DISSERTATIONES
RERUM
POLITICARUM
UNIVERSITATIS
TARTUENSIS
34

BOGDAN ROMANOV

Explaining Trust in Internet Voting: Institutional, Technological, and Contextual Determinants

DISSERTATIONES RERUM POLITICARUM UNIVERSITATIS TARTUENSIS
34

DISSERTATIONES RERUM POLITICARUM UNIVERSITATIS TARTUENSIS
34

BOGDAN ROMANOV

Explaining Trust in Internet Voting: Institutional, Technological, and Contextual Determinants

UNIVERSITY OF TARTU
Press
1632

Johan Skytte Institute of Political Studies at the University of Tartu

This doctoral thesis is accepted for commencement of the degree of Doctor of Philosophy in Political Science on the 2nd of March, 2026, by the council of the Johan Skytte Institute of Political Studies, University of Tartu.

Supervisors: Dr. Mihkel Solvak, University of Tartu, Estonia;
Dr. Margarita Zavadskaya, Finnish Institute of International Affairs, Finland.

Opponent: Dr. Micha Germann, University of Bath, United Kingdom.

Commencement: 23rd of April, 2026, at 14:30 in Senate Hall, University Main Building, Ülikooli 18, Tartu

The research work of this dissertation and the included publications were supported by ECePS ERA Chair of e-governance and digital public services, funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 857622. Views and opinions expressed are, however, those of the author only.

Funded by
the European Union

ISSN 1736-4205 (print)
ISBN 978-9908-57-161-4 (print)
ISSN 2806-2558 (pdf)
ISBN 978-9908-57-162-1 (pdf)

Copyright: Bogdan Romanov, 2026

University of Tartu Press
www.tyk.ee

TABLE OF CONTENTS

LIST OF PUBLICATIONS

The following three original publications and one research paper form the main body of the dissertation:

I. Romanov, B., Cid, D. D., & Solvak, M. (2025). “I Know, Therefore, I Trust? Quantitatively modelling how knowledge shapes the reliance on trust and confidence in the case of internet voting usage in Estonia”. Interacting with Computers. https://doi.org/10.1093/iwc/iwaf055

II. Duenas-Cid, David and Romanov, Bogdan, “Trust in Internet Voting: Preliminary Results of a Q-Methodology Experiment in Estonia.” (2025). AMCIS 2025 Proceedings. 2. https://aisel.aisnet.org/amcis2025/sig_egov/sig_egov/2

III. Romanov, B., & Babayan, V. (2025). “Trust in online voting under different regime settings: Evidence from public opinion on online voting in national elections in Estonia and Russia.” Journal of Information Technology & Politics, 1–18. https://doi.org/10.1080/19331681.2025.2486050

IV. 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

The studies are reprinted with the permission of the publishers.

Author's contribution

I. The author of the current dissertation was the writer and analyst of Study I and was responsible for the revision process with the publishing journal (55%). David Duenas-Cid was the contributing writer, focusing on the theoretical section (15%). Mihkel Solvak was responsible for the initial data analysis and general supervision (30%).

II. The author of the current dissertation supported qualitative data collection and transcription and wrote the Study II sections (i.e., methodology description and analysis) (60%). David Duenas-Cid was responsible for the writing, data collection, and review processes with the publishing journals (40%).

III. The author of the current dissertation developed the research design, served as the principal writer of Study III, and was responsible for the review process with the publishing journal (51%). Valeria Babayan was the co-writer of the text and additionally responsible for conducting the quantitative data analysis (49%).

IV. The author of the current dissertation was the principal analyst and writer of Study IV and was responsible for the revision process with the publishing journal (55%). Peeter Leets was the original creator and tester of the research design within the qualitative data analysis (15%). David Duenas-Cid offered assistance and recommendations during the writing process (30%).

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my supervisor and co-author, Mihkel Solvak, who has supported my academic development from the very early stages of my research trajectory, beginning with an essay written during a digital governance course that later evolved into a paper presented at E-Vote ID 2020, and continuing through to the completion of this dissertation. I am especially thankful for his willingness to dedicate time from a demanding schedule to discuss my articles and the broader dissertation project. I look forward to continuing our joint work in the future.

I am also deeply grateful to Margarita Zavadskaya, whose guidance introduced me to new scholarly domains and perspectives. Without her support, I would not have been able to engage with the international community of area studies scholars. Our early collaboration during my bachelor's studies now feels almost surreal in retrospect, and I am sincerely thankful for her mentorship and moral support, particularly during periods marked by a streak of desk rejections and other professional challenges.

This dissertation would not exist without collaboration with co-authors and colleagues. Among them, David Dueñas-Cid has been both a valued collaborator and a close colleague. His intellectual input, shared fieldwork, and the opportunities he provided were central to several parts of this project. I regret not having formally proposed his involvement as a supervisor, but for me, you are certainly a great mentor, and I remain sincerely grateful for your sustained support and collaboration. Let us finally write a book on the trust!

My collaboration with Valeria Babayan stands as a textbook example of effective academic cooperation. Our work developed organically, with a shared understanding established remarkably quickly, resulting in a study with a clear and innovative design. I am proud of this article and would like to wish Valeria all the best on her PhD journey. If you are looking for a co-author, you know my email!

I would also like to thank Peeter Leets, the final co-author of Study IV, whose expertise spans both academic research and programming, and who embodies the collocation 'jack of all trades and master of all'. It was a pleasure to revisit, refine, and publish his research design several years after its initial conception. I hope you obtain a position that matches your expertise.

Another important collaborator was Logan Carmichael, a co-author on an article that remained unpublished. Over time, she transitioned from a girl on Zoom joining calls from New Zealand to a research partner and trusted friend, with whom I could share the frustrations and uncertainties inherent to the doctoral journey. I am deeply thankful for her constant presence, understanding, and support throughout both the highs and lows of this process.

A final note of gratitude goes to my colleagues and friends, whom I first met as a student at the Higher School of Economics, Anna Dekalchuk and Yuri Kabanov. Over the past seven years, Anna and I have shared conversations about

academia, teaching, and their many peculiarities. She has consistently raised the bar for research excellence, and I have continuously tried to keep up. I sincerely hope that all of your grant applications will be approved on the first attempt. I will be waiting for you with a cup of coffee and a salmon sandwich. With Yuri, we have maintained a quiet and friendly competition over who will obtain a doctoral degree first. To a considerable extent, my decision to pursue a PhD was inspired by his example and experience. Beyond this, Yuri is an exceptionally empathetic supervisor and instructor. I wish you strength for the final stretch of your project, and I hope you never lose this empathy.

While this dissertation would not have been possible without the support of my supervisors and collaborators, it would also have been far less engaging and enjoyable without such a remarkable group mentioned below. Working alongside them made these five years intellectually stimulating and personally meaningful.

Speaking of remarkable people, I would also like to express my gratitude to my family in Surgut, Saint Petersburg, and Batumi. My brothers have consistently served as role models through their ambitions and achievements, and I am grateful for their support, the growth we experience together, and the brotherhood that transcends geography. This dissertation dedicates Chapter 2 to Aleksandr, Chapter 3 to Anastasia and Ulyana, and Chapter 4 to Dmitriy.

On July 15, 2025, I joined a group of colleagues at Printify/FYUL, which motivated me to grow not only as an academic researcher but also as a data analyst and engineer. I am grateful to, in no particular order, Andrejs Ļubimovs, Nikolajs, Dmitrijs, Svetlana, Andrejs Šohins, Elvis, Olga, Ēriks, and Ekaterina, and for nearly two years of professional development, collaboration, and an inspiring working environment. I look forward to seeing you again in Riga!

Gadir, Masha, Sergey, and Dmitriy are the names I mention whenever I am asked how many close friends from earlier stages of my life remain part of my inner circle. Thank you for being present in my life from school and university years and for remaining by my side to this day.

Separately, I would like to thank my partner, Victoria, for her patience, encouragement, and unwavering support throughout the doctoral journey. I am deeply grateful to her for listening to my rants on how difficult it is to study for 11 years back-to-back, that the publication cycle is the worst, and that combining a PhD with Estonian language courses might be too much for a puny human brain! Without you along, not only would the end goal be less visible and meaningful, but all the challenges would be much more complicated.

Finally, I would like to express my gratitude to all the people I met during the course of my doctoral studies who contributed to this journey in ways both large and small. Whether through academic discussions (Robet Krimmer, thanks a lot for being there in the moments of need), professional collaboration, administrative assistance (yes, Varje, Kerli, Kristel, Piret, with you in mind), or simple acts of kindness and encouragement, their support helped shape both the process and the experience of completing this PhD. While it is not possible to name everyone individually, their contributions are sincerely appreciated and gratefully acknowledged!

1. INTRODUCTION

The digitalization of electoral processes has fundamentally reshaped how citizens engage with democratic institutions. Electronic or digital voting broadly encompasses a variety of voting technologies, including electronic ballot machines used in polling stations, electronic counting systems, and remote electronic voting solutions (Alvarez & Hall, 2010). Introduced primarily as a solution to streamline electoral processes, reduce errors associated with manual counting, and improve accessibility, electronic voting promised to enhance voter convenience, increase electoral participation, and bolster democratic legitimacy (Krimmer & Volkamer, 2005; Norris, 2002). However, despite early optimism in the 2000s and a subsequent global rush to implement electronic voting solutions (Dalmau, 2015; Fujiwara, 2015), the diffusion and acceptance of these technologies have been uneven, marked by significant skepticism and resistance in various contexts, stemming from technical, social, and political concerns (Gerlach & Gasser, 2009; Gibson et al., 2016).

Within the broader spectrum of electronic voting solutions, Internet voting (also called online voting or i-voting) refers to casting votes remotely via Internet-connected devices (e.g., laptops, desktop computers, smartphones). Internet voting emerged in the late 1990s and early 2000s, driven by the rapid proliferation of the Internet and digital technologies and the growing public expectation for convenient electoral participation (Solvak & Vassil, 2016). Estonia notably pioneered this form of voting, first implementing it nationally in 2005, and has consistently expanded its use since then, positioning itself as a global leader and providing valuable empirical insights into the long-term adoption and implications of Internet voting (Vassil et al., 2016). Despite its transformative potential, Internet voting in general has faced persistent challenges relating to security, transparency, and public trust, leading to limited global uptake, with most democracies either avoiding its implementation entirely or cautiously experimenting with pilot programs and regional trials (i.e., Norway, Switzerland, Canada) (Alvarez et al., 2011; Appel, 2022). The experience with, and sustained commitment to, Internet voting in Estonia offers a unique vantage point for understanding how public trust in such a complex digital technology is built over time (Agbesi et al., 2023, 2024; Park et al., 2021). This is crucial, since trust is not simply an added benefit but a foundational prerequisite for the legitimacy and successful implementation of digital electoral or other state-promoted, state-affiliated technologies (Carter & Bélanger, 2005; Choi & Kim, 2012). More on that in section 2. However, the processes through which trust in Internet voting develops and the factors underpinning such trust remain inadequately understood.

The existing academic literature has predominantly approached trust in electoral technologies through a narrow technological lens. Such a perspective emphasizes technical security, system reliability, and usability, often underestimating or neglecting the broader institutional and sociopolitical dimensions of trust formation (Byrne, 2017; Fuglerud & Røssvoll, 2012; Marky et al., 2021; Zantalis et al., 2024; Zhu et al., 2021). This technologically driven viewpoint

tends to frame public trust as primarily responsive to the performance and robustness of electoral technology itself, without sufficiently considering how broader institutional and political contexts significantly shape trust dynamics (Duenas-Cid & Calzati, 2023; S. Grimmelikhuijsen et al., 2017). In response, this dissertation offers a complex multi-level approach to trust formation in Internet voting. More specifically, this dissertation seeks to unpack the effects of individual, regime-driven, discursive, and institutional features on trust in Internet voting as well as its usage. By addressing these questions, this research moves beyond simplistic discussions of technology acceptance and offers a nuanced examination of the mechanisms by which trust is constructed, proposing a complex picture of Internet voting use tied to technology and political institutions.

This dissertation employs a mixed-method research strategy integrating quantitative and qualitative methodologies, including survey data analyses, expert interviews, and Q-methodological assessments. Empirically, it primarily examines Estonia as a case of a democracy that has implemented Internet voting since 2005 and as a critical case of a country with a high degree of Internet voting exposure and information and communication technology (ICT) penetration. Estonia's extensive experience provides a unique empirical base for exploring the dynamics of trust formation. Within the dissertation, Estonia is not regarded as an isolated or exceptional case of digital democracy but rather as an illustrative example of how trust can be maintained in a context of extensive technological integration. While Estonia's experience with Internet voting is unparalleled in its duration and institutional maturity, the mechanisms of trust formation it reveals are not confined to this specific national setting. Trust in technology and institutions constitutes a global challenge that transcends regime types and levels of digital development. Therefore, the Estonian case offers transferable insights into how democracies, and, more broadly, governance systems worldwide, may foster and sustain public trust as digital governance and remote participation tools become increasingly prevalent. Additionally, the comparative insights from the limited and recent adoption of Internet voting in autocratic Russia enrich the analysis by illustrating variations in trust-building strategies, providing deeper insight into the institutional, technological, and societal factors influencing public trust in autocracies.

The empirical core of the dissertation is structured around four interrelated studies, each examining a distinct yet complementary aspect of trust in and usage of Internet voting:

- **Study I. I Know, Therefore, I Trust? Quantitatively Modeling How Knowledge Shapes the Reliance on Trust and Confidence in the Case of Internet Voting Usage in Estonia.** This study examines how individual-level characteristics of technical knowledge influence citizens' trust in Internet voting. It assesses whether greater technical competence leads individuals to rely primarily on their personal understanding of the technology or on institutional assurances of trustworthiness (i.e., the technology's performance, or trust in political institutions).

- **Study II. Trust and Distrust in Internet Voting: A Mixed-Methods Examination of Expert Insights and Public Perceptions in Estonia.** Utilizing expert interviews and Q-methodology, this study provides an in-depth investigation of discourses surrounding Internet voting, revealing how public perceptions constitute issues of transparency, technical security, and institutional performance, and how these perceptions add to trust or distrust in Internet voting.
- **Study III. Trust in online voting under different regime settings: Evidence from public opinion on online voting in national elections in Estonia and Russia.** This comparative analysis explores the mechanisms shaping trust in Internet voting by examining motivational and perceptual factors, such as civic duty, convenience, and perceived fairness. It emphasizes the varying rationales, ranging from instrumental trust in the technology to loyalty to, and trust in, the government, that citizens adopt in expressing trust in Internet voting systems.
- **Study VI. State versus Technology: The Role of Institutional and Technological Trust in Personal Trust and Usage of Internet Voting.** This final empirical chapter quantitatively evaluates the association between institutional trust (the form of trust demonstrated towards political institutions) and technological trust (the trust placed in technologies of any sort) in the trust and use of Internet voting. Additionally, it proposes a novel angle on the operationalization of the concepts of institutional and technological trust.

By synthesizing empirical evidence from these studies, the dissertation advances scholarly understanding of the multidimensional nature of trust in digital governance, focusing on Internet voting and moving beyond a narrow technological focus. Rather than limiting the analysis to technical aspects such as cybersecurity, user interface design, or system efficiency, this research integrates a broader framework that considers institutional transparency, regime-specific trust-building strategies, and users' characteristics. It explicitly illustrates how non-technological factors, such as public perceptions of institutional credibility, political regime characteristics, and civic norms, interact with technological factors in shaping trust. Thus, the dissertation offers a comprehensive framework that situates trust within a multidimensional context, contributing both theoretically and empirically to a more holistic understanding of digital governance and democratic legitimacy. As an additional output of the dissertation, there is a range of practical suggestions relevant to democracies with long exposure to this technology.

The following sections present the findings of five years of research structured into six sections. Section 2 develops the dissertation's conceptual framework by synthesizing theoretical perspectives from sociology, political science, and human-computer interaction (HCI). It defines trust and Internet voting, conceptualizes Internet voting as a sociotechnical system, and examines how trust operates as a social mediator within digitally mediated elections. It further elaborates on how

trust is converted into usage and pinpoints mechanisms that shape trust in Internet voting, including knowledge and confidence, political regime context, discourses, and the relationship between institutional and technological trust. Section 3 delineates the dissertation's scope and scholarly contribution. It clarifies how the four empirical studies, taken together, advance the understanding of trust in Internet voting by integrating insights across disciplinary, methodological, and contextual boundaries. Emphasis is placed on the dissertation's contribution to conceptual innovation, particularly through its critical engagement with narrowly conceived technological approaches and its articulation of a multidimensional trust framework. Section 4 outlines the data sources and methods employed in the dissertation, including quantitative surveys, expert interviews, and Q-methodology. It also addresses methodological limitations, particularly those arising from data harmonization challenges and temporal constraints. Section 5, "Main Findings," summarizes the key findings from the empirical studies and maps them onto the conceptual framework developed earlier. Finally, section 6 discusses the broader implications of the findings for the theoretical status quo and provides additional applied recommendations for effective policy interventions.

2. CONCEPTUAL FRAMEWORK

Trust is a foundational concept underpinning the effectiveness and legitimacy of democratic institutions and practices, and it has become increasingly pivotal in the digital age. The transition from traditional electoral systems to digital, Internet-based voting necessitates a nuanced understanding of how trust operates in this technologically enhanced democratic context.

This section establishes the conceptual framework for the dissertation by systematically developing the theoretical underpinnings of trust in Internet voting. Section 2.1 defines trust and Internet voting through the lenses of sociology, political science, and HCI, highlighting their relevance to democratic participation and digital governance. Section 2.2 frames Internet voting as a socio-technical system in which trust is indispensable due to procedural opacity and technical complexity, thereby providing additional justification for the dissertation's relevance. It further differentiates trust in Internet voting from that in traditional paper-based elections, underscoring the distinctive relational demands of digital electoral technologies. Finally, the last subsection of 2.2 conceptualizes trust as a social mediator in technologically mediated elections, positioning it as a relational mechanism that bridges citizens with the institutions and infrastructures behind Internet voting. Section 2.3 extends this analysis by exploring how trust translates into the actual usage of Internet voting systems, drawing from trust-transfer theory and technology acceptance models. Section 2.4 places discussion about trust into the democratic and autocratic political regime context as well as surrounding discourses to make the research composition more enriched. Finally, section 2.5 offers a theoretical synthesis by identifying four central mechanisms that shape trust in Internet voting: (1) knowledge and confidence, (2) regime context and technology usage rationale, (3) discourses of trust and distrust, and (4) the interaction between institutional and technological trust. Together, these five sections form a multidimensional conceptual framework that guides the empirical analysis in subsequent sections.

2.1. Definitions and dimensions of trust and Internet voting

Trust, broadly conceptualized as a psychological state encompassing the willingness to accept vulnerability based on positive expectations of another's intentions or behaviors (Mayer et al., 1995; Rousseau et al., 1998), serves as a critical facilitator of cooperation and collective action in complex modern societies. As the inherent uncertainty and complexity of social interactions and technologies increase, trust operates as a fundamental mechanism to mitigate such uncertainty by providing a heuristic framework for decision-making (Gambetta, 1988; Luhmann, 1979).

Definitions of trust vary across academic disciplines. In sociology, trust is often seen as a socially embedded mechanism that allows individuals to act despite uncertainty and incomplete information. Sztompka (1999) defines trust as a bet on others' future contingent actions, highlighting its normative and relational dimensions. Giddens (1990), on the other hand, emphasizes the role of trust in abstract systems characteristic of late modernity. Here, trust is displaced from personal relations onto expert systems, institutions, and technological frameworks, which individuals rely on without fully understanding their internal workings, for example, due to limited knowledge. Another crucial strain of the conceptual literature in this tradition is Robert Putnam's work, which holds that generalized social trust constitutes a core component of social capital alongside norms of reciprocity and civic engagement, and reflects historically embedded patterns of civic engagement, cooperation, and institutional performance. Putnam's work emphasizes that generalized trust and social capital are not primarily a rational assessment of specific actors or systems, but rather a background orientation that shapes how individuals relate to collective institutions and public authority (Putnam, 2001; Putnam et al., 1994). Societies characterized by high levels of generalized trust tend to exhibit stronger institutional legitimacy and greater acceptance of collective decision-making procedures, whereas low-trust societies display persistent skepticism toward political institutions and public governance (Fukuyama, 1996; Putnam, 2001; Putnam et al., 1994). Within the body of the PhD project, this juxtaposition of high and low degrees of social capital will be demonstrated through the cases of autocratic Russia, which initiated trials for Internet voting and is infamous for fraudulent elections, against the democratic nation of Estonia, boasting at least 20 years of experience with Internet voting and transparency within the electoral field.

