we don’t know that?”* (P10). This reflection highlights a gap between trust and institutional transparency, where the issue extends beyond vulnerability to manipulation to the lack of accessible information about the companies and individuals entrusted with critical electoral functions. Participants’ words emphasise the connection between technological trustworthi-

ness and institutional clarity: without knowing who is responsible, how they are selected, and under what conditions they operate, citizens cannot meaningfully evaluate the integrity of the system. Thus, distrust stems not necessarily from a specific technical flaw, but from the structural invisibility of those in power.

The connection between distrust of political institutions and the internet voting system is further reinforced by concerns about manipulation, with other participants emphasising that, while technological safeguards may exist, no system is immune to failure or corruption. P18 remarks that *“when it comes to voting in elections, I don’t feel we can really completely 100% trust anyone,”* and advocates instead for *“healthy scepticism”* toward institutional authorities. This view is not grounded in rejection of technology, but in an understanding of political systems as inherently fallible and shaped by power relations.

The centrality of human error is echoed by P20, who expresses faith in the convenience and general functioning of the system but concedes, *“Of course [the system] is good, but... after 2005, only one party is always winning [internet voting] elections. It seems a little bit strange”* (P20). While not asserting direct manipulation, such a statement reflects a lingering distrust in patterns that remain insufficiently explained. The limited transparency as a point for distrust was expressed by P1: *“So I think maybe I would trust more [in internet voting], maybe after an independent analysis, we take a group of IT experts and so on who are not connected with [government]. They’re completely independent. They look through technology, and then they give a report of what is actually going on. But that means that if they do find some mistakes and flaws, then the government actually has to act on it.”* (P1) This quote highlights the demand for expert oversight, but especially for independent and external validation of the system’s integrity, indicating a deeper issue of institutional trust rather than technological confidence. Technical reports or evaluations seem insufficient unless they are politically actionable and transparently addressed. Transparency appears, hence, linked to responsiveness, framing trust as contingent not only on audit mechanisms but on whether those mechanisms produce real accountability and reform when issues are uncovered.

Participants also advocate maintaining alternatives to internet voting, both as a safeguard against failure and to accommodate those who do not or cannot engage with digital systems. P1 emphasises the value of traditional paper-based voting, not only for its tangible nature but also for its cultural and civic significance. Others viewed paper voting as a fallback in case of failure or as a necessary means to ensure inclusive participation. While P20 states that he continues to vote online for convenience, he nevertheless emphasises the importance of *“collect[ing] more*

knowledge and studies on the topic,” and adds that he would stop voting online “*if I knew that they are using this central voting system [for] hacking*” (P20).

What unites this discourse is not a frontal opposition to innovation, but an insistence on the side effects of internet voting: human mistakes can arise, and the concentration of control creates vulnerabilities. The refusal to assume infallibility is central to the discourse. In this sense, the perspective diverges from optimism-driven narratives and instead calls for a balanced assessment of both capabilities and limitations. This reinforces the broader analytic insight that while trust in internet voting can be supported by both political and technological assurances, distrust arises largely from the political and institutional context in which the system is embedded. These participants do not question the importance of digital governance, but they challenge the idea that trust can or should be taken for granted. Their stance insists on transparency, contingency planning, and accountability, not as signs of doubt, but as necessary foundations of a resilient democratic process.

Discussions

Applying Duenas-Cid and Calzati's (2023) framework to the Estonian case reveals an important asymmetry, though not the one initially hypothesised. Rather than trust discourses separating cleanly along the in/through axis, the composite Q-sorts show that both trust-oriented discourses (1 and 2) are overwhelmingly anchored in ‘trust in’ internet voting, that is, in confidence in the system's technical reliability and institutional competence, while differing in the basis on which that trust is extended. Discourse 1 reflects a habitual, experience-based form of trust: confidence accumulates through repeated, uneventful use, reinforced by the broader legitimacy of Estonia's e-governance infrastructure, and does not require active verification to be sustained. Discourse 2 reflects a conditional, verification-based form of trust: confidence is extended on the basis of demonstrable safeguards – audits, training, technical readiness, transparent communication and is explicitly withheld from framings that ask citizens to simply accept residual risk. Both discourses, therefore, sit within the ‘trust in’ category as originally defined, differentiated not by whether trust is oriented toward the system itself or toward its downstream democratic consequences (the ‘in/through’ distinction), but by whether that trust is earned through habituation or through verifiability. Elements of Trust through internet voting as a vehicle for democratic legitimacy, participation, or Estonia's international standing, are present in both discourses but occupy a secondary, rather than defining, role.

By contrast, the distrust discourse (Discourse 3) shows no equivalent internal dif-

ferentiation. Its most distinguishing statements combine concerns about technical opacity, human error, and system downtime ('distrust in') with concerns about institutional risk-taking, organised political opposition, and the concentration of power ('distrust through') at the same extreme of the distribution, without separating into distinct sub-discourses the way trust does. This pattern is corroborated by the statement classification underlying the Q-sample itself (Appendix C): among the 36 statements, the only items that resisted assignment to a single ideal type were distrust-oriented or straddled the trust/distrust boundary on the technical dimension; no trust-oriented statement required dual-coding. Taken together, the factor-level and item-level evidence converge on the same conclusion: distrust toward internet voting in Estonia is discursively less differentiated than trust, whether measured in how citizens sort statements or in how the statements themselves were originally articulated by experts.

This revised picture qualifies our initial hypothesis. The four ideal types proposed by Duenas-Cid and Calzati (2023) remain analytically useful for constructing a balanced Q-sample and for identifying which concerns are technical versus political in origin, but they do not map onto citizen discourse as four empirically separable clusters. Instead, our findings suggest a more asymmetric structure: trust differentiates along a basis-of-trust axis (habitual vs. conditional/verification-based), while distrust remains a comparatively undifferentiated fusion of technical and political concerns spanning 'in' and 'through'. This asymmetry, rather than undermining the typology, extends it empirically: it suggests that in a mature internet voting context such as Estonia, trust has had the opportunity to develop multiple, distinguishable rationales, whereas distrust, being the minority, oppositional position, has not undergone the same discursive elaboration.

Conclusions

The implication is that, at least in the Estonian case, discourses of trust in internet voting are differentiated not primarily along the in/through axis originally hypothesised, but along the basis on which trust is extended (i.e., habitual, experience-accumulated trust on one hand, and conditional, verification-dependent trust on the other) with both forms remaining largely anchored in confidence in the system itself ('trust in') rather than in its downstream democratic consequences ('trust through'). Distrust discourses, by contrast, combine technical and political arguments without this internal differentiation, fusing concerns about system opacity with those about institutional accountability into a single, less elaborated register. This does not mean that distrust is absent or irrelevant; rather, it suggests that the

long-term embedding of internet voting within a trusted e-governance infrastructure has generated multiple, distinguishable rationales for trust, while scepticism has not yet crystallised into equally differentiated categories. By contrast, both categories of distrust ('in' and 'through') are in a feedback loop in which the discourses feed each other.

The combined nature of distrust discourses opens the door to further reflection on how distrustful arguments are presented and on their impact on the construction of perceptions of distrust. Some forms of distrust (Sztompka, 1998) or scepticism (Norris & Norris, 2022) focus on improving democracy's functioning by highlighting the weaknesses of existing systems and proposing alternatives. But these discourses often go hand in hand with other forms of distrust whose goal is to erode democracy and fragment society (Butzlaff & Messinger-Zimmer, 2020). As paradoxical as it might seem, distrust discourses might still need to evolve and complexify to distinguish between the two forms of distrust ('in'/'through') and benefit from their positive and necessary outcomes for democracy, without feeding the opposite.

As a final disclaimer, the results of this research do not imply that the system in use in Estonia is trustworthy. This paper reflects citizens' perceptions but does not focus on the system's security properties. As previous research has shown (Duenas-Cid, 2024; Oostveen, 2010), citizens can place trust in untrustworthy systems based on factors that are not necessarily linked to the system's properties (Romanov et al., 2025).

Limitations and further research

While the findings of this study provide insights into how trust and distrust in internet voting are constructed in a democracy with extensive experience with the technology, three methodological limitations should be acknowledged. Firstly, Q-methodology is primarily designed to capture the conceptual relations and subjective structure of individuals' viewpoints, rather than to estimate the actual distribution or status quo within the population. Hence, the discourses identified in the analysis should not be interpreted as representative of all Estonian citizens, but rather as ideal-typical discourses that illustrate the range and internal logic of perspectives in the public sphere.