In political science, trust is generally conceptualized in relation to institutions and collective governance. Levi (1998) defines political trust as a rational assessment of institutional performance and procedural fairness. Hardin (2002), meanwhile, introduces the notion of "encapsulated interest," (Hardin, 2002, p. 3) wherein trust arises from the belief that the trusted party has an interest in fulfilling the trustor's expectations. These perspectives converge on the importance of legitimacy, accountability, and transparency as critical conditions for institutional trust, especially in contexts where institutions govern complex technological systems. More recently, scholars have applied these principles to digital elections, arguing that electoral trust must be understood as both institutional and procedural. Duenas-Cid (2024), for example, highlights how the withdrawal of electronic voting in the Netherlands revealed that trust is not generated by technical functionality alone, but by citizens' belief in the motives and responsiveness of institutional actors. Similarly, Farooq, Warkentin, and Virtanen (2024) demonstrate that perceived legitimacy in Internet voting environments hinges not only on the system's technical performance but also on the relational trust between citizens and public authorities, particularly when voters perceive a shared identity or civic agency in the electoral process.

HIC scholars, by contrast, tend to frame trust as an evaluative response to system design, usability, and user control. Corritore, Kracher, and Wiedenbeck (2003) propose a multidimensional model of online trust, emphasizing users' perceptions of competence, benevolence, and integrity in digital systems. Based on the Norwegian experience with Internet voting trials, Nestas and Hole (2012) claim that, within their HCI understanding of trust, all measures aimed at improving the security and privacy of the procedures increase trust. Schneider (1999) similarly argues that trust depends on whether users experience systems as intuitive, transparent, and responsive. These insights have been further developed in recent studies of Internet voting, which show that usability, verifiability, and interface feedback mechanisms significantly influence user trust (Agbesi et al., 2023; Farooq et al., 2024). Agbesi and colleagues (2023, 2024) find that system transparency and the ability to verify one's vote are among the most critical predictors of trust in Internet voting platforms. Erb, Duenas-Cid, and Volkamer (2023) also argue that trust repair strategies, such as enhancing post-election audits or issuing clearer communication about system safeguards, can re-establish voter trust after real or perceived failures. As these contributions demonstrate, trust in technologies is not merely a technical feature, but a dynamic and experience-driven psychological response shaped by both system design and contextual messaging.

Speaking of technologies, the dissertation's cornerstone technology is Internet voting, stemming from the field of electronic voting. Electronic voting broadly refers to the use of electronic means to cast or count votes, encompassing various technologies such as electronic voting machines used at polling stations, digital ballot scanning, and remote voting methods (Alvarez & Hall, 2010; Krimmer & Volkamer, 2005). The primary objective of electronic voting systems is to enhance electoral efficiency, accuracy, and accessibility by replacing or supplementing traditional paper-based voting processes (Norris, 2002). However, electronic voting inherently introduces complexities associated with technological reliability, security, transparency, and voter confidence (Choi & Kim, 2012; Gerlach & Gasser, 2009; Gibson et al., 2016). Consequently, the adoption and acceptance of electronic voting systems are closely tied to trust in both the technology itself and the institutions responsible for overseeing electoral processes (Krimmer & Volkamer, 2005).

Internet voting, a specific subset of digital voting, involves casting votes remotely via devices with Internet access, thereby further intensifying the complexities and stakes associated with electoral integrity (Alvarez et al., 2011; Carter & Bélanger, 2012; Solvak & Vassil, 2016). Unlike traditional paper-based, or even electronic voting, conducted within controlled physical environments, Internet voting presents unique challenges due to its reliance on complex technological infrastructures, cybersecurity considerations, and the requirement for voters to trust remotely managed digital processes (Alvarez et al., 2011; Licht et al., 2021). Under this voting mode, the role of trust becomes more important because voters must believe in the integrity and confidentiality of their ballots despite lacking direct oversight of the voting procedures, which are present and

comprehensive in conventional paper voting. This role of trust is once again echoed in Putnam's work, as generalized social trust provides the societal context within which more specific forms of trust, such as institutional and technological trust, are formed and interpreted. In high-trust societies, institutional and technological arrangements are more likely to be perceived as legitimate and worthy of reliance, even when their operation is complex or partially unclear; conversely, in low-trust societies, skepticism toward institutions tends to extend to the procedures and technologies those institutions deploy (Putnam, 2001; Putnam et al., 1994; Rothstein & Stolle, 2008).

Given these inherent challenges, the transition to Internet voting magnifies the importance of both institutional trust, which refers to the trust placed in electoral management bodies and governmental institutions, and technological trust, referring to user confidence in the reliability and security of the technological systems employed (S. Grimmelikhuijsen et al., 2017; Mcknight et al., 2011). This perspective is particularly relevant for Internet voting, which amplifies reliance on abstract systems and unseen actors. Trust in Internet voting can therefore be understood not only as an evaluation of technical performance or institutional competence, but also as an expression of deeper societal trust dispositions. This trust-related status quo is fundamental to understanding and analyzing the acceptance, use, and legitimacy of Internet voting systems.[1] The subsequent discussion elaborates on these dimensions, highlighting their distinctive yet interdependent roles within the sociotechnical context of Internet voting.

2.2. Internet voting as a trust-dependent sociotechnical system

2.2.1. Internet voting as a sociotechnical system

As noted in the previous section, Internet voting technology must be understood as a sociotechnical system: a complex ensemble of technical components (hardware, software, networks) intertwined with socio-political elements (people, political institutions, legal frameworks) (Clarke & Martens, 2016). Researchers have emphasized that many past electronic voting initiatives focused too narrowly on technical requirements, neglecting the human and contextual factors that critically affect success (Adeshina & Ojo, 2020; Dueñas-Cid, 2024). Adeshina and Ojo (2014), for example, argue that treating electronic voting as a sociotechnical system is essential because its adoption depends not only on cryptographic protocols, Zero Trust architectures, and software reliability but also on users' attitudes, organizational trust, and political context (Farooq et al., 2024).

[1] In order to streamline the core argument, interpersonal trust, despite potentially being another impactful factor in the question of adoption, is not covered in the dissertation.

In other words, the technology cannot be separated from the social domain in which it operates. Trust is the connective tissue binding these technical and social elements together – voters must trust the technology and the people and institutions that manage it, as well as the technology produced by these people or an independent technology vendor (Clarke & Martens, 2016). A secure voting server, for instance, is of little value if citizens do not trust the electoral commission that is responsible for it, and vice versa. Thus, any conceptualization of Internet voting must account for both the technical system and the surrounding social system, highlighting their interdependence. This sociotechnical perspective frames Internet voting as inherently trust-dependent: the proper functioning of the system and its acceptance, use, and acceptance by users are predicated on complex trust relationships among voters, technology, and political institutions in general, and electoral authorities in particular (Erb et al., 2023). Ignoring these relationships risks overlooking why people may accept or reject Internet voting. Negative examples include assuming that a well-engineered system will automatically be trusted, or that an extensive period of usage without major flaws will be "attractive" enough to engage new users. Such assumptions may lead to what has been described as technological fixes – attempts to address complex social and institutional challenges through purely technical solutions. In the context of digital governance or Internet voting in particular, these fixes often fail to resolve underlying trust problems because trust is not reducible to system performance or design features alone, but is embedded in broader sociopolitical relations and institutional accountability (i.e., a new version of the Internet voting application is realized, promising improved vote privacy, while in reality people never had issues with the technical side of voting via Internet in the first place, but rather with the political part) (Beck, 1992; Bijker et al., 1987; Jasanoff, 2004; Winner, 1980). As highlighted by Beck (1992) and Jasanoff (2004), technological systems that disregard the social and normative dimensions of risk and legitimacy may even deepen distrust by appearing unresponsive to citizens' concerns. Therefore, understanding trust in Internet voting requires moving beyond technical robustness to examine institutional credibility, communicative transparency, and users' lived experiences within their sociotechnical context.

In practice, all voting systems require some degree of trust; Internet voting amplifies this demand because of its intangible, expert-dependent nature. Sociological theories of trust help explain this. Niklas Luhmann (1979) famously argued that trust functions as a mechanism to reduce social complexity, enabling individuals to act in situations where they cannot fully control or understand all aspects (Volkamer et al., 2011). Casting a vote over the Internet is precisely such a situation: the voter cannot see the physical ballot or the count, hence they must trust complex software processes to faithfully record and tally their choice. Trust, in Luhmann's sense, makes this leap of faith manageable by reducing the daunting complexity of cryptographic algorithms and network security into an expectation of reliability (Volkamer et al., 2011). The need for trust in Internet voting increases when juxtaposed with the conventional paper-based voting,

which is observable, involves material artifacts, is easy to comprehend, and is practiced globally (Willemson, 2018).

Similarly, trust fulfills a need for stability and predictability in modern systems (Benk et al., 2024; Erb et al., 2023; Volkamer et al., 2011). As Piotr Sztompka noted (1999), citizens look for transparency and accountability in institutions; when interacting with a complex technological system, trust is what assures voters that "things will work as they should," even if they themselves cannot observe or verify each step (Marky et al., 2021; Volkamer et al., 2011). Furthermore, Anthony Giddens' concept of abstract systems is highly relevant: in high-modernity societies, many critical processes (from banking to air travel) operate as abstract, expert-run systems that laypeople must simply trust to function (Volkamer et al., 2011). The litmus test in this scenario is: do you, the reader, use the banking application with all your savings because you trust the application itself, or do you trust the abstract banking system and expect the application to work as expected? Hence, Internet voting is a quintessential example of an abstract system: the average voter lacks the specialized knowledge to evaluate the encryption protocols, server security, and software integrity that determine the election's outcome. There is an inherent knowledge imbalance between the system's designers/operators and its users. Giddens (1990) argues that under such conditions, trust in expert systems is "faceless" – people extend trust without any personal acquaintance, basing their confidence on an assumption of expert competence. In Internet voting, voters are asked to trust an impersonal technical apparatus and the "unseen" experts maintaining it. This trust bridges the technical knowledge gap, allowing citizens to participate in the election without personally verifying every mechanism (Volkamer et al., 2011). Crucially, this involves vulnerability: trusting a system means risking that one's expectations could be betrayed. Mayer, Davis, and Schoorman's (1995) classic definition of trust as the willingness to be vulnerable based on positive expectations of the other's actions applies here. Voters make themselves vulnerable when they cast an electronic ballot, they are relying on the technology and its administrators to do the right thing with their vote, with no immediate way to intervene or correct errors, besides the verification mechanism in the Estonian case, which requires trust as well (the proof on the screen shall be treated as genuine, while there could be manipulation from an attacker's side aiming to convince the voter that the vote was recorded-as-cast) (Solvak, 2020). In sum, Internet voting inherently demands trust because it asks citizens to act under conditions of complexity, invisibility, and unequal knowledge in a secret-vote system, where the connection between the voter's identity and the ballot is deliberately broken. Trust is what enables action in this context of uncertainty: it is the leap of faith that underlies any use of Internet voting technology.

2.2.2. Trust in Internet voting vs. traditional voting

The trust required for Internet voting differs in both degree and kind from that in traditional paper-based voting. In a traditional polling station scenario, many safeguards are tangible and visible: ballot boxes are observed by poll workers and party agents, paper ballots can be recounted by hand, and the count is often conducted in public or with observers present (Garnett & James, 2020; Wadowski, 2025). These features mean that much of the verification is social and transparent, reducing voters' need to simply "trust" that everything is honest; they or their representatives can literally watch it happen (Alvarez & Hall, 2010). Moreover, the chain of custody for paper ballots is straightforward and understandable to most voters (i.e., ballots go from the voter's hand into a box, then to a counting table, etc.). Of course, trust is still needed; one must trust poll workers to not tamper with ballots, for instance, but it is a trust distributed among many people and steps, often reinforced by direct oversight and auditability.

Internet voting, especially remote Internet voting from one's personal device, largely eliminates the transparent, observable aspects of election administration that voters are accustomed to. In a typical Internet voting system, once the voter clicks "submit," the remainder of the voting process occurs within software and hardware the voter cannot see or touch (Appel, 2022; Appel et al., 2019). There is no physical artifact in the voter's hand, no observers crowding around a ballot box, and usually no simple way for the voter to personally verify that their vote was counted as intended (besides the verification code on the paper, as in the case of Switzerland, or second phone, used for the verification, as in the case of Estonia). However, these codes are used only to verify that the vote was cast as intended and later recorded, and that, at the final stage of elections, the vote was included unmodified and counted correctly as part of the encrypted tally. In technical terms, most Internet voting systems today lack a voter-verifiable paper trail (Halderman & Teague, 2015). As a result, the traditional ability to conduct an independent recount or audit is fundamentally altered or lost (Schryen & Volkamer, 2010; Volkamer et al., 2011).

Election security experts underscore that while paper ballots can be audited and recounted to resolve doubts, purely electronic votes cannot be validated in the same manner – the system must be designed to be correct and the public must believe it is correct (Appel, 2022). This shifts the burden of trust: voters must trust the technology itself to accurately capture and store their vote, and trust that no unseen malware, network attack, or software bug has compromised the outcome (Duenas-Cid, 2024). They must also trust the processes and people behind the technology. For instance, that election officials and system vendors have implemented the software correctly, that no insider is malicious, and that proper security protocols are followed at all times.

In a paper system, most of the electoral fraud efforts do not scale much and would require a large number of actors involved (e.g., stuffing many paper ballots or altering counts in multiple locations), whereas a digital attack could, in theory, be executed by a small group or a single hacker if the system has vulnerabilities

(Springall et al., 2014). This asymmetry means the scope of who must be trusted narrows but deepens: one must have very high trust in a few technical and institutional guardians of the system, rather than moderate trust in many distributed actors. Furthermore, paper voting offers psychological reassurance through visible physical evidence. Internet voting typically provides only digital receipts or confirmations that voters cannot verify independently (Solvak, 2020). Even cryptographically enhanced verification depends on user comprehension of complex protocols. Zollinger et al. (2025) found that when voters do not understand receipt-based verification mechanisms, overall trust remains low.

In summary, Internet voting demands a qualitatively deeper level of trust in the integrity of the technical system, because the usual physical guarantees of transparency are replaced by invisible digital assurances. As Appel (2022, p. 533) bluntly concluded, "no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet" (the Estonian system of Internet voting would be a counterargument to the claim). Thus, voters and policymakers are left with a question of how much trust and risk they are willing to accept for the sake of convenience and transparency. One can make the Internet voting code public, but there are two scenarios: white hackers can try to improve the system by proposing fixes and changes to the code, while in parallel, hostile hackers have "full" access to the production code. The difference is not that paper voting is infallible (since it is not true, as showcased by electoral autocracies), but that irregularities in a paper system can often be detected and addressed through human witnesses and audits, whereas irregularities in a cyber system may go undetected without extraordinary expert analysis (Springall et al., 2014). Therefore, trust in Internet voting is more all-or-nothing: citizens either trust that the entire technical system and its operators and affiliated parties work properly, or they suspect the entire outcome, since they have little option to verify or contest specific issues themselves without engaging in the trust loop. This means that the electorate, due to their limited knowledge, has to trust the Internet voting expert that would validate that the Internet voting system is trustworthy. This dynamic is a profound shift from traditional voting and lies at the heart of debates over the adoption of Internet voting.

2.2.3. Trust as a social mediator in technologically mediated elections

The preceding comparison of Internet and traditional voting systems illustrates that trust in the former is more centralized, abstract, and dependent on complex technical assurances. However, trust does not emerge solely from system architecture or auditability. Instead, it is also profoundly shaped by voters' broader relationships with political institutions (including the political alignment with the core political actors, such as parties, and their stance towards Internet voting (Ehin & Solvak, 2021)), cultural norms, and perceptions of procedural fairness. This section explores how trust operates as a social mediator in technologically

mediated elections, bridging the gap between individual voter decisions and the institutional and technological environment in which those decisions unfold.

Given the above, how does trust function within an Internet voting context? Theoretically, trust serves as a mediator between citizens and the complex socio-technical system that conducts the election – the mediation results in the use of technology under conditions of uncertainty. Several layers of trust can be delineated. First, there is trust in the technology itself as a non-human actor. Voters must believe that the hardware and software will perform as intended (e.g., accurately recording votes, preserving secrecy, and resisting fraud). This kind of trust resembles what HCI researchers call "trust in automation," in which the machine is the trustee (Hoff & Bashir, 2015). Notably, trusting a machine is different from trusting a person: the machine has no intentions or moral agency; it cannot choose to be honest or dishonest, but it can succeed or fail based on its design and operation (Hoff & Bashir, 2015; Lee & See, 2004). As theorists point out, a technological artifact has limited capabilities and does exactly what it is programmed to do, which may or may not align with the user's expectations (Hoff & Bashir, 2015; Parasuraman & Riley, 1997). Thus, trust in a voting system's technology often boils down to trust in its designers and in the rigorous testing of that technology.

This leads to the second layer: trust in institutions and people who deploy and oversee the system. Voters need confidence that election officials, software developers, cybersecurity experts, and auditors have acted competently and ethically. In democratic theory, this institutional trust is crucial – democratic processes are legitimized not just by their outcomes but by public belief in the integrity of those who run them (Duenas-Cid, 2024; Freitag & Ackermann, 2016). If citizens do not trust the authorities responsible for an Internet voting system, they are unlikely to trust the technical system those authorities put in place. Conversely, if election administrators and the government enjoy high public trust, that goodwill can transfer to the new voting system. Empirical studies in digital voting have observed such "trust transference" effects: for instance, in Estonia's long-running Internet system, general trust in the national government and election commission has been identified as a factor reinforcing citizens' trust in the Internet voting process (Ehin & Solvak, 2021; Solvak & Vassil, 2018; Vassil et al., 2016). This implies that the social context of trust – trust in, for example, government, parties, and media can significantly improve perceptions of Internet voting. From a sociology of technology perspective, the trustworthiness of a sociotechnical system is not inherent solely in its technical design; it is co-produced by social narratives, reputations, and relationships (Bijker et al., 1987; Corritore et al., 2003). A highly secure system can still be distrusted if the public lacks trust in those operating it, and a marginally secure system might be widely trusted if it is surrounded by strong social legitimacy (Dueñas-Cid, 2024).

The third layer of trust involves trust-building measures and interfaces that connect the human user to the technical process. Here, insights from HCI are particularly valuable. HCI research suggests that users are more willing to trust an automated system when they receive feedback, explanations, or tangible

confirmations of the system's actions (Carback et al., 2010; Juma & Oguk, 2020; Ryan et al., 2009). In the context of Internet voting, this translates into design features such as confirmation screens, printable or digital receipts, public transparency portals, and verification tools that reassure voters that their vote was cast and counted as intended. For example, Zollinger et al. (2025) show that trust falters when verification tools are incomprehensible, while more transparent mechanisms can foster higher user confidence (Chondros et al., 2016; Solvak, 2020). In a voting scenario, a voter might be given a tracking code to confirm their ballot was received, or a mechanism to verify after the election that their vote was included in the tally (without revealing its content). Such features can strengthen trust during the "initial stages of trust development," when users are naturally cautious and seek external reassurance.

Over time, as voters gain experience and the system builds a track record of credible performance, the need for constant verification may diminish, and a more implicit trust can develop. This pattern is observed in Estonia, where repeated successful elections gradually normalized Internet voting as a trusted option (Solvak & Vassil, 2018; Vassil et al., 2016). Still, from an HCI standpoint, maintaining appropriate trust is vital: designers must avoid both extreme skepticism (which deters use) and over-trust (which could lead users to ignore the important cues of problems). Usability and transparency go hand in hand with trust. If an Internet voting interface is confusing or opaque, it can undermine trust by making voters unsure whether their actions were recorded correctly. Likewise, if the system is too complex for the average voter to comprehend at a basic level, it may constitute feelings of helplessness or blind faith, neither of which is desirable in a democratic context. The goal, instead, is an informed trust: voters should understand enough about the system to know where their trust is required and where it is being safeguarded by verifiable mechanisms (Hoff & Bashir, 2015; Lee & See, 2004).