Secondly, the sample size and composition, while sufficient for Q-methodology and its purposes, limit the generalisability of the findings, particularly due to the language requirement, as participants were English-speaking Estonians. Although

the final sample reflected a relatively broad age range (22–67 years old), the English proficiency requirement may still have favoured respondents who are more internationally oriented, digitally engaged, or comfortable interacting with technological systems. As a result, some perspectives, particularly among less digitally integrated populations or citizens with lower levels of exposure to internationalised environments, may be underrepresented. At the same time, participants were selected to ensure diversity of experience and familiarity with internet voting rather than proportional demographic representation, which is consistent with the interpretive logic of Q-methodology. One vector for follow-up research would be to replicate the same research design with Estonian-speaking researchers and participants to further triangulate and compare the resulting discourses across linguistic and social contexts.

Finally, future research could extend these findings through large-N quantitative or mixed-methods approaches, allowing the discourses identified here to serve as departing hypotheses for studying how widespread these orientations are and under what social, political, and technological conditions they emerge. Such validation would deepen our understanding of how citizens across different contexts adopt, adapt, or contest the narratives of trust and distrust in digital elections.

Acknowledgements

The authors are grateful for the feedback from conference participants during E-Vote ID 2024 in Tarragona, Spain. Additionally, authors express their appreciation to all the interviewees involved in data collection.

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*, 10659129251321424. <https://doi.org/10.1177/10659129251321424>
- Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives*, 31, 211–236. <https://doi.org/10.1257/jep.31.2.211>
- Alvarez, R. M. (2003). *Point, click, and vote*. Rowman & Littlefield Publishers. <https://doi.org/10.5771/9780815796275>
- Alvarez, R. M., Hall, T. E., & Trechsel, A. H. (2009). Internet voting in comparative perspective: The case of Estonia. *PS: Political Science & Politics*, 42(03), 497–505. <https://doi.org/10.1017/S1049096509090787>
- Alvarez, R. M., Katz, G., & Pomares, J. (2011). The impact of new technologies on voter confidence in

- Latin America: Evidence from e-voting experiments in Argentina and Colombia. *Journal of Information Technology & Politics*, 8(2), 199–217. <https://doi.org/10.1080/19331681.2011.559739>
- 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>
- Banasick, S. (2023). *shawnbanasick/ken-q-analysis: Ken-Q analysis version 2.0.0* (Version v2.0.0) [Computer software]. Zenodo. <https://doi.org/10.5281/ZENODO.8310377>
- 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>
- Bodó, B., Bene, M., & Boda, Z. (2025). False sense of security and a flurry of misplaced trust: The construction of trust in and by Facebook. *Information, Communication & Society*. <https://doi.org/10.1080/1369118X.2025.2482651>
- Campante, F., Durante, R., & Sobbrío, F. (2018). Politics 2.0: The multifaceted effect of broadband internet on political participation. *Journal of the European Economic Association*, 16, 1094–1136. <https://doi.org/10.1093/jeea/jvx044>
- Carter, L., & Bélanger, F. (2012). *Internet voting and political participation: An empirical comparison of technological and political factors*. 43(3), 21.
- 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), 28–42. <https://doi.org/10.4067/S0718-18762011000300004>
- Castells, M. (2013). *Communication power* (Second Edition, Second Edition). Oxford University Press.
- 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>
- Council of Europe. (2010). *Electronic voting pilot in the 2008 municipal elections in Finland*.
- Database result (question only). (2025, September 8). International IDEA. <https://www.idea.int/data-tools/data/question>
- 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)*. 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>
- Duenas-Cid, D., & Misev, V. (2024). *Challenging the idea that internet voting verification tools create trust—They serve as distrust mitigation tools*. 109–124. <https://dl.gi.de/handle/20.500.12116/45867>
- Echeverría, M., García Santamaría, S., & Hallin, D. C. (2024). *State-sponsored disinformation around the globe*. Routledge. <https://doi.org/10.4324/9781032632940>
- 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