In summary, trust in Internet voting functions as a multi-layered mediator. It is the psychological state that allows individual citizens to confidently delegate the handling of their vote to an unseen technological process; it is the social consensus that the electoral outcome is valid and honest; and it is the product of deliberate design choices that seek to make an inherently opaque process more transparent and user-friendly. Each of these layers, technological and institutional, reinforce the others. Theoretically, this underscores contributions from the sociology of technology (which reminds us that technology and society are co-constructed through trust relationships), from democratic theory (which highlights trust as foundational to legitimacy and consent), and from HCI (which guides the design of systems that users find credible and trustworthy). All three perspectives converge on a central insight: Internet voting cannot succeed as a democratic practice unless citizens trust it. And earning that trust requires careful balancing of technical rigor, social accountability, and user-centric design. It is a demanding standard, but a necessary one if Internet voting is to complement or replace traditional voting in a manner that strengthens rather than weakens democratic trust (Marky et al., 2021; Springall et al., 2014; Volkamer et al., 2011).

Taken together, the preceding subsections of section 2.2 have illustrated that trust in Internet voting is a multifaceted construct shaped by both technological and social dynamics. Section 2.2.1 positioned Internet voting as a complex socio-technical system, emphasizing that trust must compensate for the inherent complexity of digital infrastructures. Section 2.2.2 further distinguished the nature of trust required for Internet voting from that of traditional voting systems, highlighting a shift from socially distributed, observable safeguards to individualized reliance on technical and institutional intermediaries. Finally, section 2.2.3 theorized trust as a relational mediator between citizens and voting technologies, showing how this trust is anchored not only in system design and interface usability but also in institutional legitimacy and broader socio-political contexts. These insights underscore the importance of understanding trust not merely as a disposition but as a socially constructed mechanism that enables democratic participation in technologically mediated elections.

The next section, 2.3, builds on this foundation by first explaining how trust is translated into technology usage and later articulating the specific theoretical mechanisms that shape trust in the context of Internet voting. Section 2.4 situates notions of trust and usage within a political regime-driven context, shaped by discourses, thereby showing that adoption is not only dependent on user-centric features but is also heavily tied to the context in which technology is deployed. The final theoretical section offers a structured synthesis of key conceptual dimensions, including knowledge and confidence, regime context, institutional and technological trust, and discursive framings, that together provide an analytical framework for interpreting the empirical findings of this dissertation.

2.3. How trust converts into the usage of Internet voting

Understanding how trust translates into the actual usage of Internet voting involves analyzing the psychological, institutional, and technological mechanisms through which trust influences behavioral intentions and subsequent actions. Trust, as defined above, is fundamentally a psychological state that mitigates uncertainty and enables individuals to make decisions under conditions of incomplete information (Luhmann, 1979; Mayer et al., 1995). In the specific context of Internet voting, trust functions as an essential mediator, translating abstract assurances provided by electoral authorities and technology into concrete behavioral choices, specifically, the decision to adopt and continuously use Internet voting systems.

The conversion of trust into usage follows a user-centric logic rooted in established theories from HCI and technology acceptance models (TAM) (Bahmanziari et al., 2003; Davis, 1989; Venkatesh et al., 2003). According to these frameworks, perceived usefulness and perceived ease of use serve as critical intermediate variables linking trust to actual usage behavior. Trust, in this respect, enhances perceptions of both usefulness and ease of use by reducing perceived risks and uncertainties associated with technology adoption (Gefen et al., 2003; Pavlou, 2003). When voters trust an Internet voting system, believing it to be secure,

reliable, and effectively managed, they are more likely to perceive the system as both beneficial (usefulness) and user-friendly (ease of use), which significantly increases their likelihood of choosing to use it (Carter et al., 2016; Farooq et al., 2024; Warkentin et al., 2018).

Institutional credibility plays a significant role in this conversion process. High institutional trust, resulting from perceptions of competence, integrity, transparency, and accountability, boosts voter trust in the legitimacy of electoral processes (S. G. Grimmelikhuijsen & Meijer, 2014; Norris, 2014). When electoral institutions are viewed positively, trust in these bodies can spill over to trust in the technologies they deploy. This institutional trust reinforces voters' confidence in the technology, facilitating its adoption and sustained use (Solvak & Vassil, 2018). Conversely, low institutional credibility can create skepticism and reduce the likelihood of adopting Internet voting, even if the technology itself is robust (Alvarez et al., 2011). However, there might be exceptions or paradoxes, as is the case in Russia.

Technological trust similarly influences the conversion of trust into usage by directly affecting voters' perceptions of system reliability and security (Carter & Bélanger, 2012; Mcknight et al., 2011). Effective cybersecurity measures, transparent operational procedures, and demonstrable system robustness enhance technological trust, making voters more comfortable with adopting Internet voting as a reliable method of electoral participation (Springall et al., 2014). This technological reassurance helps voters overcome potential psychological barriers related to technological complexity and the abstract nature of digital systems.

Furthermore, the individual-level dimensions of knowledge and confidence significantly shape how trust is translated into usage. As previously discussed, voters with high technical knowledge rely less on institutional assurances and more on their understanding of the technology (Romanov et al., 2025). For these individuals, trust translates more directly into usage through personal confidence and technical assurance. Conversely, individuals with lower technical knowledge require additional institutional reassurance, indicating that institutional trust is particularly critical for converting their trust into actual usage behavior (Solvak & Vassil, 2018; Volkamer et al., 2011).

In conclusion, trust translates into Internet voting usage through a multifaceted process that involves psychological, institutional, and technological dimensions. High institutional credibility and robust technological safeguards significantly enhance the perceived usefulness and ease of use, which, in turn, mediate the relationship between trust and the actual adoption of Internet voting. The interaction of these dimensions underscores the need for electoral bodies to develop comprehensive trust-building strategies, ensuring transparency, reliability, and user-centric design to foster widespread adoption and sustained use of Internet voting technologies.

2.4. Trust and usage of Internet voting within political regimes and discursive contexts

While previous sections conceptualized trust in and usage of Internet voting primarily through sociotechnical and individual-level dynamics, it is equally necessary to situate these processes within a broader political and communicative context. Trust in technology does not emerge in a vacuum but is continuously shaped by the institutional configurations, political incentives, and narrative frames through which digital elections are introduced, debated, and normalized. This dissertation is aware of the trust and usage environment.

Political regimes provide the normative and institutional foundations that condition how citizens interpret and evaluate everything, from pension reforms to the introduction of Internet voting technology. In consolidated democracies such as Estonia or Switzerland (*Explore the Map*, 2025; *The V-Dem Dataset – V-Dem*, 2025), Internet voting is embedded in systems characterized by transparency, pluralism, and stable electoral management institutions (Alvarez et al., 2009; Espinosa & and Pino, 2025; Germann & Serdült, 2017; Mendez & Serdült, 2017). These contexts encourage the development of trust through mechanisms of procedural reliability and institutional continuity, where repeated credible performance reinforces confidence and legitimacy (Norris, 2014; Solvak & Vassil, 2018). Citizens perceive technology as an extension of accountable governance rather than a substitute for it, and long-term exposure can routinize and habituate Internet voting (Vassil et al., 2016). This continuity of experience exemplifies what Giddens (1990) calls "trust in abstract systems" (p. 83): confidence maintained through institutionalized expertise and stable routines rather than direct verification.

By contrast, in competitive or digital autocracies such as Russia, Internet voting operates within constrained political environments. Here, the technology becomes entangled with regime-maintenance strategies rather than participatory innovation. As Guriev and Treisman (2020) argue, informational autocracies rely on selective transparency and managed participation to maintain legitimacy while avoiding open contestation. Digital technologies, including Internet voting, serve several functions, for instance, symbolic functions, demonstrating administrative modernity and citizen engagement without altering power asymmetries (Morozov, 2011; Roberts & Oosterom, n.d.). An alternative use case could be the reduction of transactional costs for data collection for the autocrat, as in China, another case of digital autocracy (Deng & Liu, 2017; Du et al., 2019). In these contexts, trust often becomes performative. Citizens may publicly express confidence in the system while privately doubting its neutrality, reflecting what Reuter (2020) describes as "compliance-based legitimacy." The result is a paradox in which trust serves as an expression of loyalty rather than an evaluative belief in procedural fairness.

Discursive environments reinforce these regime-dependent logics. In democratic contexts, open media and civil society generate pluralistic narratives around Internet voting, framing it through discourses of efficiency, accessibility, and

transparency while allowing for institutional criticism and contestation (Downing & Brun, 2022; Duenas-Cid & Calzati, 2023; Ehin & Solvak, 2021). Conversely, in authoritarian settings, discursive space is restricted and official narratives monopolize the meaning of technological innovation. Digital reforms are framed as proof of state efficiency and national modernity, while oppositional voices risk marginalization or sanction (*Digital Authoritarianism in China and Russia*, 2020; Dukalskis & Gerschewski, 2018; Gritsenko & Indukaev, 2021). This discursive asymmetry converts technological trust into a component of political conformity and limits citizens' ability to interpret the technology independently.

Consequently, both the trust and usage of Internet voting must be understood as politically and discursively embedded acts. Citizens' willingness to use digital voting systems reflects not only their evaluation of technological reliability, institutional credibility, or their individual-level preferences, but also their interpretation of the surrounding political narratives. In democracies, using Internet voting can signify civic confidence and institutional legitimacy; in autocracies, it may indicate normative compliance, habitual adaptation, or even quiet dissent within constrained boundaries of expression (Reuter & Szakonyi, 2021). Hence, this broader perspective expands the sociotechnical framework developed in earlier sections by linking micro-level mechanisms of knowledge and confidence with macro-level regime structures and communicative practices. It underscores that Internet voting is simultaneously a technical artifact, a governance instrument, and a symbolic resource within political discourse (Beck, 1992). Understanding its adoption, therefore, requires examining how these dimensions interact: how regimes frame technological adoption, how discourses circulate trust and distrust, and how citizens navigate these overlapping meanings when deciding whether to vote online, while being aware of the technology itself.

In summary, situating Internet voting within its political regime and discursive context explains why similar technologies evoke distinct trust logics across countries. The degree of institutional openness, media pluralism, and discursive freedom determines whether trust manifests as reflective confidence or as strategic conformity. The next section builds on this foundation by specifying the theoretical mechanisms through which these contextual factors operate. These include knowledge and confidence, discourses, regime context, and institutional and technological trust, together forming a coherent multi-level framework for analyzing how trust in Internet voting is created, maintained, and contested.

2.5. Mechanisms shaping trust in and usage of Internet voting: A theoretical synthesis

This section offers a comprehensive theoretical synthesis of the mechanisms that influence trust formation in Internet voting. Its primary purpose is to articulate, clearly and systematically, the conceptual underpinnings that guide the empirical investigations of this dissertation, providing a coherent analytical lens through which trust dynamics can be assessed and interpreted. By explicating these

mechanisms: (1) knowledge-confidence, (2) various discourses, (3) political regime and rationale for usage, and (4) mere institutional and technological trust, the section establishes a detailed theoretical foundation, critical for understanding the multifaceted connections across factors that shape public trust in digital electoral systems. The subsequent analysis of each mechanism integrates existing scholarly discourse and highlights the empirical relevance to the specific context of Internet voting.

2.5.1. Knowledge and confidence

The knowledge-confidence mechanism is introduced first because it operates at the micro level, relying on a minimal set of individual attributes to explain how people relate to complex technical systems like Internet voting. It foregrounds the users' characteristics, which shape individuals' orientations toward Internet voting. Such as whether they trust the system as an external object or have internalized a sense of confidence grounded in their own understanding. This makes it analytically distinct from other mechanisms, which depend more heavily on macro-institutional or discursive factors. Moreover, because Internet voting systems are largely opaque in their operation, users must compensate for this opacity through a combination of personal knowledge and contextual cues. Theoretical distinctions among knowledge, confidence, and trust thus offer a simplistic yet powerful framework for explaining individual-level variance in the acceptance and use of such systems.

Knowledge, in this framework, is conceptualized not merely as factual understanding but as an individual-level condition that allows individuals to reduce uncertainty and complexity when interacting with abstract systems (Giddens, 1990; Luhmann, 1979). It is linked to rationalization and reflexivity in late modernity, where individuals are increasingly expected to assess risks and make informed choices about technologies embedded in their daily lives. In the specific context of Internet voting, knowledge involves understanding the system's operation, including its security principles, verification protocols, and reliability expectations. However, this is rarely expert-level comprehension; rather, it is an average orientation shaped by digital literacy and prior exposure to similar systems.

Confidence, on the other hand, refers to a taken-for-granted attitude toward the future performance of a system or actor, derived from routine expectations or prior familiarity (Giddens, 1991; Luhmann, 1988). Unlike trust, confidence does not require a leap of faith or engagement with risk; it presumes that the system will continue functioning as expected without deliberate reflection or institutional validation. Confidence is directed toward "systems" or "background conditions" of action, where breakdowns are rare, and system logic is invisible (Lewis & Weigert, 1985). For example, using an ATM or online banking platform typically reflects confidence rather than trust.

The distinction between confidence and trust is analytically central. As Luhmann (1988) argued, trust becomes relevant only when confidence is insufficient, when individuals face unknowns, potential risks, or system breakdowns.

Trust presupposes uncertainty and a conscious decision to accept vulnerability (Misztal, 2013). Tilly (2004) further emphasized that trust involves contingent social relations, while confidence often operates impersonally. In the case of Internet voting, confidence may be present when users perceive the system as stable, familiar, and predictable. But when doubts arise about manipulation, fraud, or malfunction, trust must substitute for confidence, particularly in the absence of technical expertise.

Knowledge plays a dual role here. It can generate confidence by reducing perceived complexity and risk. When individuals feel capable of evaluating a system themselves, they no longer need to rely entirely on institutional guarantees. However, in the absence of sufficient knowledge, users must lean on trust in institutions, experts, or media representations to bridge the knowledge gap. This dynamic is particularly acute in Internet voting, where most of the system's core processes (e.g., encryption, authentication, server security) are not observable. As Giddens (1991) noted, abstract systems demand trust precisely because their operations lie beyond the layperson's direct scrutiny.

Sociological insights into technological modernity confirm this logic. Simmel (1950) observed that confidence in systems is stabilized through routine and habitual interaction, whereas trust is always provisional and context-sensitive. Lewis and Weigert (1985) proposed that trust is both cognitive and emotional, distinct from the routinized expectations associated with confidence. In technologically mediated elections, this distinction matters. Internet voting presents an "invisible" infrastructure, in which confidence is fragile and easily disrupted. Misztal (2013) and Beck (1992) both emphasized how modern technological systems tend to shift risk perception from the realm of knowledge to that of trust. As such, individuals must draw on institutional credibility, expert narratives, or social cues to reorient themselves toward the system.

In sum, the mechanism of knowledge and confidence offers a foundational perspective for understanding the micro-level conditions under which Internet voting becomes acceptable or suspect. Where knowledge is sufficient, it generates confidence; where it is absent, trust must compensate. The capacity to assess technological reliability becomes stratified across individuals, rendering the sociotechnical architecture of Internet voting both cognitively and normatively contingent.

These conceptual distinctions yield several theoretical expectations regarding how knowledge, confidence, and trust interact to shape the usage of Internet voting. First, it is reasonable to expect that greater technical knowledge reduces individuals' reliance on trust by enabling them to gain confidence in the system's performance through self-directed evaluation. Knowledge functions as a moderator of trust: when knowledge is high, confidence can substitute for trust; when knowledge is low, trust becomes indispensable. In this sense, confidence and trust are not mutually exclusive but relationally contingent. Second, confidence in Internet voting is likely to be a stronger predictor of actual usage than abstract trust, because confidence is grounded in perceived familiarity and practical assurance. However, in the absence of knowledge or prior experience, trust in institutional actors, such as government or electoral authorities, becomes essential

for justifying participation. In this way, institutional trust serves as a compensatory mechanism that stabilizes the decision to use the technology under conditions of uncertainty (Luhmann, 1988; Misztal, 2013).

Finally, a residual but theoretically important role is played by technological trust, understood as general trust in digital systems or IT infrastructures. While often conceptually adjacent to confidence, technological trust is more diffuse and backgrounded. It may reinforce or erode confidence depending on whether users perceive the Internet voting system as aligned with broader experiences of secure technology. In this respect, trust in the Internet voting system's performance and trust in government are not just empirical variables but conceptually distinct dimensions of mediated trust, shaped respectively by system-level cues and institutional reputation (Giddens, 1991; Lewis & Weigert, 1985). The interaction between these types of trust and users' own knowledge is thus central: a technically literate individual with low institutional trust may still vote online due to confidence, while a layperson may require both trust in the system's technical functioning and in the institutions overseeing it.

This conceptual framework posits a triadic mechanism. That knowledge enables confidence, confidence reduces the need for trust, and trust signals (institutional or technological) compensate when knowledge is absent or uncertain. All three, in turn, shape the ultimate behavioral outcome, whether or not the individual chooses to use Internet voting.

2.5.2. Discourses of trust and their sources

As discussed in section 2.4, trust in Internet voting is not solely an outcome of institutional performance or technological robustness; rather, it is shaped discursively through competing societal narratives about technologies and institutions. Drawing on the theoretical model proposed by Duenas-Cid and Calzati (2023), trust and distrust are conceptualized as distinct yet interdependent constructs, each governed by its own logic and articulated through separate discursive channels. These constructs coexist in continuous dialogue, with each shaping the interpretive lens through which citizens evaluate digital voting systems.

This perspective underscores that Internet voting is embedded in a communicative landscape where discourses circulate through media, political rhetoric, and public deliberation. Trust is often anchored in affirmative narratives that emphasize institutional continuity, technological maturity, and past successes. Such discourses normalize Internet voting as a habitual, low-risk, and future-oriented practice. These constructions are particularly powerful in contexts like Estonia, where long-term exposure to the technology has facilitated the formation of positive feedback loops between everyday usability and trust in institutional performance (Duenas-Cid & Misev, 2024; Solvak & Vassil, 2018)

Yet, this communicative environment is not politically neutral. Elections constitute inherently contested arenas, in which narratives of trust and distrust become instrumentalized by political actors seeking legitimacy or advantage. Political elites, parties, and media outlets actively shape how citizens assess the reliability and fairness of Internet voting, framing it either as an emblem of

technological progress and democratic innovation or as a potential source of manipulation and institutional bias. Consequently, trust forms not only through repeated positive experiences with technology and governance but also through the ongoing struggle over meaning that unfolds in the public sphere. In this sense, trust in Internet voting emerges as both a sociological and political phenomenon, rooted in institutional performance and technological reliability, yet constantly renegotiated through political discourse and electoral competition.

Conversely, distrust emerges through narratives that question transparency, institutional motives, and the integrity of the electoral process[2] (Bauer & Fatke, 2014; Duenas-Cid & Calzati, 2023). These narratives are often animated by opposition actors, critical media, or skeptical citizens who foreground themes of vulnerability, secrecy, or unaccountable design. Importantly, such discourses do not necessarily dispute the technical functionality of Internet voting but rather highlight its sociopolitical implications. They stress the invisibility of back-end processes, inadequate public engagement, and the perceived absence of account-ability in system design and deployment (Dueñas-Cid, 2024; Ehin & Solvak, 2021).

By treating trust and distrust as discursively constructed, this framework allows for a nuanced interpretation of how citizens make sense of Internet voting beyond cost-benefit analysis. It recognizes that even in highly digitalized societies, trust is not simply inherited from system performance but is actively negotiated through competing claims about what the system represents, whom it serves, and how it is governed. Therefore, electoral authorities seeking to enhance public confidence must attend not only to technological and institutional dimensions but also to the symbolic and rhetorical environments in which these technologies are embedded.

2.5.3. Political regime context and technology usage rationale

This third mechanism shifts analytical focus from the micro-level cognitive dynamics of knowledge and confidence and discourses to the level of political regimes shaping citizen motivation, as also discussed in section 2.4. Political regimes are understood as systems of rule that differ in their degrees of electoral competitiveness, institutional accountability, and openness to dissent (Linz & Stepan, 1996; Norris, 2014). The structural differences shape not only the formal adoption of Internet voting but also the motivational frames through which citizens make sense of such systems. As such, political contextual moderators condition the underlying logics that drive both the willingness and trust to use Internet voting. In this sense, political context anchors the operation of all other mechanisms discussed in this section, determining whether trust emerges as confidence in institutional reliability or as compliance with authority.