- Erlich, A., & Garner, C. (2023). Is pro-Kremlin disinformation effective? Evidence from Ukraine. *International Journal of Press/Politics*, 28, 5–28. <https://doi.org/10.1177/19401612211045221>
- 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>
- Fabrigar, L. R., Wegener, D. T., Fabrigar, L. R., & Wegener, D. T. (2012). *Exploratory factor analysis*. Oxford University Press.
- Fukuyama, F. (1995). *Trust: The social virtues and the creation of prosperity*. Free Press.
- Germann, M. (2021). Internet voting increases expatriate voter turnout. *Government Information Quarterly*, 38(2), 101560. <https://doi.org/10.1016/j.giq.2020.101560>
- Germann, M., & Serdült, U. (2017). Internet voting and turnout: Evidence from Switzerland. *Electoral Studies*. <https://doi.org/10.1016/j.electstud.2017.03.001>
- Giddens, A. (1991). *Modernity and self-identity: Self and society in the late modern age*. Stanford University Press.
- Goodman, N., Gabel, C., & Budd, B. (2018). Online voting in Indigenous communities: Lessons from Canada. In R. Krimmer, M. Volkamer, V. Cortier, R. Goré, M. Hapsara, U. Serdült, & D. Duenas-Cid (Eds), *Electronic Voting* (pp. 67–83). Springer.
- Goodman, N. J. (2014). Internet voting in a local election in Canada. In B. Grofman, A. H. Trechsel, & M. Franklin (Eds), *The Internet and Democracy in Global Perspective: Voters, Candidates, Parties, and Social Movements* (pp. 7–24). Springer International Publishing. https://doi.org/10.1007/978-3-319-04352-4_2
- Goodman, N., McGregor, M., Couture, J., & Breux, S. (2018). Another digital divide? Evidence that elimination of paper voting could lead to digital disenfranchisement: Elimination of paper voting in local elections. *Policy & Internet*, 10(2), 164–184. <https://doi.org/10.1002/poi3.168>
- Goodman, N., & Pyman, H. (2016). *Understanding the effects of internet voting on elections: Results from the 2014 Ontario municipal elections*. Centre for e-Democracy, Toronto.
- Hardin, R. (2002). *Trust and trustworthiness*. Russell Sage Foundation.
- Hardy, A. (2024, July 22). *Estonia's digital diplomacy: Nordic interoperability and the challenges of cross-border e-governance* [Info:eu-repo/semantics/article]. Alexander von Humboldt Institute for Internet and Society gGmbH. <https://doi.org/10.14763/2024.3.1785>
- Heawood, J. (2018). Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. *Information Polity*, 23, 429–434. <https://doi.org/10.3233/IP-180009>
- Heiberg, S., Krips, K., & Willemson, J. (2020). Planning the next steps for Estonian internet voting. *Proceedings of the Fifth International Joint Conference on Electronic Voting E-Vote-ID 2020*, 82–97. <https://www.semanticscholar.org/paper/Planning-the-next-steps-for-Estonian-Internet-Heiberg-Krips/9a54275d54de899a31b1804f333f0bb222c600bd>
- Hoxha, E., Josifi, J., & Alimemeti, D. (2024). Electronic voting in Albania—Pilot implementation, insights, and evaluations. *E-Vote-ID 2024 Proceedings*. https://doi.org/10.18420/e-vote-id2024_11
- Hupcey, J. E., Penrod, J., Morse, J. M., & Mitcham, C. (2001). An exploration and advancement of the concept of trust. *Journal of Advanced Nursing*, 36, 282–293. <https://doi.org/10.1046/j.1365-2648.2001.01970.x>

Janssen, M., Rana, Nripendra P., Slade, Emma 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>

Jerit, J., & Zhao, Y. (2020). Political misinformation. *Annual Review of Political Science*, 23, 77–94. <https://doi.org/10.1146/annurev-polisci-050718-032814>

Kattel, R., & Mergel, I. (2019). Estonia's digital transformation: Mission mystique and the hiding hand. In P. 't Hart & M. Compton (Eds), *Great Policy Successes* (p. 0). Oxford University Press. <https://doi.org/10.1093/oso/9780198843719.003.0008>

Krimmer, R. (2012). *The evolution of e-voting: Why voting technology is used and how it affects democracy*. TUT Press.