[2] The notion of distrust is not applicable to the entire PhD project and is introduced exclusively in one article, hence, it will be only locally defined.

For instance, in democratic regimes, citizens operate within a framework of political pluralism, legal accountability, and institutional transparency. Within such environments, trust in Internet voting tends to be constructed instrumentally. That is, individuals assess whether the technology fulfills normative expectations regarding electoral fairness, accessibility, and procedural reliability. The willingness to use Internet voting is motivated by perceptions of personal benefit, civic efficacy, and confidence in the system's capacity to deliver accurate and secure results (Carter & Campbell, 2011). Instrumental trust thus rests on a logic of individual reasoning, oriented toward performance evaluation and democratic self-expression (Tolbert & Mossberger, 2006).

In contrast, non-democratic regimes, such as electoral autocracies or hybrid systems, are characterized by limited political competition, reduced accountability, and a narrower public sphere. In these contexts, trust in Internet voting is more likely to reflect duty-based or norm-enforcing motivations. Citizens may relate to voting technologies not through evaluative reasoning but through frames of loyalty, obligation, or habitual compliance (Guriev & Treisman, 2020). Motivations in such regimes are often shaped by hegemonic narratives of state modernity, civic duty, or symbolic participation. The relationship to Internet voting is therefore less about system performance and trust in the technology, and more about affirming membership within a politically structured order (Reuter, 2020; Reuter & Szakonyi, 2021).

Theoretically, this distinction gives rise to several expectations. First, the logic of motivation, whether instrumental or duty-based, will vary systematically with regime type. Second, the source of trust differs: while institutional trust grounded in procedural accountability dominates in democracies, political alignment and regime legitimacy may act as functional equivalents in non-democratic contexts. Third, the use of Internet voting reflects these deeper motivational logics. In democracies, use is expected to follow from system credibility; in non-democracies, it may follow from normative compliance or political socialization. Lastly, while technological and institutional trust remain relevant across contexts, their meaning is filtered through regime-specific discourses. Trust in government, for example, may signify faith in democratic accountability in one case, and deference to centralized authority in another.

This mechanism thus emphasizes that trust in Internet voting is not only about the technology or the institutions that implement it, but also about the political regime that frames its legitimacy. Motivations and rationales are embedded in political structures, and understanding these differences is essential for theorizing how and why individuals engage with technologically mediated elections.

2.5.4. Institutional versus technological trust

The preceding sections have identified three mechanisms through which trust in Internet voting is formed: knowledge and confidence, discourses, and political regime context. Each mechanism implicitly engages with two foundational dimensions of trust, trust in institutions and trust in technology. This section brings these dimensions into direct focus, offering a conceptual synthesis of how

they operate independently and interactively to shape public perceptions and use of Internet voting.

Institutional trust refers to individuals' confidence in the organizations responsible for governance, including electoral commissions, government agencies, and political authorities. It reflects perceived legitimacy, transparency, accountability, and procedural competence (S. G. Grimmelikhuijsen & Meijer, 2014; Mishler & Rose, 2001; Perez & Ross, 2020). In the context of Internet voting, institutional trust reassures citizens that the voting process will be administered fairly, that their privacy will be protected, and that the outcomes will be honored. When direct technical evaluation is difficult or impossible, institutional trust allows citizens to delegate the responsibility for system integrity to authorized actors (Abdala et al., 2025; Toots, 2019).

Technological trust, by contrast, is directed toward the reliability and functionality of the system itself. It encompasses confidence in technical features such as software stability, encryption standards, verification mechanisms, and cybersecurity design (Carter & Bélanger, 2012; Lin, 2011; McKnight & Chervany, 2001). Technological trust is distinct from but not independent of institutional trust. For individuals with high levels of technical knowledge and confidence, technological trust may be constructed through direct understanding and evaluation of system performance. For others, it may depend on third-party endorsements or demonstrable transparency in system operation.

The relationship between institutional and technological trust is dynamic and often compensatory. Where institutional trust is strong, it can reduce the cognitive demand placed on individuals to understand the technical system in detail. Where technological design is robust, transparent, and verifiable, it can partially compensate for weaker institutional credibility (Abdala et al., 2025; S. G. Grimmelikhuijsen & Meijer, 2014). Yet these two forms of trust are rarely substitutable in full. Institutional trust frames how technological assurances are interpreted, especially in environments where system complexity exceeds most users' expertise. Likewise, even highly secure technical systems may fail to generate public confidence if they are embedded in institutions perceived as opaque, biased, or incompetent (Mishler & Rose, 2001; Toots, 2019).

The mechanisms discussed earlier reinforce this duality. The knowledge-confidence mechanism clarifies how technological trust may develop independently among technically literate individuals, while others rely on institutional trust. The regime-type mechanism shows that trust varies in form across political systems, with democratic institutions promoting evaluative trust and non-democratic ones relying more heavily on norm-enforcing legitimacy. The discursive mechanism further demonstrates how both institutional and technological trust are constructed in public narratives that frame the meaning of Internet voting. Across all three, institutional and technological trust appear not as isolated constructs but as interdependent foundations of legitimacy and usability.

In summary, these four mechanisms collectively illustrate how trust in Internet voting is contextually and cognitively constructed, influenced by individual knowledge, institutional credibility, technological assurance, and the broader environments in which these elements operate. As visualized in Figure 1, they

interact through two interdependent yet analytically distinct dimensions of trust: technological and institutional. Technological trust emerges from users' experiences with everyday digital services such as online banking, prescriptions, or taxation systems, where repeated successful usage builds confidence transferable to electoral technologies. Institutional trust, in contrast, originates from citizens' evaluations of the performance and integrity of government bodies, courts, elections, and the broader e-state infrastructure. Both dimensions converge at the individual level, where personal characteristics and prior experiences mediate how users interpret risks and reliability in digital elections. These micro-level dynamics unfold within contextual environments shaped by regime characteristics and prevailing public discourses. Regime features determine how authority, transparency, and accountability are institutionalized, while discourses circulating through media, expert debate, and political communication frame how Internet voting is collectively interpreted and justified. Together, these contextual variables condition the formation and maintenance of trust and explain its behavioral outcome, the actual use of Internet voting, thus linking individual-level characteristics, institutions, technology, and the sociopolitical context into a coherent framework for understanding trust in digital democracy.

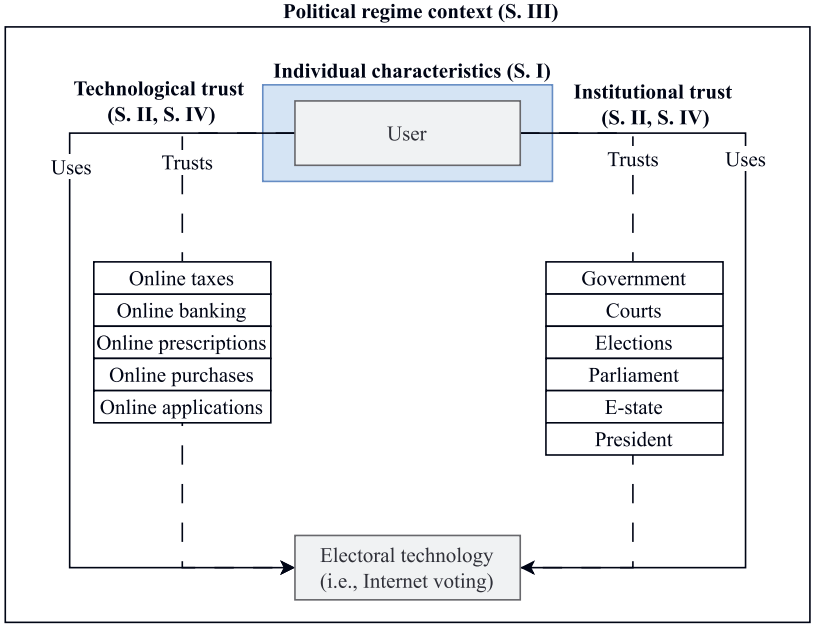

Figure 1. The dissertation's theoretical framework combines core notions of technological and institutional trust with contextual variables of the political regime and discourses. "S. #" in the parentheses indicates the study number within which the association is studied.

In short, the framework acknowledges generalized social trust as a background societal disposition that precedes and conditions more specific trust evaluations. Generalized trust refers to a diffuse expectation that others and collective institutions will behave in a predictable and non-opportunistic manner. Such trust is not primarily derived from evaluations of particular institutions or procedures but is rooted in historically embedded patterns of civic engagement and social cooperation (Putnam, 2001; Putnam et al., 1994). In this sense, generalized trust and consequent social capital constitute a baseline context within which citizens interpret institutional performance and the legitimacy of collective decision-making arrangements; hence, it is taken for granted within this project and not directly analyzed, but kept in mind.

Building on this societal foundation, the framework depicted in Figure 1 differentiates between institutional trust and trust in technology, both of which operate at a more specific level and are directly relevant for understanding attitudes toward Internet voting. These four studies operationalize a theoretical framework that views trust as a multi-level, dynamic construct shaped by individual knowledge and confidence, institutional performance, and the socio-political environment. This enriches the previous versions of technology-driven theoretical lenses. Now, Internet voting, or any other state-endorsed technology, is tied to individuals, political and discursive contexts, as well as the underpinning mechanisms of trust.

3. SCOPE AND CONTRIBUTION OF THE DISSERTATION

Figure 2 contains the core logic of the PhD project structure. This order of studies allows for the development of the argument cumulatively: from the individual characteristics of technology users and their discourses to the regime-driven features of trust formation, as well as the face-to-face comparison of technological and institutional trust and their embedded variables.

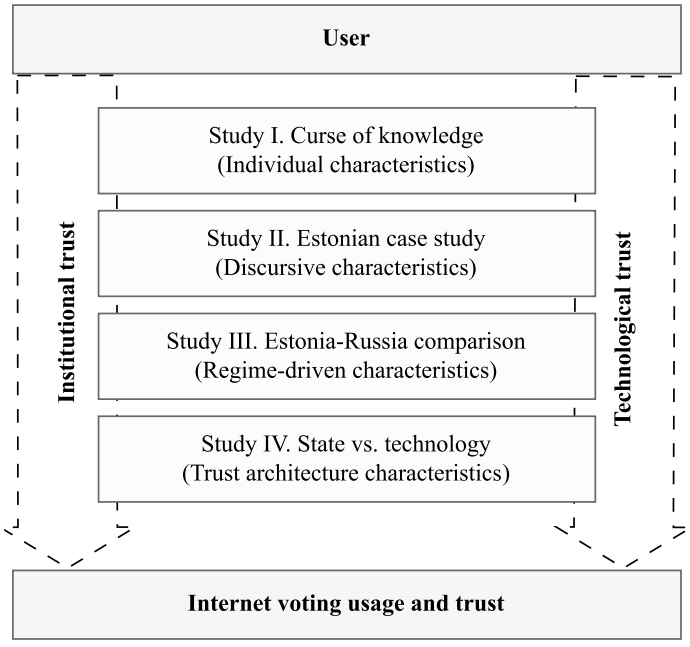

Figure 2. The logic of studies within the PhD project

The primary objective of this dissertation is to analyze the mechanisms shaping trust in Internet voting by examining how individual, institutional, and technological factors interact within specific contextual environments. Rather than treating trust as a unidimensional construct or as an outcome of technological performance alone, the dissertation conceptualizes it as a dynamic sociotechnical phenomenon that emerges from the interplay between individual knowledge and experience, institutional credibility, and technological confidence. These interactions are further conditioned by contextual variables of political regime characteristics and public discourses, which define how citizens interpret the legitimacy and reliability of digital electoral systems. By adopting this multidimensional approach, the dissertation advances an integrative understanding of how trust in Internet voting is formed, maintained, and challenged.

Important gaps remain in understanding how these institutional and technological factors interact with individual-level determinants such as knowledge, perceived competence, and prior digital experience. Furthermore, limited attention has been paid to the contextual conditions that shape these relationships –

particularly the influence of regime characteristics and discursive framings of technology and authority. This dissertation addresses these gaps by systematically examining how institutional legitimacy, technological assurance, and individual-level features intersect across different contexts. Drawing primarily on Estonia's extensive experience with Internet voting, it demonstrates how these mechanisms co-produce citizens' trust perceptions and usage behaviors, offering generalizable insights into the governance of trust in digital democracies.

To provide a comprehensive analysis, the dissertation approaches trust in Internet voting through two complementary strategies. Some of the empirical articles focus on Estonia, a consolidated democracy with the longest history of legally binding Internet voting. This extensive experience makes Estonia an ideal case for exploring the long-term dynamics of trust formation. Another angle is comparative analysis, juxtaposing Estonia with Russia, a competitive autocracy that has recently introduced Internet voting under vastly different political conditions. This enables a contextualized examination of the diverse mechanisms through which trust is constructed and contested across political regimes.[3]

Hence, the dissertation's contributions to academic discourse and empirical understanding can be summarized in three key areas:

- Comparative contribution: The research examines trust in Internet voting across diverse political and cultural contexts, assessing how trust-building mechanisms differ between democratic and autocratic regimes. It evaluates the role of institutional legitimacy, technological security, and political incentives in shaping attitudes toward Internet voting.
- Theoretical contribution: This dissertation contributes to the theoretical understanding of trust in digital governance by offering a structured account of how trust in Internet voting emerges from the interplay among institutional credibility, technological assurance, and individual-level characteristics. Rather than treating trust as a unified or static construct, the study disaggregates it into the analytically distinct yet interdependent forms of institutional trust, technological trust, and user features and opinions. By examining how these dimensions interact under varying political and informational conditions, the

[3] Even though the Estonia-Russia comparison is not the corner piece of the dissertation, the case selection is taken seriously. While these two cases differ profoundly in terms of institutional design, electoral integrity, and public accountability, such contrast serves an analytical purpose rather than posing a limitation. The comparison follows a most-different systems logic, where the extreme variation in political context allows for the isolation of core mechanisms of trust formation that persist irrespective of regime type (Anckar, 2008). Instead of undermining comparability, these contextual contrasts highlight how the same technological instrument of Internet voting can acquire distinct political meanings, institutional roles, and legitimacy functions. In democratic settings like Estonia, Internet voting operates as an extension of institutional reliability, whereas in autocratic contexts such as Russia, it may serve as a tool of regime legitimation. Recognizing these divergences transforms contextual difference into an empirical advantage, unpacking the variety of trust under different political conditions.

dissertation refines existing models of trust formation and clarifies the mechanisms through which trust and distrust are constructed, negotiated, and translated into behavioral engagement.

- Methodological contribution: By employing a mixed-methods approach, this dissertation weaves together several strands of evidence. First, large-N post-election surveys conducted in Estonia (2021, 2023) and Russia (2021) establish the prevalence of trust and identify its socio-demographic and regime-specific predictors. Second, elite interviews with Estonian election officials, cyber-security specialists, and journalists explain the institutional logics and transparency claims that frame public debate. Third, a Q-methodology study invites citizens to sort interview-derived statements, thereby mapping the subjective discourses through which technical safeguards and political trust are interpreted. Juxtaposing these complementary lenses links micro-level attitudes, meso-level narratives, and macro-level regime incentives, providing a more complex final image. At the same time, the design offsets the method-specific blind spots whereby surveys quantify but cannot contextualize, interviews reveal institutional rationales but not prevalence, and Q-sorting foregrounds interpretive frames while sacrificing representativeness. Their integration thus yields a resilient, multi-level explanation of how citizens come to trust or withhold trust from Internet voting systems.

In studying trust in Internet voting, this dissertation assesses the mechanisms that foster, challenge, or undermine trust, providing new insights into how digital technologies interact with electoral legitimacy. Trust is operationalized across multiple dimensions, including institutional trust, technological confidence, and knowledge-based self-reliance, enabling a nuanced analysis of how different publics engage with Internet voting.

The general research question of the project is the following:

What drives the formation of trust in Internet voting, and how do individual, institutional, technological, and regime-level factors shape both trust and the actual usage of Internet voting systems across different political contexts?

To operationalize this broad question, the dissertation will address the following specific research questions:

Study I

The role of knowledge and confidence in trust formation: This study investigates how technical knowledge and digital literacy shape confidence in Internet voting in Estonia. It examines whether technically informed voters rely less on trust and more on the confidence derived from their own understanding of the system.

The study operationalizes the conceptual distinction between trust, understood as reliance on institutional integrity under conditions of uncertainty, and

confidence, understood as reliance on personal knowledge and perceived control, as developed in this dissertation's theoretical framework. The analysis tests whether higher technical literacy conditions the mechanisms through which voters form positive expectations toward Internet voting, shifting the basis of their decision-making from trust to knowledge-based confidence. In doing so, it helps explain how individual-level factors, such as technical education, interact with trust signals to shape the use of Internet voting technologies.

RQ: *How does technical knowledge about Internet voting moderate the reliance on trust versus confidence?*

Study II

Expert and public perceptions of trust and distrust in Internet voting: This study employs a mixed-methods design, combining expert interviews and Q-methodology to examine how trust and distrust in Internet voting are constructed in Estonia. The expert interviews were used to identify the main themes and statements reflecting professional concerns about security, transparency, and institutional accountability, which then formed the basis for the Q-method experiment with citizens. The Q-study reveals three existing discourses: institutional trust and practical optimism, emphasizing positive experiences and confidence in Estonia's digital governance; concerns over transparency and accessibility, focusing on communication and inclusiveness; and skepticism about security and human vulnerabilities, reflecting fears of manipulation and insufficient oversight. Together, these discourses demonstrate that trust in Internet voting is socially and discursively produced, shaped not only by system performance but also by how political debates and public communication frame its legitimacy.

RQ: *How are trust and distrust in Internet voting perceived by citizens in Estonia, and what existing discourses structure these perceptions?*

Study III

Comparing trust in Internet voting across different regime settings: This study examines how political regime conditions shape the mechanisms through which trust in Internet voting is formed. Using Estonia and Russia as contrasting examples of liberal democracy and electoral autocracy, this analysis explores how trust emerges through either procedural transparency and institutional credibility (as in Estonia) or state-driven legitimation and duty-based mobilization (as in Russia).

RQ: *What accounts for trust in Internet voting under different political contexts?*

Study IV

Institutional vs. technological trust in Internet voting: This study examines the relationship between trust in political institutions and trust in Internet voting technologies, assessing which factor plays a greater role in shaping confidence in Internet voting. It highlights that, in a democratic setting, institutional trust remains the dominant factor in influencing voter confidence.

RQ: *Which trust, institutional or technological, has a higher impact on the trust and usage of Internet voting?*

By addressing these research questions, the dissertation contributes to the broader fields of digital democracy, electoral governance, and political trust. It offers a comparative framework for understanding how Internet voting is perceived and accepted under different political conditions, emphasizing that trust in electoral technologies is not simply a function of regime type but a product of layered institutional, technological, and discursive configurations (Abdala et al., 2025). This approach advances beyond earlier studies that either treated trust primarily as an institutional outcome (Mishler & Rose, 2001; Norris, 2014) or emphasized technical functionality in isolation (Alvarez et al., 2011; Carter & Bélanger, 2012). The dissertation demonstrates that trust and usage are shaped by inter-dependent mechanisms, including user knowledge and confidence, regime-specific motivational logics, and publicly circulating narratives, that were often overlooked in prior models. It thus reframes Internet voting trust as a contingent, multilevel construct, highlighting the strategic role of state actors, system design, and legitimacy narratives in shaping adoption and resistance (Duenas-Cid & Calzati, 2023; Ehin & Solvak, 2021; Erb et al., 2023; Wang, 2016).

This research has direct implications for policymakers, electoral commissions, and technology developers. By identifying the factors that shape trust in Internet voting, it provides recommendations for enhancing transparency, security, and public trust in Internet-based electoral processes. In democratic settings, this involves reinforcing procedural safeguards and public engagement, whereas in non-democratic contexts, it requires addressing state-driven trust narratives and their implications for electoral legitimacy.

Overall, this dissertation contributes to a deeper understanding of how trust in Internet voting is built, maintained, or eroded, offering insights into the political and technological conditions that influence Internet voting participation. Integrating perspectives from political science, digital governance, and electoral studies provides a comprehensive framework for assessing the legitimacy of Internet voting across diverse governance models. More detailed yet summarizing information is provided in Table 1.

Table 1.Topics, dependent variables, and main expectations of the publications

	I	II	III	IV
Topic	Role of technical knowledge in trust/confidence in Internet voting in democracies.	Discourses constructing trust and distrust in Internet voting in democracies.	Trust in Internet voting in democratic and autocratic political regimes.	Role of institutional and technological trust in Internet voting in democracies.
Dependent variable	Usage of Internet voting (10-point scale recoded into binary).	Trust profiles in Internet voting (factor scores from Q-methodology) and discourses based on thematic coding of post Q-sort interviews.	Trust in Internet voting (10-point Likert scale in Estonia, 7-point scale in Russia).	Trust (measured on a 10-point scale recoded into binary) in and usage of Internet voting (ordinal 4-point scale recoded into binary variable).
Independent variables	• Technical knowledge • Trust in technology's performance • Trust in government • Trust in Internet voting • Confidence	Not applicable in quantitative terms, but in quantitative terms it would be the various backgrounds of the participants.	• Institutional trust (trust in elections, government, electoral authorities) • Features of the Internet voting • Political alignment (winner effect) • Perceived fairness of Internet voting	• Institutional trust composite index (e.g., trust in government, elections, e-state and 4 other sub-indicators) • Technological trust composite index (e.g., trust in online banking and 5 other sub-indicators)
Control variables	• Age • Gender • Education • Language spoken at home • Left-right self-position • Frequency of Internet usage	• Prior exposure to Internet voting technology (13 respondents used Internet voting and 12 did not) • No selection based on age, gender, education	• Age • Gender • Education • Income • Political affiliation	• Technical knowledge • Age • Gender • Education
Expectations	Higher technical knowledge leads to lower reliance on trust factors and greater reliance on confidence.	Trust and distrust in Internet voting are expected to emerge through competing narratives in public discourse, with institutional actors emphasizing system security and reliability, while critics focus on transparency, communication shortcomings, and the political risks surrounding digital elections.	Institutional trust is the primary predictor of trust in Internet voting in Estonia; in Russia, political alignment with the ruling party matters more (winner effect).	Institutional trust has a stronger impact on Internet voting adoption than technological trust.

The aim of Study I is to assess how individual-level characteristics influence the use of Internet voting. The primary focus is on technical knowledge. The study examines whether individuals with greater technical knowledge are more likely to rely on personal confidence in the technology rather than on trust-based factors such as technology performance or institutional trust when deciding to use Internet voting. The research is based exclusively on the Estonian population's experience with Internet voting, yet this case study adds to the general understanding of how trust-building mechanisms may differ across cohorts. The study examines the relationship among a limited number of variables: trust in performance, trust in government (as an operationalization of institutional trust), trust in Internet voting, confidence in technology's performance, and technical knowledge. The logic is to check the niche mechanism of technology usage under the rationale of trust or confidence, with the expectation that those with a higher degree of technical knowledge tend to be confident in the technology and hence use it due to their expertise-based confidence. In comparison, those with lower technical knowledge have to use mediating entities (such as the government or technology itself) to adopt and use Internet voting. As a side comment, the executed design oversimplifies the relationship and presents a nearly linear association between trust and knowledge. The initial design assumed a reversed U-curve association: the highest degree of trust is reached at the "moderate" knowledge level, while the lowest and highest knowledge levels lead to lower degrees of trust. This assumption could not be tested with existing data, hence, the more straightforward alternative was selected.

Study II explores trust and distrust in Internet voting in Estonia through a qualitative lens, employing Q-methodology with citizens. The study builds on statements derived from prior expert interviews, which served as input for constructing the Q-sort but were not analyzed independently. Unlike the other studies in this dissertation that focus on isolating specific predictors, this one adopts a discourse-centered approach. Its primary goal is to reveal how trust is socially and discursively constructed, capturing the underlying narratives and reasoning patterns through which citizens interpret the Internet voting process. The analysis identifies distinct discourses that emphasize different sources of trust and distrust, including prior experiences with digital services, perceptions of institutional performance, and concerns about security and political influence. Thus, the study conceptualizes trust and distrust not as direct reflections of technological attributes or institutional quality, but as outcomes of meaning-making processes shaped by societal context, generational outlooks, and individual interpretations of electoral integrity and technological risk.

Study III also addresses the nature of trust in Internet voting. However, in this iteration, the comparative angle is introduced. By comparing the mechanisms of trust in democratic Estonia and autocratic Russia, civic duty was expected to be the primary driver of trust in a non-democratic regime. In contrast, in democracies, Internet voting is incentivized by the technology's instrumental features, such as anonymity, security, and privacy. This viewpoint not only highlights the differences in usage and trust-building associated with government-affiliated

technologies but also reveals distinct intentions behind the new mode of voting implementation.

Finally, Study IV revisits the relationship between technological and institutional trust introduced in earlier studies but adopts a more rigorous methodological approach. Unlike Study I, which uses single-item variables to capture trust dimensions, this research operationalizes technological and institutional trust as composite indices derived from multiple indicators. The rationale for this methodological refinement is twofold: first, to acknowledge that trust in complex domains like digital governance cannot be adequately measured by single indicators; second, to test whether institutional trust systematically exerts a greater influence on Internet voting trust and usage than technological trust, especially in contexts where citizens have extended exposure to digital voting systems. Consequently, the study hypothesizes that institutional trust remains the dominant factor influencing both the adoption and sustained use of Internet voting, even when accounting for demographic characteristics and technical literacy.

4. DATA AND METHODS

The dissertation employs a mixed-method research design to investigate how individual, institutional, and technological mechanisms interact within different contextual environments to shape trust in Internet voting. Rather than combining methods to achieve methodological diversity, each empirical study is designed to capture a specific dimension of the trust-construct outlined in the theoretical framework. Quantitative analyses of survey data examine how individual features, confidence, and institutional trust influence the use of Internet voting. Q-methodology uncovers the discursive structures through which citizens interpret and express trust and distrust. Expert interviews provide insight into the institutional logic and communicative practices that frame Internet voting within the broader governance system. Finally, the comparative perspective between Estonia and Russia enables the analysis of how regime characteristics and discursive contexts condition the formation, maintenance, and contestation of trust in digital elections.

The methodological framework is designed to capture both macro-level (institutional and political) and micro-level (individual knowledge and technological confidence) influences on trust in Internet voting.

Three (I, III, IV) of the four empirical analyses comprising the dissertation employ Estonian post-election survey data from the 2021 (national) and 2023 (local) elections. Study III also includes similar post-election survey data, but for the Russian national 2021 elections. The approach to making the questionnaire and thus the data comparable was as follows: a battery of questions on trust was extracted from the Russian survey, translated into English and Estonian, and retained in Russian for the 2023 post-election survey in Estonia. This approach provided the same dimensions for the answers and constitutes a unique dataset.

Table 2. Data and methods of publications

	I	II	III	IV
Data	Post-election survey data from Estonia (2021, 2023), sample size ~1000.	Q-sorting study (2023) with 26 respondents, based on statements from 16 interviews with Estonian experts.	Comparative survey data from Estonia (2023, ~1000 respondents) and Russia (2021, ~1600 respondents).	Post-election survey data from Estonia (2021, 2023), sample size ~1000.
Method	Binary logistic regression with interaction terms and predictive margins.	Q-methodology combining factor analysis and qualitative interpretation of discursive factors via thematic coding.	Multivariate linear regression.	Exploratory Factor Analysis and Confirmatory Factor Analysis, linear regression, and logistic regression.

The second paper's research (II) used a different data-gathering mechanism. Initially, 16 semi-structured expert interviews were conducted in Estonia with the election officials, policymakers, and cybersecurity experts involved in the administration and oversight of Estonia's Internet voting system. Once the interviews were transcribed, 36 statements were extracted and used in the on-site Q-methodology with 25 respondents in Estonia. Participants are asked to rank these statements according to their level of agreement, enabling the identification of distinct attitudinal profiles. Factor analysis is then applied to extract clusters of trust orientations, distinguishing between institutional trust-based confidence, technological optimism, and security-focused skepticism.

4.1. Alternative techniques for exploring the relationships

Despite the variety of quantitative methods employed in the project (e.g., factor analysis and regression-based techniques), some alternatives were not selected for the analysis. This section outlines several such alternatives and explains their exclusion on theoretical or practical grounds.

One basic yet often underutilized diagnostic is correlation analysis. In Study IV, this approach was used as a preliminary step to assess association and its direction across the variables. The correlation matrix, as an output, shows how institutional trust is associated with trust in Internet voting. However, correlation analysis alone does not account for confounding variables, measurement error, or simultaneous effects, which were among the core rationales for the initial research design. It cannot distinguish between direct and spurious relationships, nor can it test statistical significance in a multivariate context. For these reasons, it serves as a valuable descriptive but insufficient inferential technique in isolation. The same logic applies to Studies I and III. The initial "sanity" check correlation analysis is perfectly suited, but it does not provide in-depth answers and should not be used to validate or falsify the hypotheses.

A second notable alternative is Qualitative Comparative Analysis (QCA). QCA is a set-theoretic method ideal for exploring configurations of causal conditions across cases rather than assessing effects (C. Q. Schneider & Wagemann, 2012). In the context of Study III, which, in other words, asks what factors drive trust in Internet voting in democratic vs. autocratic contexts, QCA could have been employed to assess how combinations of institutional context, perceived anonymity, convenience, fairness, and regime type jointly condition trust in Internet voting. Prior research has used QCA in comparative governance and digital participation studies to great effect (Breaugh et al., 2023; Cruz, 2023; De Blasio & Selva, 2019; Li et al., 2024). However, QCA is better suited to small-N comparative case studies or most-different/similar-system designs, and its reliance on dichotomization may oversimplify graded attitudes such as trust. In other terms, even though Russia and Estonia do constitute a sample of most-different-system-design cases, converting the variables to binary (e.g., trust in Internet voting / the absence of trust in Internet voting) for the crisp-set approach

would result in the loss of the variance across the cases, which was so meticulously extracted with the help of surveys. An alternative method would be preserving the graduated nature of the survey answers within the fuzzy-set logic, yet the calibration for the cut-off points would be cumbersome and excessive (e.g., in Estonia, the trust-related answers range from 0 to 10, the answer of 7 entails what exactly? Does the respondent have a relatively high trust degree, but how much higher is it in comparison to 6 or 8? etc.). That is why the decision was made in favor of regression models for Study III and other quantitative research.

A final methodological consideration raised during discussions with the supervisory team concerns the use of Structural Equation Modeling (SEM) as a widely recognized alternative analytical strategy. SEM is a technique that enables the simultaneous estimation of latent constructs (such as institutional and technological trust) and the structural relationships among them. It has been extensively applied in studies of public trust in e-government and technology adoption (Abu-Shanab, 2014; Chen et al., 2023; Luo et al., 2024, p. 202; Wong et al., 2023). In the context of Internet voting, SEM could be used to model not only the direct effect of trust on usage behavior but also how trust in political institutions might be shaped by technical competence and, in turn, influence the likelihood of adopting Internet voting technologies. Also, in Study I, we have added an SEM version of the same analysis, which showed the same results.

However, the application of SEM in every study in the present research context is constrained by both data structure and sample size. SEM assumes multivariate normality and is particularly sensitive to missing data and the ordinal nature of variables, both of which characterize the current dataset (Kline, 2011). For example, in the most recent wave of the Estonian post-election survey, the total sample included approximately 1,000 respondents, of whom only about 500 reported voting via the Internet. Among those, roughly 350 provided complete responses to all key indicators, including education, technical literacy, and multiple dimensions of trust. This effectively reduces the usable sample to approximately one-third of the full dataset, thereby undermining the statistical power required for reliable SEM estimation. Additionally, the model's complexity and the risk of non-convergence further limit the feasibility of SEM in this context.

Nonetheless, within the five-year project, I obtained enough theoretical and practical knowledge on the method's application, and, in theory, SEM remains a valuable analytical framework that could be applied to the empirical design of Study IV to deepen the understanding of the interplay between institutional and technological trust, once the data limitation issues are fixed. Conceptually, SEM enables the simultaneous estimation of measurement and structural models, where latent constructs, such as institutional trust and technological trust, are represented by multiple observed indicators. These latent variables could then be modeled as predictors of trust in and use of Internet voting, while controlling for socio-demographic and attitudinal covariates. This approach would enable the assessment of indirect effects, for instance, whether institutional trust enhances technological trust, which in turn mediates the likelihood of using Internet voting.

Additionally, the composition of the technological and institutional trust indices could be omitted. Yet, the acknowledgement that SEM is a valid tool relevant to some of the project's study designs does not undermine the use of the selected tools.

4.2. Methodological limitations of the data sources in question

Now the alternative methods have been presented and their irrelevance to the methodological designs are justified, the final part of this section will introduce limitations that should be acknowledged to contextualize the findings appropriately. Some of the comments are deduced from the journal reviewers' feedback.

4.2.1. Quantitative data

One of the core limitations of the survey data used in Studies I, III, and IV is the reliance on self-assessed ordinal measures for key constructs such as technical knowledge and trust (i.e., trust in Internet voting, political trust, and technological trust). Respondents were asked to rate themselves or their beliefs on Likert-type scales, which introduces two methodological challenges. First, ordinal measures lack interval properties, and their treatment as continuous variables in linear regressions may introduce distortions in effect size and inference (Agresti, 2010; Norman, 2010). Second, and more critically, self-assessment measures are vulnerable to subjective bias and inter-respondent inconsistency. For instance, two individuals with comparable technical skills may rate themselves differently (e.g., one choosing 4 and the other 5 on a 5-point scale), introducing random measurement error that cannot be statistically corrected. During the doctoral years, while tinkering on the next iteration of the survey, there was a proposal to introduce more "feasible" indicators of technical knowledge, for instance, "Have you ever written a script on Python?" that would correspond to 4. Yet, no consensus was reached, and the question format remained intact.

Ideally, constructs such as technological knowledge would be assessed using a validated instrument, such as the Affiliation to Technology Interaction (ATI) scale (Attig et al., 2018; Franke et al., 2019), which offers better psychometric properties and enables cross-sample comparability. Similarly, constructs such as technological and political trust would benefit from structured instruments, such as the Human-Technology Confidence Scale (HTCS) (Gulati et al., 2019; Merritt et al., 2013) or multi-item trust batteries validated in prior political science or HCI research. The absence of such validated instruments limits the internal reliability of the measurement model and complicates the interpretation of subtle gradations in trust and knowledge levels. Nonetheless, the current approach remains analytically viable and informative, particularly in the absence of standard scales tailored for the specific context of Internet voting. Self-assessment items, while imperfect, offer a pragmatic way to capture individuals' subjective perceptions, which are crucial determinants of behavior in technology use.

Secondly, harmonization challenges across survey waves limit the potential to examine whether the observed mechanisms of trust formation remain stable over time. As summarized in Table 2, Studies I, III, and IV rely exclusively on survey data from 2021 and 2023, as only these most recent waves include items consistently worded to capture key trust constructs. This restricts the possibility of conducting longitudinal analysis. Although temporal comparison is not a primary aim of the dissertation, it would have provided valuable insights into the stability and durability of trust mechanisms. Furthermore, although another election took place in 2024, the corresponding post-election survey was not fielded due to organizational constraints. As a result, the project draws on two data waves out of a possible fifteen since the introduction of Internet voting in Estonia in 2005. While this is a notable limitation, it lies beyond the control of the research design and must be regarded pragmatically as a constraint inherent to the available data landscape.

Finally, nonresponse and missing data disproportionately affect the subpopulation of i-voters who completed the full battery of relevant items. This reduces the effective sample size and statistical power for multivariate analysis, particularly when examining subgroups or interaction effects. Yet, the nature of the phenomenon is treated in the same way as the non-homogeneous survey data's availability.

4.2.2. Qualitative data

The qualitative strand, comprising expert interviews and Q-methodology, is subject to limitations in sample size and linguistic scope. Expert interviews were conducted using purposive sampling to ensure variation across key stakeholder groups, including election officials, cybersecurity professionals, and journalists. While this approach effectively captures elite perspectives and institutional framings, it does not aim to represent public opinion. Moreover, due to the researchers' limited proficiency in Estonian, only English-speaking experts were included, potentially excluding relevant voices from local professional communities.

Language constraints similarly limit the Q-methodological component of the study. All respondents were English-speaking individuals physically based in Tartu. While Q-methodology prioritizes discursive diversity over statistical representativeness (McKeown & Thomas, 2013; Watts & Stenner, 2012), this recruitment strategy may have biased the sample toward more educated, internationally oriented, and digitally literate individuals. Such profiles are more likely to hold favorable views of Internet voting and may underrepresent discourses of skepticism, particularly among older, rural, or Estonian-speaking nonusers. That said, the sample was not composed exclusively of young people, as the mean age was 38, and the median was 39. Nevertheless, the reliance on English-speaking urban residents may have filtered out alternative framings of trust and distrust present in other segments of the electorate.

5. MAIN FINDINGS

5.1. Summary of the studies

The dissertation's main findings are presented in two stages. First, each of the four empirical studies is summarized individually, highlighting their key contributions to understanding trust in Internet voting. Second, the overarching theoretical and empirical insights are synthesized to clarify how the dissertation advances knowledge in the field of digital electoral governance in regard to the electorate's behavior.

Study I, "*I Know, Therefore, I Trust? quantitatively modelling how knowledge shapes the reliance on trust and confidence in the case of internet voting usage in Estonia,*" examines how individual technical knowledge conditions the mechanisms through which citizens develop trust and confidence in Internet voting. Using pooled post-election survey data from the 2021 local and 2023 parliamentary elections in Estonia, the study demonstrates that technical knowledge moderates the relationships among trust, confidence, and Internet voting use. The results show that confidence in the system is the decisive factor among respondents with high technical knowledge, substantially increasing the likelihood of Internet voting. By contrast, institutional trust exerts a weaker, less consistent effect, emerging as significant only among voters with higher levels of knowledge. Both trust in system performance and trust in Internet voting itself, however, show robust positive effects across the electorate. These findings indicate that knowledge does not replace trust but reshapes its foundation: individuals with greater technical literacy rely more on knowledge-based confidence, while others depend on institutional assurances. **The study thereby refines the conceptual distinction between trust and confidence, explaining how cognitive factors and institutional credibility jointly determine engagement with digital elections.**

Study II, "*Trust and Distrust in Internet Voting: A Mixed-Methods Examination of Expert Insights and Public Perceptions in Estonia,*" takes a qualitative approach to examine trust and distrust in Internet voting through a Q-methodology based on expert interviews and citizen sorting tasks. The analysis identifies three dominant attitudinal discourses in Estonia: (1) institutional trust-based confidence, (2) technological optimism, and (3) security-focused skepticism. While both institutional performance and technological experience provide grounds for trust, distrust primarily stems from political reasoning – particularly perceptions of bias, lack of transparency, or poor communication regarding the voting system. **The study thereby demonstrates that trust in Internet voting is not merely a matter of system design but is socially and discursively constructed through diverse experiential and political pathways.**

Study III, "*Trust in Online Voting under Different Regime Settings: Evidence from Public Opinion on Online Voting in National Elections in Estonia and Russia,*" introduces a comparative perspective, analyzing post-election surveys from Estonia and Russia to explore how trust in Internet voting functions under

democratic and autocratic regimes. The findings reveal that in democratic Estonia, trust is closely linked to institutional performance and perceptions of procedural integrity. In contrast, in autocratic Russia, use and trust in Internet voting are largely shaped by non-instrumental motives, such as civic duty and political alignment with the ruling party (the so-called "winner effect"), which is corrupted under autocratic regimes due to a tilted electoral playing field. **These findings underscore that while regime type sets important contextual parameters, it does not deterministically shape trust in electoral technologies; instead, trust emerges from specific motivational logics and legitimacy narratives embedded within each regime** (Guriev & Treisman, 2020; Putnam et al., 1994; Reuter & Szakonyi, 2021).