Krimmer, R., Duenas-Cid, D., & Krivososova, I. (2021). New methodology for calculating cost-efficiency of different ways of voting: Is internet voting cheaper? *Public Money & Management*, 41(1), 17–26. <https://doi.org/10.1080/09540962.2020.1732027>

Krimmer, R., Duenas-cid, D., Krivososova, I., & Serrano, R. A. (2019). *Nordic Pioneers: Facing the first use of internet voting in the Åland Islands (Parliamentary Elections 2019)*.

Krivososova, I. (2022). The forgotten election administrator of internet voting: Lessons from Estonia. *Policy Studies*, 43(6), 1254–1276. <https://doi.org/10.1080/01442872.2021.1958179>

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>

Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S. A., Sunstein, C. R., Thorson, E. A., Watts, D. J., & Zittrain, J. L. (2018). The science of fake news. *Science*, 359, 1094–1096. <https://doi.org/10.1126/science.aao2998>

Lee, T. (2019). The global rise of “fake news” and the threat to democratic elections in the USA. *Public Administration and Policy*, 22, 15–24. <https://doi.org/10.1108/PAP-04-2019-0008>

Leppiman, A., Riivits-Arkonsuo, I., & Pohjola, A. (2021). Old-age digital exclusion as a policy challenge in Estonia and Finland. In K. Walsh, T. Scharf, S. Van Regenmortel, & A. Wanka (Eds), *Social Exclusion in Later Life: Interdisciplinary and Policy Perspectives* (pp. 409–419). Springer International Publishing. https://doi.org/10.1007/978-3-030-51406-8_32

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

Licht, N., Duenas-Cid, D., Krivososova, I., & Krimmer, R. (2021). To i-vote or not to i-vote: Drivers and barriers to the implementation of internet voting. In R. Krimmer, M. Volkamer, D. Duenas-Cid, O. Kulyk, P. Rønne, M. Solvak, & M. Germann (Eds), *Electronic Voting* (pp. 91–105). Springer International Publishing. https://doi.org/10.1007/978-3-030-86942-7_7

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. <https://doi.org/10.1177/0165551506066042>

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

- Madise, Ü., & Vinkel, P. (2014). Internet voting in Estonia: From constitutional debate to evaluation of experience over six elections. In *Regulating E-technologies in the European Union: Normative Realities and Trends* (pp. 53–72). https://doi.org/10.1007/978-3-319-08117-5_4
- 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>
- Männiste, M., & Masso, A. (2018). The role of institutional trust in Estonians’ privacy concerns. *Studies of Transition States and Societies*, 10(2). <https://doi.org/10.58036/stss.v10i2.676>
- Marsh, S., & Dibben, M. R. (2005). The role of trust in information science and technology. *Annual Review of Information Science and Technology*, 37(1), 465–498. <https://doi.org/10.1002/aris.1440370111>
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review*, 20(3), 709–734. <https://doi.org/10.2307/258792>
- McKeown, B., & Thomas, D. (2013). *Q methodology*. SAGE Publications, Inc. <https://doi.org/10.4135/9781483384412>
- McKnight, D. H., & Chervany, N. (1996). *The meanings of trust*.
- Möllering, G. (2001). The nature of trust: From Georg Simmel to a theory of expectation, interpretation and suspension. *Sociology*, 35, 403–420.
- 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>
- Morgan, S. (2018). Fake news, disinformation, manipulation and online tactics to undermine democracy. *Journal of Cyber Policy*, 3, 39–43. <https://doi.org/10.1080/23738871.2018.1462395>
- 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>
- Musial-Karg, M. (2017). Electronic voting as an additional method of participating in elections. Opinions of Poles. In R. Krimmer, M. Volkamer, N. Braun Binder, N. Kersting, O. Pereira, & C. Schürmann (Eds), *International Joint Conference on Electronic Voting* (pp. 218–232). Springer.
- Nemeslaki, A., Aranyossy, M., & Sasvári, P. (2016). Could on-line voting boost desire to vote? - Technology acceptance perceptions of young Hungarian citizens. *Government Information Quarterly*, 33(4), 705–714. <https://doi.org/10.1016/j.giq.2016.11.003>
- Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the internet worldwide*. Cambridge University Press. <https://doi.org/10.1017/CBO9781139164887>
- Norris, P., & Norris, P. (2022). *In praise of skepticism: Trust but verify*. Oxford University Press.
- 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>
- Pierri, F., Artoni, A., & Ceri, S. (2020). Investigating Italian disinformation spreading on Twitter in the context of 2019 European elections. *PLoS One*, 15, e0227821. <https://doi.org/10.1371/journal.pone.0227821>
- Putnam, R. D. (2001). *Bowling alone: The collapse and revival of American community*. Simon and

Schuster.

Ramlo, S. E., & Newman, I. (2011). Q methodology and its position in the mixed-methods continuum. *Operant Subjectivity*, 34(3). <https://doi.org/10.22488/okstate.11.100594>

Romanov, B., Cid, D. D., & Leets, P. (2025). *State versus technology: What drives trust in and usage of internet voting, institutional or technological trust?* *Government Information Quarterly*, 42(4), 102068. <https://doi.org/10.1016/j.giq.2025.102068>

Schiffrin, D., Tannen, D., & Hamilton, H. E. (2008). *The handbook of discourse analysis*. John Wiley & Sons.

Serdült, U., Germann, M., Mendez, F., Portenier, A., & Wellig, C. (2015). Fifteen years of internet voting in Switzerland: History, governance and use. *Second International Conference on eDemocracy & eGovernment (ICEDEG) 2015*. <https://doi.org/10.1109/ICEDEG.2015.7114482>

Serdült, U., & Kryssanov, V. (2018). Internet voting user rates and trust in Switzerland. *Third International Joint Conference on Electronic Voting*, 211–212. <https://www.zora.uzh.ch/server/api/core/bitstreams/44b97390-5e31-4715-897e-dbb0230eaeda/content>

Shu, K., Bhattacharjee, A., Alatawi, F., Nazer, T. H., Ding, K., Karami, M., & Liu, H. (2020). Combating disinformation in a social media age. *WIREs Data Mining and Knowledge Discovery*, 10. <https://doi.org/10.1002/widm.1385>

Simmel, G. (1964). *The sociology of Georg Simmel*. Free Press of Glencoe Division of Macmillan Company.

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>

Six, F. E., & Latusek, D. (2023). Distrust: A critical review exploring a universal distrust sequence. *Journal of Trust Research*, 13(1), 1–23. <https://doi.org/10.1080/21515581.2023.2184376>

Solvak, M., Unt, T., Rozgonjuk, D., Vörk, 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>

Solvak, M., & Vassil, K. (2018). Could internet voting halt declining electoral turnout? New evidence that e-voting is habit forming. *Policy & Internet*, 10(1), 4–21. <https://doi.org/10.1002/poi3.160>

Spycher, O., Volkamer, M., & Koenig, R. (2011). Transparency and technical measures to establish trust in Norwegian internet voting. In A. Kiayias & H. Lipmaa (Eds), *International Conference on E-Voting and Identity (Vote-ID 2011)* (pp. 19–35). Springer.

Sztompka, P. (1998). Trust, distrust and two paradoxes of democracy. *European Journal of Social Theory*, 1(1), 19–32. <https://doi.org/10.1177/136843198001001003>

Sztompka, P. (2003). *Trust: A sociological theory*. Cambridge University Press.

Toots, M., Kalvet, T., & Krimmer, R. (2016). Success in evoting—Success in edemocracy? The Estonian paradox. In *Lecture Notes in Computer Science* (pp. 55–66). https://doi.org/10.1007/978-3-319-45074-2_5

Turnbull-Dugarte, S. J., & Devine, D. (2023). Support for digitising the ballot box: A systematic

Appendix B.

	INTERVIEWEES COUNT
Technical researcher	3
Politician	3
Technology vendor	2
Public administrator	3
Social researcher	3
Activist/journalist	2

Appendix C.