Study IV, "*State versus Technology: What Drives Trust into Internet Voting, Institutional or Technological Trust?,*" revisits the Estonian case with an enhanced methodological framework, constructing composite indices for institutional and technological trust. Using survey data from 2021 and 2023, the study finds that institutional trust is a stronger predictor of both trust in and usage of Internet voting than technological trust. This pattern holds across demographic subgroups and remains robust after controlling for education and age. The study also confirms Study I's results, which show that greater technical knowledge is associated with a higher usage rate. **These findings refine previous assumptions by demonstrating that institutional trust is not merely a proxy for general optimism but a key determinant of Internet voting legitimacy.**

Taken together, the four studies provide a multi-layered account of how trust in Internet voting is formed, maintained, and contested. First, the research reveals that trust in Internet voting is not monolithic; it is mediated by technical knowledge (Study I), embedded in public discourse (Study II), shaped by regime incentives (Study III), and operationalized primarily through institutional trust (Study IV). Second, the dissertation underscores the contextual dependency of trust mechanisms. Users of the technology in the same country might express contradictory narratives tied to various arguments, indicating that politics and technology are heavily intertwined. Additionally, democratic and autocratic regimes rely on qualitatively different trust-building strategies, ranging from transparency and legal guarantees to symbolic appeals and loyalty narratives. Viewed together, the studies thus validate one another across methods and contexts, yielding precise new knowledge: trust in Internet voting emerges from the interaction among institutional credibility, technological assurance, and contextual framing, with institutional trust functioning as the central integrative force linking individual confidence, social discourse, and the political regime.

Ultimately, the findings demonstrate that institutional trust consistently outperforms technological confidence as a predictor of both trust in and use of Internet voting, at least in a highly digitalized environment with high exposure to Internet voting, such as Estonia. This highlights the critical role of electoral authorities, government transparency, and legitimacy in fostering digital participation. In other words, the results expose a central puzzle of digital democracy: even in a technology-intensive voting mode, it is not the technical system itself

that primarily generates trust, but rather the surrounding institutional environment (e.g., transparency, accountability, and perceived fairness) that enables citizens to extend confidence to the technology.

5.2. Synthesis of main findings

Across the four studies, several consistent insights have emerged. Study I demonstrated that the decision to use Internet voting depends primarily on the interaction between knowledge and confidence. Voters with high technical literacy rely more on their confidence in the system, while those with limited knowledge rely more on broader institutional trust. This finding empirically substantiates Simmel's (1950) and Giddens's (1990, 1991) distinction between trust and confidence, offering evidence that their interplay varies across levels of individual competence.

Study II, and its short AMCIS version, further deepened understanding of the discourses of trust and distrust. Using expert interviews and Q-methodology, the study identified three stable discourse clusters: (1) institutional trust and practical optimism, where habitual experience reinforces confidence in both institutions and technology; (2) concerns over transparency and accessibility, where trust is conditional on procedural openness and clear communication; and (3) skepticism about security and human vulnerability, where distrust arises from political polarization and communication gaps. These findings corroborate the argument that trust in Internet voting is sustained not only by performance but also by the discursive normalization of digital elections within public debate (Bodó, 2021; Duenas-Cid & Calzati, 2023).

Study III expanded this analysis to the macro-political level by comparing Estonia and Russia. Despite shared post-Soviet origins and technological infrastructures, the two countries exhibit radically different trust logics. In Estonia, trust in Internet voting is instrumentally grounded in perceptions of efficiency, convenience, and procedural fairness. In Russia, where electoral competition and accountability are limited, trust is largely non-instrumental, anchored in civic duty and regime loyalty rather than in system performance. This contrast confirms that regime type acts as a contextual moderator rather than an independent causal mechanism (Putnam et al., 1994), consistent with Norris's (2014) typology of electoral integrity and Reuter's (2020) work on authoritarian participation.

Finally, Study IV quantified the interplay between institutional and technological trust, revealing that institutional trust remains the dominant driver of both trust in and use of Internet voting. Technological trust, while significant, functions largely as a reinforcing factor dependent on the perceived reliability of institutions. This pattern confirms Luhmann's (1979) thesis that institutional frameworks reduce the complexity of technological systems, allowing citizens to engage with technologies they only partially understand.

5.3. Broader-scope findings

Taken together, the empirical studies included in this dissertation converge on a consistent set of findings regarding the formation and functioning of trust in Internet voting. Although the individual articles rely on different data sources, analytical strategies, and methodological traditions, they point in the same substantive direction. This convergence is not accidental but reflects a deliberate triangulation strategy across cases, methods, and analytical levels. Empirically, the project draws on evidence from both Estonia and Russia, allowing the analysis to capture variation across contexts with markedly different levels of generalized societal trust, institutional capacity, and political contestation. Methodologically, the dissertation combines large-scale survey data and statistical modeling with qualitative interviews and Q-methodology, enabling the examination of trust from both behavioral and discursive perspectives. Across these different empirical settings and methodological approaches, the results consistently demonstrate that trust in Internet voting cannot be reduced to a single dimension but that it emerges from the interaction between institutional evaluations and technology-specific perceptions.

Taken together, the four studies do not merely replicate similar findings using comparable tools but validate one another through systematic variation in methods, data (to a lesser extent), and empirical contexts. The robustness of the results, therefore, does not rest on the internal consistency of a single methodological approach but on their repeated confirmation across distinct analytical designs, ranging from statistical modeling to discursive and qualitative inquiry. This cumulative validation emerges from the combined configuration of cases, methods, and theoretical lenses rather than from any individual study in isolation. In this sense, the dissertation constitutes a coherent research program articulated through four interlinked empirical investigations. The convergence of findings across these studies increases confidence in their broader scope and theoretical relevance, allowing conclusions about trust in Internet voting that extend beyond the specificitiesof any single dataset, method, or national context.

At a more substantive level, the findings reveal that trust and distrust follow distinct logics and are grounded in different sets of arguments. Quantitative analyses demonstrate that confidence and trust-related variables affect Internet voting adoption in distinct ways depending on voters' knowledge levels, while qualitative and Q-methodological evidence reveals that trust and distrust are articulated through qualitatively different discourses rather than opposite ends of a single continuum. Importantly, these patterns appear consistently across methods and cases, reinforcing the robustness of the conclusions. The Estonian case illustrates how high levels of institutional capacity and generalized trust enable trust in electoral technology to stabilize over time, whereas the Russian case highlights how lower societal trust and politicized institutional environments constrain the emergence of technology-specific trust, regardless of technical design.

Beyond the specific case of Internet voting, the cumulative findings suggest that this dissertation can serve as a conceptual and methodological backbone for future research on trust in digital governance more broadly. While Internet voting constitutes a particularly demanding case due to its political sensitivity and technical opacity, other digital governance technologies may exhibit different trust patterns depending on their visibility, reversibility, and perceived risks. The framework developed here offers a reference point for analyzing such variation by explicitly distinguishing between institutional trust and technological trust, and by treating trust and distrust as analytically distinct processes rather than as mirror images. The works by Alishani and Homburg (2025) and Abdala and colleagues (2025) present different results, which contrast with the findings of this PhD project, which unpacks trust and the use of various technologies through different methods.

Ultimately, the dissertation provides a transferable research template for investigating trust in complex sociotechnical systems. By integrating quantitative modeling with qualitative and interpretive methods, the project demonstrates how trust can be analyzed simultaneously as an individual-level disposition, a discursive construction, and a context-dependent outcome of institutional arrangements. This mixed-method approach is not limited to the study of Internet voting but can be applied to a wide range of political technologies, from digital identity systems to algorithmic decision-making tools. In this sense, the dissertation not only advances empirical knowledge of Internet voting but also provides political scientists with a structured, replicable strategy for examining trust in digital governance across domains and cases.

6. CONCLUSION

This dissertation has examined the multifaceted nature of trust in and usage of Internet voting by combining theoretical, empirical, and methodological perspectives across four interrelated studies. Trust has been approached not as a static psychological state but as a relational outcome that emerges from the interaction of individuals, institutions, technologies, and broader political contexts. Through mixed-methods and multilevel analysis, the project has illuminated how citizens decide to participate in technologically mediated elections, how institutions sustain this participation over time, and how political and communicative environments shape public perceptions of legitimacy.

6.1. Theoretical Contributions

The dissertation makes three principal contributions to the interdisciplinary study of digital trust and governance.

First, it advances a multi-level conceptualization of trust that integrates individual, institutional, and contextual dimensions. While existing literature often isolates trust in technology from trust in political institutions (Carter & Campbell, 2011; Warkentin et al., 2018), this work demonstrates that the two are interdependent. Institutional legitimacy compensates for citizens' limited technological understanding, while technological performance reinforces institutional credibility through visible efficiency and transparency.

Second, the project contributes to the sociology of digital elections by treating Internet voting as a sociotechnical institution. Building on the work of Beck (1992), it shows that technology itself is not politically neutral: its meaning is co-produced by the institutional arrangements and discursive environments in which it operates. Estonia's case illustrates that technological stability can anchor democratic legitimacy, whereas in autocratic contexts, the same tools can be instrumentalized for symbolic legitimation.

Third, the dissertation refines the methodological toolkit for studying trust by demonstrating the complementarity of quantitative modeling and interpretive approaches. Logistic regression and factor analysis provided measurable insights into causal mechanisms, while Q-methodology uncovered the subjective structure of trust and distrust narratives. The reflexive engagement with Structural Equation Modeling (SEM) further enriched methodological awareness by showing how latent constructs could be tested under ideal data conditions.

6.2. Practical Recommendations

The empirical and theoretical insights from this project lead to several practical recommendations for policymakers, electoral management bodies, and system designers.

1. Institutional transparency and communication. Electoral authorities should adopt proactive communication strategies that demystify Internet voting procedures and address emerging concerns (similarly to what is done on the Estonian elections webpage devoted to debunking myths (*Valimised | Elections in Estonia*, n.d.)). Additionally, this transparency should be upheld by the experts as well; here, the precedent by Swiss Post can be helpful: open-source publication of cryptographic protocols,[4] system code with bug hunting program, and vulnerability reports significantly enhanced perceived integrity (*Swiss Post – E-Voting Bug Bounty Program – YesWeHack*, n.d.). These examples demonstrate that transparency can be operationalized not merely as a principle but as a measurable practice of communication.
2. Public trust maintenance through continuity. Trust in Internet voting consolidates through long-term stability and predictability. Estonia's commitment to incremental rather than radical system updates has been pivotal. The core cryptographic design introduced in 2005 has evolved gradually, ensuring that procedural familiarity and institutional continuity outweigh transient controversies. This stands in contrast to Norway's discontinuation of Internet voting pilots in 2011 and 2013, where limited public communication and fragmented political support weakened confidence in the process. According to official documentation from the Norwegian Ministry of Local Government and Regional Development (2014) and subsequent analyses by the Institute for Social Research in Oslo, the pilots were suspended due to concerns over verifiability, data protection, and a lack of cross-party consensus rather than specific technical failures. Yet, the absence of clear and timely communication created uncertainty even among experts following the project. Participants at later E-Vote ID conferences often recalled that the exact rationale for discontinuation remained ambiguous in the international debate, highlighting how incomplete transparency can erode institutional credibility. The Norwegian case thus demonstrates that discontinuity without comprehensive explanation can undo years of accumulated trust, whereas Estonia's steady, well-communicated evolution of its system exemplifies how procedural predictability and openness are crucial for sustaining confidence in Internet voting.
3. Targeted digital literacy initiatives. Since individual knowledge and confidence are key drivers of trust, governments should invest in educational programs that familiarize citizens with core principles of digital authentication, encryption, and vote verification. Since the primary pain point lies in the technical aspect of the process rather than the procedural, not how to cast a vote, but how it is encrypted and decrypted, and why it is a sufficient and necessary step for the elections, attention should be paid here. The format can

[4] The Estonian election management body publishes the code and now it will be done before even the test of Internet voting (ERR, 2025), but the point is the code itself might not generate enough attraction besides those activists, who are keeping a close eye on the technology implementation process, such as Märt Põder.

be of pre-recorded videos that are also uploaded to the election's webpage and in which local experts answer these questions and provide explanations. Additionally, overall computer literacy is used to minimize the share of those who have "no computer skills."

4. Discursive engagement with criticism. Low trust should not be treated as an anomaly but as a democratic resource that can improve system resilience. Estonia's post-2019 parliamentary election debate, where opposition parties questioned the integrity of Internet voting results, led to an independent review by the Cyber Security Centre and the public release of verification software. Rather than silencing critics, authorities turned contestation into an opportunity to reaffirm transparency. Similar models of inclusive accountability exist in Switzerland, where digital voting pilots require public consultations before reauthorization, and in Canada, where the federal Advisory Board on Digital Electoral Integrity incorporates civil society representatives. Institutionalizing such deliberative mechanisms transforms political skepticism into iterative oversight.
5. International benchmarking and peer learning. The common question during the Q-methodology was: "If Internet voting is so secure, why does no one use it but Estonia?" Luckily, these people live in Estonia, where Internet voting has been performing on par for more than two decades. That is why cross-national collaboration can strengthen the credibility and operational standards of the technology in general. More explicit collaboration between Estonia, Switzerland, Norway, and other countries would increase trust in the local technology due to the trust diffusion. However, collaborations should not be limited to academic research and should instead move in the direction of joint work between policymakers and technology vendors.
6. Research-practice integration. Speaking of academia, collaboration between academic researchers and election administrators could be institutionalized through memoranda of understanding, ensuring that data collection, auditing, and evaluation practices contribute simultaneously to scholarly knowledge and operational improvement.

6.3. Concluding Remarks

Ultimately, the dissertation demonstrates that trust in Internet voting is not a technological artifact but a societal achievement. It is sustained by informed citizens, credible institutions, and stable communicative environments that collectively make democratic participation intelligible in the digital age. The broader contribution of this research lies in demonstrating how the micro-dynamics of user confidence, meso-level institutional reliability, and macro-level political legitimacy merge into a single sociotechnical system of democratic trust.

By integrating theories of trust, confidence, and knowledge with empirical analysis of Estonia and Russia, the dissertation not only advances scholarly understanding of digital elections but also provides a transferable framework for analyzing public trust in other emerging technologies of governance – from AI-assisted decision-making to digital identity systems. As democracies continue to digitize their core functions, the lessons from Internet voting in Estonia underscore a fundamental principle: technological innovation can enhance democracy only when embedded in institutions that are themselves worthy of trust.

SUMMARY IN ESTONIAN

Usaldus elektroonilise hääletamise vastu: institutsionaalsed, tehnoloogilised ja kontekstuaalsed tegurid

Käesolevas doktoritöös uuritakse usaldust elektroonilise hääletamise vastu – selle teket, struktuuri ning tagajärgi –, keskendudes eelkõige usalduse rollile tehnoloogiate vastu ning usaldusele e-hääletamise rakendamise ja korraldamise eest vastutavate poliitiliste institutsioonide vastu. Politoloogia, e-valitsemise ja inimese-arvuti interaktsiooni uurimisdistsipliinide ristumiskohta paigutuv teadustöö edendab mitmetasandilist arusaama usaldusest riigiga seotud tehnoloogiate vastu, kombineerides võrdleva juhtumianalüüsi, segameetoditel põhinevaid empiirilisi disaine ja teoreetiliselt põhistatud kontseptuaalset raamistikku. Keskne empiiriline fookus on Eestil, ainsal demokraatlikul riigil, mis on üle 20 aasta õiguslikult siduvalt rakendanud ja kasutanud elektroonilist hääletamist kõikide valimiste puhul. Eesti puhul on kaheks peamiseks andmeallikaks kvantitatiivsed uuringuandmed ajavahemikul 2005–2023 ja poolstruktureeritud intervjuud, millele lisanduvad Q-metoodika tulemused. Fookust demokraatlikule Eestile täiendab võrdlev perspektiiv, mis hõlmab kontrastse juhtumina autokraatlikku Venemaad. Viimast iseloomustab kasutajate vähesem kokkupuude tehnoloogiaga ning valimistega seotud pettuste ajalugu.

Väitekiri lähtub tõdemusest, et usaldus on digiajastu valitsemise uurimisel muutunud üheks kesksemaks mõisteks, seda eriti kontekstides kus tehnoloogiad vahendavad demokraatia tuumprotsesse – nagu režiimi stabiilsus – läbi nendele antud legitiimsuse. Elektrooniline hääletamine on usalduse uurimise seisukohalt eriti suur väljakutse, kuna see on tehniliselt keeruline, poliitiliselt tundlik ja piiratud läbipaistvusega tavakodaniku jaoks, kellel puuduvad põhjalikud teadmised oluliste põhikontseptsioonide (nt krüptograafia) kohta. Eelnevad uurimused on käsitlenud usaldust e-hääletamise suhtes erinevatest vaatenurkadest, sealhulgas turvalisuse, kasutatavuse ja institutsionaalse ülesehituse seisukohast, ent käesolev töö väidab, et usaldust ei saa mõista ühest komponendist koosneva nähtusena. Selle asemel käsitletakse usaldust mitmekihilise ja suhtelise nähtusena, mida kujundavad ühiskondlikud hoiakud (st poliitiline režiim ja üldistatud usaldus), hinnangud institutsioonidele (st usaldus tehnoloogiaga seotud institutsioonide vastu), tehnoloogiaspetsiifilised arusaamad (st usaldus tehnoloogia vastu, mis hõlmab varasemaid kogemusi, teadmisi, isiklikke arvamusi, jne) ning kasutajaspetsiifilised omadused (st teadmised tehniliste aspektide kohta ja kindlus omaenda pädevuse suhtes).

Doktoritöö kontseptuaalne raamistik põhineb üldistatud usalduse mõistel, mis on aluseks kodanike suhtumisele poliitilistesse institutsioonidesse ja kollektiivsetesse otsustusprotsessidesse. Hoolimata üldistatud usalduse tähtsusest, ei ole seda doktoritöös põhjalikult käsitletud. Sellele käsitlusele tuginedes eristatakse kontseptuaalses raamistikus usaldust institutsioonide ja usaldust tehnoloogia vastu, mis on analüütiliselt erinevad, kuid omavahel seotud. Usaldus institutsioonide vastu viitab usaldusele poliitiliste asutuste ja valimiste korraldamise eest

vastutavate organite vastu, samas kui usaldus tehnoloogia vastu hõlmab hinnanguid elektrooniliste hääletussüsteemide aususe ja usaldusväärsuse kohta. Eelmainitud mitmetasandiline kontseptualiseerimine võimaldab doktoritöös seostada ühiskondliku tasandi usalduse taset indiviidi tasandi käitumisega ning suhtumisega e-hääletamisse.

Doktoritöö on üles ehitatud artiklipõhisena ning koosneb neljast uurimusest, mis käsitlevad e-hääletuse usaldusväärsuse erinevaid tahke, luues seeläbi kumulatiivselt sidusa argumentide jada. Esimene uurimus käsitleb seda, kuidas teadmised mõjutavad usaldust ja kindlustunnet elektroonilise hääletuse kasutamise otsuse tegemisel. Kasutades Eesti 2021. aasta kohalike ja 2023. aasta parlamendivalimiste järgsete küsitluste andmeid, analüüsitakse logistilise regressiooni mudelite abil, kuidas tehnilised teadmised mõjutavad usalduse, kindlustunde ja e-hääletuse kasutamise vahelist suhet. Tulemused näitavad, et kindlustunne mängib otsustavat rolli tehniliste teadmistega inimeste seas, samas kui usaldus tehnoloogia toimimise vastu ja usaldus elektroonilise hääletamise vastu avaldavad tugevamat mõju kõikide valijate seas, sõltumata nende teadmiste tasemest. Oluliseks leiuks on, et usaldus ja kindlustunne ei ole omavahel asendatavad, vaid toimivad erinevate mehhanismide kaudu, kus teadmised määravad selle, milline mehhanism domineerib.

Teises uurimuses kasutatakse kvalitatiivset ja interpretatiivset lähenemist uurimaks, kuidas usaldus ja usaldamatus e-hääletamise vastu diskursiivselt konstrueeritakse. Tuginedes ekspertintervjuudele ja Q-meetodi eksperimendile, mis viidi läbi Eesti valijatega (50% neist kasutas e-hääletamist, 50% ei ole kunagi e-hääletanud), määratleb uurimus eristuvad usalduse ja usaldamatuse diskursused, selmet käsitleda usaldust ühemõõtmelise hoiakuna. Analüüs näitab, et usalduse diskursused on peamiselt seotud positiivsete kogemustega, institutsioonilise võimekuse ja elektroonilise hääletamise normaliseerumisega laiemas digitaalse valitsemise ökosüsteemis. Seevastu umbusalduse diskursused on seotud poliitiliste vastuoludega, murega valimistulemustega manipuleerimise pärast ja skepsisega riigi kommunikatsioonitavade või läbipaistvuse suhtes. Tulemused rõhutavad, et usaldus ja usaldamatus järgivad erinevat loogikat ja on juurdunud erinevates argumenteerimisstruktuurides, toetades teoorias levinud väidet, et neid tuleks uurida analüütiliselt erinevate protsessidena ning ka „taastada" erinevate vahenditega. Näiteks hääletamisprotsessi läbipaistvamaks muutmine võib vähendada usaldamatust, kuid see ei pruugi mõjutada usalduse dünaamikat.

Kolmas uurimus sisaldab võrdlevat mõõdet, vastandades demokraatliku Eesti ja autokraatliku Venemaa, kus on madalam usalduse tase, nõrgem institutsioonine legitiimsus ja lühem e-valimiste kasutamise ajalugu. Artikkel toob esile terava kontrasti konsolideeritud demokraatliku režiimi ja valimiste kaudu toimiva autokraatia vahel ning näitab, et usaldus e-valimiste vastu on režiimide kontekstis moodustunud põhimõtteliselt erinevate motivatsiooniloogikate alusel. Eestis on usaldus tihedalt seotud hinnangutega institutsioonidele ning viimaste töö tulemuslikkusega: tajutavad eelised nagu mugavus, ausus, anonüümsus ja turvalisus, on usaldust tugevalt ennustavad tegurid, samas kui usaldus valimiste vastu on

eriti tugev selgitav indikaator. Venemaa puhul on aga üldine usaldus elektrooniliste valimiste vastu madal; usalduse väljendamine ja e-hääletamise kasutamine on kujunenud pigem mitte-instrumentaalsete motiivide – eelkõige kodanikukohustuse ja valitseva parteiga samastumise – tõttu. Venemaal ilmnev „võitja-efekt" viitab sellele, et usaldus internetihääletuse vastu peegeldab pigem riigi poolt propageeritavate narratiivide aktsepteerimist kui usaldust hääletusprotsessi aususe vastu. Artikkel näitab seega, et usaldust e-valimiste vastu ei saa seletada eraldi režiimispetsiifilistest legitiimsuse narratiividest ja institutsionaalsest kontekstist, rõhutades seda, et valimistehnoloogiad on poliitiliselt juurdunud.

Neljandas artiklis uuritakse, kuidas kujundab usaldust elektroonilise hääletamise vastu ja e-hääletamise kasutamist usaldus institutsioonide ja usaldus tehnoloogia vastu. Metoodiliselt täiendab artikkel varasemat teaduskirjandust, luues faktoranalüüsi abil institutsioonide ja tehnoloogia usalduse komposiitindeksid, minnes kaugemale usalduse mõõtmisest vaid ühe faktori abil korraga. Empiiriliselt näitavad tulemused, et usaldus institutsioonide vastu on järjepidevalt tugevaim ja kindlaim muutuja, mis aitab prognoosida nii usaldust e-hääletamise vastu kui ka süsteemi tegelikku kasutamist. Usaldus poliitiliste institutsioonide, sealhulgas valitsuse, parlamendi ja valimiste vastu, on tugevalt ja statistiliselt olulisel määral seotud e-hääletamise kasutamisega. Juhul kui indikaatorit „usaldus tehnoloogia vastu" kombineerida „usaldusega institutsioonide vastu", omab see elektroonilise hääletamise kasutamisel vaid väga piiratud iseseisvat selgitusvõimet või puudub see sootuks. Tulemused näitavad veel, et kõrgelt digitaliseeritud ühiskondades, kus avalikud e-teenused on laialt levinud, on variatiivsus usalduses tehnoloogia vastu suhteliselt väike, mis omakorda vähendab selle selgitavat tähtsust. Selle asemel tuginevad kodanikud poliitiliselt tundliku tehnoloogia kasutamisel ja usaldamisel, mida e-hääletamine on, peamiselt institutsioonide läbipaistvuse, vastutuse ja legitiimsuse hindamisele. Näidates, et tehnoloogilised garantiid ei suuda kompenseerida institutsioonilise usalduse puudujääke, toetab artikkel tugevalt väidet, et usaldus digitaalsete demokraatlike tehnoloogiate vastu põhineb põhimõtteliselt usaldusel institutsioonide vastu, mis neid tehnoloogiaid kujundavad, haldavad ja nende üle järelevalvet teostavad. See tulemus võimaldab kinnitada ka doktoritöö põhiväidet.

Kokkuvõttes näitavad neli artiklit, et usaldus e-valimiste vastu on mitmemõõtmeline ja kontekstist sõltuv nähtus, mis tekib individuaalsete teadmiste, institutsioonide usaldusväärsuse, poliitilise konteksti ja tehnoloogiaspetsiifiliste arusaamade koostoimel. Esimene uurimus näitab, et tehnilised teadmised ei asenda usaldust, vaid kujundavad seda ümber, nihutades usalduse institutsioonilistelt märguannetelt teadlikumate valijate kindlustundel põhinevate hinnangute poole. Teises uurimuses näidatakse, et usaldus ja usaldamatus väljenduvad erinevate diskursiivsete loogikate kaudu, rõhutades, et suhtumine internetihääletusse ei moodusta ühtset poolt-vastu telge, vaid see on sotsiaalselt ja poliitiliselt konstrueeritud. Kolmanda uurimuse võrdlev perspektiiv tõestab, et režiimi kontekst mõjutab oluliselt usaldusmehhanisme. Kui usaldus demokraatlikus Eestis põhineb peamiselt hinnangul vahendite ja institutsioonide töö tulemuslikkuse kohta, siis autokraatlikul Venemaal on usaldus kujunenud mitte-instrumentaalsete

motiivide – kodanikukohustus ja poliitiline kuuluvus – mõjul, peegeldades nii režiimile omast legitiimsuse narratiivi. Lõpetuseks näitab neljas uurimus, et usaldus institutsioonide vastu kaalub järjekindlalt üles usalduse tehnoloogiate vastu, selgitades nii usaldust e-valimiste suhtes kui ka elektroonilise hääletamise kasutamist isegi väga digitaliseeritud keskkonnas. Kokkuvõttes viivad need tulemused ühe keskse järelduseni: usaldus e-valimiste vastu ei teki ainult tehnoloogia abil, vaid on kinnistunud laiemas institutsioonilises ja poliitilises kontekstis, kus usaldus institutsioonide vastu toimib peamise ühendava jõuna, sidudes individuaalse usalduse, avaliku diskursuse ja režiimile omased stiimulid.

Lisaks empiirilistele tulemustele annab väitekiri laiema teoreetilise ja metodoloogilise panuse digitaalse valitsemise usalduse uurimisse. Kontseptuaalselt edendab see usalduse mitmekihilist mõistmist, sidudes institutsionaalse analüüsi ja ühiskondlikud-tehnilised perspektiivid. Metodoloogiliselt näitab doktoritöö, kuidas usaldust saab uurida nii kvantitatiivsest kui ka kvalitatiivsest vaatenurgast, hõlmates mitte ainult käitumistulemusi, vaid ka diskursiivseid konstruktsioone ja kontekstuaalseid tähendusi. See segameetodeid kombineeriv lähenemine pakub ülekantavat uurimismudelit, mida saab rakendada teistele digitaalse valitsemise tehnoloogiatele, nagu elektroonilise identiteedi süsteemid, algoritmidel põhinevad otsustusmudelid või veebipõhised osalusplatvormid.

Kokkuvõttes näitab doktoritöö, et usaldus e-valimiste vastu ei sõltu ainult tehnilisest turvalisusest või halduspädevusest, vaid on seotud ka laiemate ühiskondlike ja institutsionaalsete kontekstidega. Tehnoloogilise usalduse, institutsionaalse usalduse, kindlustunde ja teadmiste rollide lahti seletamisega loob uurimus nüansirikka arusaama sellest, miks internetihääletust usaldatakse ja kasutatakse mõnes kontekstis, samas kui teistes kontekstides on see vastuoluline või kõrvale jäetud. Sellega annab käesolev doktoritöö ühest küljest panuse nii usaldust ja digitaalset valitsemist käsitlevasse teaduskirjandusse kui teisalt ka praktilistesse aruteludesse tingimuste üle, mille alusel valimistehnoloogiad demokraatlikku legitiimsust saavutavad ja säilitavad.

REFERENCES

1. 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
2. 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
3. Adeshina, S. A., & Ojo, A. (2014). *Design imperatives for e-voting as a socio-technical system* (pp. 1–4). IEEE. https://mural.maynoothuniversity.ie/id/eprint/15830/
4. Adeshina, S. A., & Ojo, A. (2020). Factors for e-voting adoption – Analysis of general elections in Nigeria. *Government Information Quarterly*, *37*(3), 101257. https://doi.org/10.1016/j.giq.2017.09.006
5. Agbesi, S., Budurushi, J., Dalela, A., & Kulyk, O. (2023). Investigating Transparency Dimensions for Internet Voting. In M. Volkamer, D. Duenas-Cid, P. Rønne, P. Y. A. Ryan, J. Budurushi, O. Kulyk, A. Rodriguez Pérez, & I. Spycher-Krivonosova (Eds.), *Electronic Voting* (pp. 1–17). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-43756-4_1
6. Agbesi, S., Budurushi, J., Dalela, A., Nissen, C., & Kulyk, O. (2024). How to increase transparency and trust in internet voting systems: An experimental study. *Proceedings of the 13th Nordic Conference on Human-Computer Interaction*, 1–18. https://doi.org/10.1145/3679318.3685362
7. Agresti, A. (2010). *Analysis of Ordinal Categorical Data*. John Wiley & Sons.
8. Alishani, A., & Homburgh, V. (2025). *When citizens meet the chatbot: Evidence from a survey vignette experiment in Estonia*. https://doi.org/10.1177/09520767251404286
9. Alvarez, R. M., & Hall, T. E. (2010). *Electronic Elections: The Perils and Promises of Digital Democracy*. Princeton University Press. https://doi.org/10.1515/9781400834082
10. 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
11. 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
12. Anckar, C. (2008). On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research. *International Journal of Social Research Methodology*, *11*(5), 389–401. https://doi.org/10.1080/13645570701401552
13. Appel, A. (2022). Is Internet Voting Trustworthy? The Science and the Policy Battles. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4209296
14. Appel, A., DeMillo, R., & Stark, P. B. (2019). *Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters* (SSRN Scholarly Paper No. 3375755). Social Science Research Network. https://doi.org/10.2139/ssrn.3375755
15. Attig, C., Wessel, D., & Franke, T. (2018). *Human-Technology Interaction from a Personal Resource Perspective: The Affinity for Technology Interaction (ATI) Scale*.

16. Bahmanziari, T., Pearson, J. M., & Crosby, L. (2003). Is Trust Important in Technology Adoption? A Policy Capturing Approach. *Journal of Computer Information Systems*.
17. Bauer, P. C., & Fatke, M. (2014). Direct Democracy and Political Trust: Enhancing Trust, Initiating Distrust-or Both? *Swiss Political Science Review*, *20*(1), 49–69. https://doi.org/10.1111/spsr.12071
18. Beck, U. (1992). *Risk Society: Towards a New Modernity*. SAGE Publications.
19. Benk, M., Kerstan, S., von Wangenheim, F., & Ferrario, A. (2024). Twenty-four years of empirical research on trust in AI: A bibliometric review of trends, overlooked issues, and future directions. *AI & SOCIETY*. https://doi.org/10.1007/s00146-024-02059-y
20. Bijker, W. E., Hughes, T. P., & Pinch, T. (Eds.). (1987). *The Social construction of technological systems: New directions in the sociology and history of technology*. MIT Press.
21. 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
22. Braithwaite, V. A., & Levi, M. (1998). *Trust and Governance*. https://philpapers.org/rec/BRATAG-2
23. Breaugh, J., Rackwitz, M., Hammerschmid, G., Nõmmik, S., Bello, B., Boon, J., Van Doninck, D., Downe, J., & Randma-Liiv, T. (2023). Deconstructing complexity: A comparative study of government collaboration in national digital platforms and smart city networks in Europe. *Public Policy and Administration*, 09520767231169401. https://doi.org/10.1177/09520767231169401
24. Byrne, M. D. (2017). Improving Voting Systems' User-Friendliness, Reliability, & Security. *Behavioral Science & Policy*, *3*(1), 15–24. https://doi.org/10.1177/237946151700300103
25. Carback, R., Chaum, D., Clark, J., Conway, J., Essex, A., Herrnson, P. S., Mayberry, T., Popoveniuc, S., Rivest, R. L., Shen, E., Sherman, A. T., & Vora, P. L. (2010). *Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy* [Working Paper]. Caltech/MIT Voting Technology Project. https://dspace.mit.edu/handle/1721.1/96627
26. Carter, L., & Bélanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal*, *15*(1), 5–25.
27. Carter, L., & Bélanger, F. (2012). *Internet voting and political participation: An empirical comparison of technological and political factors*. *43*(3), 21.
28. 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
29. Carter, L., Weerakkody, V., Phillips, B., & Dwivedi, Y. K. (2016). Citizen Adoption of E-Government Services: Exploring Citizen Perceptions of Online Services in the United States and United Kingdom. *Information Systems Management*, *33*(2), 124–140. https://doi.org/10.1080/10580530.2016.1155948
30. Chen, M., Cao, Y., & Liang, Y. (2023). Determinants of open government data usage: Integrating trust theory and social cognitive theory. *Government Information Quarterly*, *40*(4), 101857. https://doi.org/10.1016/j.giq.2023.101857

31. Choi, S. O., & Kim, B. C. (2012). Voter Intention to Use E-Voting Technologies: Security, Technology Acceptance, Election Type, and Political Ideology. *Journal of Information Technology & Politics*, *9*(4), 433–452. https://doi.org/10.1080/19331681.2012.710042
32. Chondros, N., Zhang, B., Zacharias, T., Diamantopoulos, P., Maneas, S., Patsonakis, C., Delis, A., Kiayias, A., & Roussopoulos, M. (2016). *Distributed, End-to-end Verifiable, and Privacy-Preserving Internet Voting Systems*. https://www.research.ed.ac.uk/en/publications/distributed-end-to-end-verifiable-and-privacy-preserving-internet
33. Clarke, D., & Martens, T. (2016). *E-voting in Estonia* (No. arXiv:1606.08654). arXiv. https://doi.org/10.48550/arXiv.1606.08654
34. Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, *58*(6), 737–758. https://doi.org/10.1016/S1071-5819(03)00041-7
35. Cruz, J. N. (2023). A fuzzy-set qualitative comparative analysis of how corruption, education, inequality and trust in parliament affect voter-turnout. *Crime, Law and Social Change*, *80*(5), 547–567. https://doi.org/10.1007/s10611-023-10102-0
36. Dalmau, R. M. (2015). Venezuela: Finding the Relationship between E-Voting and Democracy. In *E-Voting Case Law*. Routledge.
37. Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319. https://doi.org/10.2307/249008
38. De Blasio, E., & Selva, D. (2019). Implementing open government: A qualitative comparative analysis of digital platforms in France, Italy and United Kingdom. *Quality & Quantity*, *53*(2), 871–896. https://doi.org/10.1007/s11135-018-0793-7
39. Deng, J., & Liu, P. (2017). Consultative Authoritarianism: The Drafting of China's Internet Security Law and E-Commerce Law. *Journal of Contemporary China*, *26*(107), 679–695. https://doi.org/10.1080/10670564.2017.1305488
40. *Digital authoritarianism in China and Russia: Common goals and diverging standpoints in the era of great-power rivalry – FIIA – Finnish Institute of International Affairs*. (2020, October 30). https://fiia.fi/en/publication/digital-authoritarianism-in-china-and-russia
41. Downing, J., & Brun, E. E. (2022). "I Think Therefore I Don't Vote": Discourses on abstention, distrust and twitter politics in the 2017 French presidential election. *French Politics*, *20*(2), 147–166. https://doi.org/10.1057/s41253-021-00166-6
42. Du, P., Yu, S., & Yang, D. (Eds.). (2019). *The Development of E-governance in China: Improving Cybersecurity and Promoting Informatization as Means for Modernizing State Governance*. Springer Singapore. https://doi.org/10.1007/978-981-13-1014-0
43. 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
44. Duenas-Cid, D. (2024). Trust Frameworks in Application to Technology in Elections. *E-Vote-ID 2023 Proceedings*.
45. 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
46. 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

47. Dukalskis, A., & Gerschewski, J. (2018). What autocracies say (and what citizens hear): Proposing four mechanisms of autocratic legitimation. In *Justifying Dictatorship*. Routledge.
48. 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
49. 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
50. ERR, E. |. (2025, October 28). *Supreme Court: E-voting source code must be published before test vote*. ERR. https://news.err.ee/1609841440/supreme-court-e-voting-source-code-must-be-published-before-test-vote
51. Espinosa, V. I., & and 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
52. *Explore the Map*. (2025, July 31). Freedom House. https://freedomhouse.org/explore-the-map
53. Farooq, A., Warkentin, M., & Virtanen, S. (2024). Role of shared identity and agency trust in online voting among Finnish citizens. *Technology in Society*, *76*, 102429. https://doi.org/10.1016/j.techsoc.2023.102429
54. Franke, T., Attig, C., & Wessel, D. (2019). A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction*. https://www.tandfonline.com/doi/abs/10.1080/10447318.2018.1456150
55. Freitag, M., & Ackermann, K. (2016). Direct Democracy and Institutional Trust: Relationships and Differences Across Personality Traits: Direct Democracy and Institutional Trust. *Political Psychology*, *37*(5), 707–723. https://doi.org/10.1111/pops.12293
56. Fuglerud, K. S., & Røssvoll, T. H. (2012). An evaluation of web-based voting usability and accessibility. *Universal Access in the Information Society*, *11*(4), 359–373. https://doi.org/10.1007/s10209-011-0253-9
57. Fujiwara, T. (2015). Voting Technology, Political Responsiveness, and Infant Health: Evidence From Brazil. *Econometrica*, *83*(2), 423–464. https://doi.org/10.3982/ECTA11520
58. Fukuyama, F. (1996). *Trust: The Social Virtues and the Creation of Prosperity*. Free Press.
59. Gambetta, D. (1988). *Trust: Making and Breaking Cooperative Relations*. B. Blackwell.
60. Garnett, H. A., & James, T. S. (2020). Cyber elections in the digital age: Threats and opportunities of technology for electoral integrity. *Election Law Journal*, *19*(2), 111–126. https://doi.org/10.1089/elj.2020.0633
61. 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
62. Gerlach, J., & Gasser, U. (2009). *Three case studies from Switzerland: E-voting*. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Gerlach-Gasser_SwissCases_Evoting.pdf