#	STATEMENT	IDEAL TYPE
1	The centralised nature of Estonia's internet voting system raises questions about the concentration of power and the potential for manipulating election results.	Distrust in / Distrust through
2	If you have one central component, it makes sense to invest heavily in very good protection for this one point.	Trust in
3	Internet voting enhances Estonia's image as an e-state and contributes to its international recognition.	Trust through
4	The government's dependence on the e-Estonia narrative leads it to take too many risks with the internet voting system.	Distrust through
5	Trust in the Estonian internet voting system is influenced by a high level of trust in Estonian public offices and the e-government system.	Trust in
6	Vote buying, selling, and coercion are potential risks of internet voting.	Distrust in
7	A lack of understanding of the internet system leads citizens to accept simple explanations for why we should not use	Distrust in

#	STATEMENT	IDEAL TYPE
	internet voting.	
8	Internet voting cannot be 100% secure, and we need to accept the risk. Having the option to cancel internet voting and revert to paper voting makes me feel safe.	Trust in
9	If we would cancel internet voting and ask people to vote in paper, citizens would hardly trust again internet voting.	Trust through
10	The organization of a ceremony for opening the online system and presenting the results helps trusting the system internet voting.	Trust in
11	Demonstrations of the internet voting system's security, such as breaking hard disks, are like a theatre play. They are useless.	Distrust in
12	Observing online elections is more difficult than observing paper elections. It can be done solely by people with specialised technical knowledge to understand the system, and citizens are forced to delegate their trust to these people.	Distrust in / Distrust through
13	Technology provides more tools to check what happens inside the ballot box (multiple voting, verification, open code, ...), and that helps to rely on it.	Trust in
14	Clearly communicating how problems are addressed, such as decryption failures, and demonstrating preparedness for contingencies can improve confidence in the system.	Trust in
15	Although technology is secure and protocols are established, the human factor (failure, corruption) remains the main threat to internet voting.	Distrust in

#	STATEMENT	IDEAL TYPE
16	Election organisers are sufficiently trained to understand the internal architecture of the technology provided by the company building the internet voting system.	Trust in
17	Political parties base their positions on internet voting on whether they perceive it as benefiting or harming them electorally.	Distrust through
18	Those who are in power can manipulate the system, undermining democracy and eroding trust in the voting process.	Distrust through
19	There is a significant group of people openly opposed to internet voting, driven by a general distrust in the state and government, as well as political motivations.	Distrust through
20	Experts' scepticism and concerns about the technology should be taken into account, but it is essential to avoid exaggerating problems and making them appear bigger than they are.	Trust in
21	People with deep knowledge of IT tend to be the most critical of internet voting, and their mistrust primarily comes from understanding how the system works or fails to work.	Distrust in
22	People use internet voting because it is more convenient than paper voting.	Trust in
23	Journalists do not cover concerns and criticism about internet voting, contributing to the perception that everyone supports it in Estonia.	Distrust through
24	Fake news appear cause	Distrust through

#	STATEMENT	IDEAL TYPE
	internet voting is difficult to understand, and critics use those unverifiable elements to pollute the public debate.	
25	Having an active public debate and media coverage of internet voting in Estonia would build trust and generate more discussion.	Trust through
26	e-Estonia propaganda is also fake news, trying to build trust in the internet voting.	Distrust through
27	The system is audited by external institutions/ companies, and it is not easily accessible and understandable to the general public.	Trust in / Distrust in
28	Cyberattacks on internet voting happen very often, but the state is ready to defend against them, including firewalls and measures against DDoS attacks.	Trust in
29	If the website reporting the election results is down, it negatively impacts public perception of the internet voting system.	Distrust in
30	Estonians know how to use computers to vote and smartphones to verify their votes; we are protected.	Trust in
31	We can totally trust the informaticians and the company producing the internet voting technology.	Trust in
32	Tracking digital ballot boxes is easy and efficient. There are many ways to detect that something has happened thanks to technology.	Trust in
33	Trust builds upon experience. And not failing is the very basis of that; if you don't fail for many years, then the	Trust in

#	STATEMENT	IDEAL TYPE
	public trust will increase.	
34	Habit builds trust. Estonians are used to doing everything online, so they do not question internet voting. It is just one more thing.	Trust in
35	Verifying your vote on a smartphone gives you the peace of mind that, even if the voter application is tricked, you can detect it.	Trust in
36	I think too many people are voting online. I would feel safer if fewer people voted online and more on paper.	Distrust in

Published by



ALEXANDER VON HUMBOLDT
INSTITUTE FOR INTERNET
AND SOCIETY



RESEARCH
FOR THE
DIGITAL AGE

in cooperation with



CREATE



centre
— internet
et —
societe



R&I

IN3

Internet
interdisciplinary
Institute

Universitat Oberta de Catalunya



UNIVERSITY OF TARTU
Johan Skytte Institute of
Political Studies