63. Germann, M., & Serdült, U. (2017). Internet voting and turnout: Evidence from Switzerland. *Electoral Studies*. https://doi.org/10.1016/j.electstud.2017.03.001
64. Gibson, J. P., Krimmer, R., Teague, V., & Pomares, J. (2016). A review of E-voting: The past, present and future. *Annals of Telecommunications*, *71*(7–8), 279–286. https://doi.org/10.1007/s12243-016-0525-8
65. Giddens, A. (1990). *The Consequences of Modernity*. Stanford University Press.
66. Giddens, A. (1991). *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Stanford University Press.
67. 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
68. 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
69. Gritsenko, D., & Indukaev, A. (2021). Digitalising City Governance in Russia: The Case of the 'Active Citizen' Platform. *Europe-Asia Studies*, *73*(6), 1102–1124. https://doi.org/10.1080/09668136.2021.1946013
70. Gulati, S., Sousa ,Sonia, & and Lamas, D. (2019). Design, development and evaluation of a human-computer trust scale. *Behaviour & Information Technology*, *38*(10), 1004–1015. https://doi.org/10.1080/0144929X.2019.1656779
71. Guriev, S., & Treisman, D. (2020). A theory of informational autocracy. *Journal of Public Economics*, *186*, 104158. https://doi.org/10.1016/j.jpubeco.2020.104158
72. Halderman, J. A., & Teague, V. (2015). *The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election* (No. arXiv:1504.05646). arXiv. https://doi.org/10.48550/arXiv.1504.05646
73. Hardin, R. (2002). *Trust and Trustworthiness*. Russell Sage Foundation.
74. Hoff, K. A., & Bashir, M. (2015). Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust. *Human Factors*, *57*(3), 407–434. https://doi.org/10.1177/0018720814547570
75. Jasanoff, S. (2004). *States of Knowledge: The Co-Production of Science and the Social Order*. Routledge.
76. Juma, J., & Oguk, C. O. (2020). *Election results' verification in e-voting systems in Kenya: A review*. http://repository.rongovarsity.ac.ke/handle/123456789/2316
77. Kline, R. B. (2011). *Principles and Practice of Structural Equation Modeling*. Guilford Publications.
78. Krimmer, R., & Volkamer, M. (2005). *Bits or paper? Comparing remote electronic voting to postal voting*.
79. Lee, J. D., & See, K. A. (2004). Trust in Automation: Designing for Appropriate Reliance. *Human Factors*, 31.
80. Lewis, J. D., & Weigert, A. (1985). Trust as a Social Reality. *Social Forces*, *63*(4).
81. Li, L., Li, Z., Ding, H., & Gao, M. (2024). How can digitalization be used to develop community resilience in public health emergencies?: A qualitative comparative analysis from China. *PloS One*, *19*(12), e0315713. https://doi.org/10.1371/journal.pone.0315713

82. Licht, N., Duenas-Cid, D., Krivonosova, 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
83. 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
84. Linz, J. J., & Stepan, A. (1996). *Problems of Democratic Transition and Consolidation*. Johns Hopkins University Press. https://doi.org/10.56021/9780801851575
85. Luhmann, N. (1979). *Trust and Power: Two Works*. Wiley.
86. Luhmann, N. (1988). Familiarity, Confidence, Trust: Problems and Alternatives. In *Trust: Making and Breaking of Cooperative Relations*. Basil Blackwell, Oxford. https://luhmann.ir/wp-content/uploads/2021/07/Familiarity-Confidence-Trust-Problems-and-Alternatives.pdf
87. 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), Article 24. https://doi.org/10.3390/su162411068
88. Marky, K., Zollinger, M.-L., Roenne, P., Ryan, P. Y. A., Grube, T., & Kunze, K. (2021). Investigating Usability and User Experience of Individually Verifiable Internet Voting Schemes. *ACM Trans. Comput. – Hum. Interact.*, *28*(5), 30:1–30:36. https://doi.org/10.1145/3459604
89. Mayer, R. C., Davis, J. H., & Schoorman, D. (1995). *An Integrative Model of Organizational Trust*.
90. McKeown, B., & Thomas, D. (2013). *Q Methodology*. SAGE Publications, Inc. https://doi.org/10.4135/9781483384412
91. Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Trans. Manage. Inf. Syst.*, *2*(2), 12:1–12:25. https://doi.org/10.1145/1985347.1985353
92. 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
93. 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
94. Merritt, S. M., Heimbaugh, H., LaChapell, J., & Lee, D. (2013). I Trust It, but I Don't Know Why: Effects of Implicit Attitudes Toward Automation on Trust in an Automated System. *Human Factors*, *55*(3), 520–534. https://doi.org/10.1177/0018720812465081
95. 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
96. Misztal, B. (2013). *Trust in Modern Societies: The Search for the Bases of Social Order*. John Wiley & Sons.

97. Morozov, E. (2011). *The Net Delusion: How Not to Liberate The World*. Penguin UK.
98. Nestas, L., & Hole, K. (2012). Building and Maintaining Trust in Internet Voting. *Computer*, *45*(5), 74–80. https://doi.org/10.1109/MC.2012.35
99. Norman, G. (2010). Likert scales, levels of measurement and the "laws" of statistics. *Advances in Health Sciences Education*, *15*(5), 625–632. https://doi.org/10.1007/s10459-010-9222-y
100. Norris, P. (2002). E-Voting as the Magic Ballot? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.336542
101. Norris, P. (2014). *Why Electoral Integrity Matters*. Cambridge University Press. https://doi.org/10.1017/CBO9781107280861
102. Parasuraman, R., & Riley, V. (1997). Humans and Automation: Use, Misuse, Disuse, Abuse. *Human Factors*, *39*(2), 230–253. https://doi.org/10.1518/001872097778543886
103. Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going from bad to worse: From Internet voting to blockchain voting. *Journal of Cybersecurity*, *7*(1), tyaa025. https://doi.org/10.1093/cybsec/tyaa025
104. 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
105. Perez, V., & Ross, J. M. (2020). Federalism and Polycentric Government in a Pandemic. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3570726
106. Putnam, R. D. (2001). *Bowling alone: The collapse and revival of American community*. Simon and Schuster.
107. Putnam, R. D., Leonardi, R., & Nanetti, R. (1994). *Making democracy work: Civic traditions in modern Italy* (5. print., 1. Princeton paperback print). Princeton Univ. Press.
108. Reuter, O. J. (2020). Civic Duty and Voting under Autocracy. *The Journal of Politics*, *83*(4), 1602–1618. https://doi.org/10.1086/711718
109. Reuter, O. J., & Szakonyi, D. (2021). Electoral Manipulation and Regime Support: Survey Evidence from Russia. *World Politics*, *73*(2), 275–314. https://doi.org/10.1017/S0043887120000234
110. Roberts, T., & Oosterom, M. (n.d.). Digital authoritarianism: A systematic literature review. *Information Technology for Development*, *0*(0), 1–25. https://doi.org/10.1080/02681102.2024.2425352
111. 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
112. Rothstein, B., & Stolle, D. (2008). The State and Social Capital: An Institutional Theory of Generalized Trust. *Comparative Politics*, *40*, 441–459. https://doi.org/10.5129/001041508X12911362383354
113. Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not So Different After All: A Cross-Discipline View Of Trust. *Academy of Management Review*, *23*(3), 393–404. https://doi.org/10.5465/amr.1998.926617
114. Ryan, P. Y. A., Bismark, D., Heather, J., Schneider, S., & Xia, Z. (2009). PrÊt À Voter: A Voter-Verifiable Voting System. *IEEE Transactions on Information Forensics and Security*, *4*(4), 662–673. https://doi.org/10.1109/TIFS.2009.2033233

115. Schneider, C. Q., & Wagemann, C. (2012). *Set-Theoretic Methods for the Social Sciences: A Guide to Qualitative Comparative Analysis*. 370.
116. Schneider, F. B. (1999). *Trust in Cyberspace*. National Academies Press. https://books.google.ee/books?id=8bxRZVkYn1kC
117. Schryen, G., & Volkamer, M. (2010). *Measuring eTrust in Distributed Systems*.
118. Simmel, G. (1950). *The Sociology of Georg Simmel*. Simon and Schuster.
119. Solvak, M. (2020). Does Vote Verification Work: Usage and Impact of Confidence Building Technology in Internet Voting. In R. Krimmer, M. Volkamer, B. Beckert, R. Küsters, O. Kulyk, D. Duenas-Cid, & M. Solvak (Eds.), *Electronic Voting* (pp. 213–228). Springer International Publishing. https://doi.org/10.1007/978-3-030-60347-2_14
120. Solvak, M., & Vassil, K. (2016). *E-voting in Estonia:Technological Diffusion and Other Developments Over Ten Years (2005—2015)*. University of Tartu.
121. Solvak, M., & Vassil, K. (2018). Could Internet Voting Halt Declining Electoral Turnout? New Evidence That E-Voting Is Habit Forming. *Policy and Internet*, *10*(1), 4–21. https://doi.org/10.1002/poi3.160
122. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014). Security Analysis of the Estonian Internet Voting System. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 703–715. https://doi.org/10.1145/2660267.2660315
123. *Swiss Post – E-Voting bug bounty program – YesWeHack*. (n.d.). YesWeHack #1 Bug Bounty Platform in Europe. Retrieved August 22, 2025, from https://yeswehack.com/programs/swiss-post-evoting
124. Sztompka, P. (1999). *Trust: A Sociological Theory*. Cambridge University Press.
125. *The V-Dem Dataset – V-Dem*. (2025). https://v-dem.net/data/the-v-dem-dataset/
126. Tilly, C. (2004). Trust and Rule. *Theory and Society*, *33*(1), 1–30.
127. 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
128. 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
129. *Valimised | Elections in Estonia*. (n.d.). Retrieved March 4, 2025, from https://www.valimised.ee/
130. 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
131. Venkatesh, Viswanath., 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.
132. Volkamer, M., Spycher, O., & Dubuis, E. (2011). Measures to establish trust in internet voting. *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance*, 1–10. https://doi.org/10.1145/2072069.2072071
133. Wadowski, G. (2025). A Comparative Study of Electronic and Paper Ballot Systems in Modern U.S. Elections. *Open Access Master's Theses*. https://digitalcommons.uri.edu/theses/2578

134. Wang, C.-H. (2016). Political trust, civic duty and voter turnout: The Mediation argument. *The Social Science Journal*, *53*(3), 291–300. https://doi.org/10.1016/j.soscij.2016.04.008
135. 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
136. Watts, S., & Stenner, P. (2012). *Doing Q Methodological Research: Theory, Method & Interpretation*. 1–248.
137. Willemson, J. (2018). Bits or paper: Which should get to carry your vote? *Journal of Information Security and Applications*, *38*, 124–131. https://doi.org/10.1016/j.jisa.2017.11.007
138. Winner, L. (1980). Do Artifacts Have Politics? *Daedalus*, *109*(1), 121–136.
139. 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
140. Zantalis, F., Koulouras, G., & Karabetsos, S. (2024). Blockchain Technology: A Framework for Endless Applications. *IEEE Consumer Electronics Magazine*, *13*(2), 61–71. https://doi.org/10.1109/MCE.2023.3248872
141. 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
142. Zollinger, M.-L., Rønne, P. B., Schneider, S., Ryan, P. Y. A., & Jamroga, W. (2025). Intelligo Ut Confido: Understanding, Trust and User Experience in Verifiable Receipt-Free E-Voting. In D. Duenas-Cid, P. Roenne, M. Volkamer, J. Budurushi, M. Blom, A. Rodríguez-Pérez, I. Spycher-Krivonosova, J. Castellà Roca, & J. Barrat Esteve (Eds.), *Electronic Voting* (pp. 158–174). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-72244-8_10

PUBLICATIONS

CURRICULUM VITAE

Name: Bogdan Romanov
Date of birth: 24.03.1997
E-mail: romanovbogdan4@gmail.com

Education:

2021–…	University of Tartu, PhD Studies in Political Science
2019–2021	University of Tartu, MA in Political Science
2015–2019	Higher School of Economics, Saint Petersburg, BA in Political Science

Employment:

2021–…	University of Tartu, Junior Research Fellow in E-Governance
2024–…	Printify, Engineering Analyst
2023–2024	Civitta Estonia, Consultant, Grant writer
2021–2023	Xena Exchange-Qredo, Quantitative Developer

Main research directions:

Comparative politics, digital governance, human-computer interaction

Publications:

Romanov, B., & Solvak, M. (2025). Pandemic-proof elections: Did COVID-19 increase the use of Internet voting? JeDEM – eJournal of eDemocracy and Open Government, 17(4), 1–42. https://doi.org/10.29379/jedem.v17i4.1024

Romanov, B., Cid, D. D., & Solvak, M. (2025). I Know, Therefore, I Trust? Quantitatively modelling how knowledge shapes the reliance on trust and confidence in the case of internet voting usage in Estonia. Interacting with Computers. https://doi.org/10.1093/iwc/iwaf055

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.

Duenas-Cid, D., & Romanov, B. (2025). *Trust in Internet Voting: Preliminary results of a QMethodology Experiment in Estonia.* America's Conference on Information Systems AMCIS 2025, 2025, 14-08-2025–16-08-2025, Montreal, Canada.

Romanov, B., & Babayan, V. (2025). *Trust in online voting under different regime settings: Evidence from public opinion on online voting in national elections in Estonia and Russia.* Journal of Information Technology & Politics, 1–18.

Malakhova, P., & Romanov, B. (2024). *Why Do Activists in Exile Support Civil Society in Non-democratic Regimes? The Case of Perviy Otdel.* Russian Politics, 9(3), 427–453.

Carmichael, L., & Romanov, B. (2022). *Domestic Decision-Making, Regional Linkages, and Cybersecurity Considerations: Implementation of Internet Voting in Russia*, September 2021. E-Vote-ID 2022, 135.

Corici, A. A., Podgorelec, B., Zefferer, T., Hühnlein, D., Cucurull, J., Graux, H., Dedovic, S., Romanov, B., Schmidt, C., & Krimmer, R. (2022). *Enhancing European interoperability frameworks to leverage mobile cross-border services in Europe.* 41–53.

Romanov, B. (2022). *Similar yet so different: The analysis of factors explaining the variance in COVID-19 deaths across the Baltic and Nordic states.* Nordiques.

Romanov, B., & Kabanov, Y. (2020). *The oxymoron of the internet voting in illiberal and hybrid political contexts.* 183–195.

Kabanov, Y., & Romanov, B. (2017). *Interaction between the internet and the political regime: An empirical study* (1995–2015). 282–291.

Conferences:

Tenth International Joint Conference on Electronic Voting, 2025 (Chairperson and Presenter)

Ninth Tartu Conference on East European and Eurasian Studies 2025 (Moderator)

Ninth International Joint Conference on Electronic Voting, 2024 (Presenter)

Aleksanteri Conference, *Resisting Authoritarianism in Eurasia: Civil Society and New Solidarities,* 2024 (Presenter)

Seventh Tartu Conference on East European and Eurasian Studies 2023 (Presenter)

Sevent International Joint Conference on Electronic Voting, 2022 (Presenter)

Sixth Tartu Conference on Russian and East European Studies 2022 (Presenter)

Sixth International Joint Conference on Electronic Voting, 2021 (Presenter)

ELULOOKIRJELDUS

Nimi: Bogdan Romanov
Sünniaeg: 24.03.1997
E-post: romanovbogdan4@gmail.com

Haridus:

2021–…	Tartu Ülikool, politoloogia doktoriõpe
2019–2021	Tartu Ülikool, politoloogia magistriõpe
2015–2019	Kõrgem majanduskool (Higher School of Economics), Peterburi, politoloogia bakalaureuseõpe

Töökogemus:

2021–…	Tartu Ülikool, e-valitsemise nooremteadur
2024–…	Printify, andmeanalüütik (Engineering Analyst)
2023–2024	Civitta Eesti, konsultant, projektikirjutaja
2021–2023	Xena Exchange–Qredo, kvantitatiivne arendaja

Peamised uurimisvaldkonnad:

Võrdlev poliitika, digivalitsemine, inim-arvuti interaktsioon

Publikatsioonid:

Romanov, B., & Solvak, M. (2025). Pandemic-proof elections: Did COVID-19 increase the use of Internet voting? JeDEM – eJournal of eDemocracy and Open Government, 17(4), 1–42. https://doi.org/10.29379/jedem.v17i4.1024

Romanov, B., Cid, D. D., & Solvak, M. (2025). I Know, Therefore, I Trust? Quantitatively modelling how knowledge shapes the reliance on trust and confidence in the case of internet voting usage in Estonia. Interacting with Computers. https://doi.org/10.1093/iwc/iwaf055

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.

Duenas-Cid, D., & Romanov, B. (2025). *Trust in Internet Voting: Preliminary results of a QMethodology Experiment in Estonia.* America's Conference on Information Systems AMCIS 2025, 2025, 14-08-2025–16-08-2025, Montreal, Canada.

Romanov, B., & Babayan, V. (2025). *Trust in online voting under different regime settings: Evidence from public opinion on online voting in national elections in Estonia and Russia.* Journal of Information Technology & Politics, 1–18.

Malakhova, P., & Romanov, B. (2024). *Why Do Activists in Exile Support Civil Society in Non-democratic Regimes? The Case of Perviy Otdel.* Russian Politics, 9(3), 427–453.

Carmichael, L., & Romanov, B. (2022). *Domestic Decision-Making, Regional Linkages, and Cybersecurity Considerations: Implementation of Internet Voting in Russia, September 2021.* E-Vote-ID 2022, 135.

Corici, A. A., Podgorelec, B., Zefferer, T., Hühnlein, D., Cucurull, J., Graux, H., Dedovic, S., Romanov, B., Schmidt, C., & Krimmer, R. (2022). *Enhancing European interoperability frameworks to leverage mobile cross-border services in Europe.* 41–53.

Romanov, B. (2022). *Similar yet so different: The analysis of factors explaining the variance in COVID-19 deaths across the Baltic and Nordic states.* Nordiques.

Romanov, B., & Kabanov, Y. (2020). *The oxymoron of internet voting in illiberal and hybrid political contexts.* 183–195.

Kabanov, Y., & Romanov, B. (2017). *Interaction between the internet and the political regime: An empirical study (1995–2015).* 282–291.

Konverentsid:

Kümnes rahvusvaheline ühiskonverents elektroonilise hääletamise teemal (International Joint Conference on Electronic Voting), 2025 (Paneeli juhataja ja ettekandja)

Üheksas Tartu idauuringute konverents (Ninth Tartu Conference on East European and Eurasian Studies), 2025 (Moderator)

Üheksas rahvusvaheline ühiskonverents elektroonilise hääletamise teemal, 2024 (Ettekandja)

Aleksanteri konverents *Resisting Authoritarianism in Eurasia: Civil Society and New Solidarities*, 2024 (Ettekandja)

Seitsmes Tartu idauuringute konverents, 2023 (Ettekandja)

Seitsmes rahvusvaheline ühiskonverents elektroonilise hääletamise teemal, 2022 (Ettekandja)

Kuues Tartu konverents Vene ja Ida-Euroopa uuringute teemal, 2022 (Ettekandja)

Kuues rahvusvaheline ühiskonverents elektroonilise hääletamise teemal, 2021 (Ettekandja)

DISSERTATIONES RERUM POLITICARUM UNIVERSITATIS TARTUENSIS

1. **Allan Sikk.** Highways to power: new party success in three young democracies. Tartu, 2006.
2. **Holger Mölder.** Cooperative security dilemma – practicing the hobbesian security culture in the Kantian security environment. Tartu, 2010.
3. **Heiko Pääbo.** Potential of Collective Memory Based International Identity Conflicts in Post-Imperial Space. Tartu, 2011.
4. **Mihkel Solvak.** Private member's bills in parliament – a comparative study of Finland and Estonia. Tartu, 2011, 217 p.
5. **Viljar Veebel.** The role and impact of positive conditionality in the EU pre-accession policy. Tartu, 2012, 230 p.
6. **Alar Kilp.** Church authority in society, culture and politics after Communism. Tartu, 2012, 177 p.
7. **Maria Groeneveld.** The role of the state and society relationship in the foreign policy making process. Tartu, 2012, 193 p.
8. **Mari-Liis Sööt.** Explaining Corruption: Opportunities for Corruption and Institutional Trust. Tartu, 2013, 120 p.
9. **Kadri Lühiste.** Regime Support in European Democracies. Tartu, 2013, 124 p.
10. **Raul Toomla.** De facto states in the international system: Conditions for (in-)formal engagement. Tartu, 2013, 209 p.
11. **Andro Kitus.** A Post-Structuralist Concept of Legitimacy. A thesis in partial fulfilment of the requirements for the degree of Doctor of Philosophy. Tartu, 2014, 189 p.
12. **Kristian Lau Nielsen.** Soft Power Europe: The Lesser Contradiction in Terms and Practices. Tartu, 2016, 156 p.
13. **Birgit Poopuu.** Acting is everything: the European Union and the process of becoming a peacebuilder. Tartu, 2016, 242 p.
14. **Kristina Kallas.** Revisiting the triadic nexus: An analysis of the ethno-political interplay between Estonia, Russia and Estonian Russians. Tartu, 2016, 152 p.
15. **Liisa Talving.** Economic conditions and incumbent support: when and how does the economy matter? Tartu, 2016, 166 p.
16. **Ryhor Nizhnikau.** Externally Induced Institutional Change in the EU's Eastern Neighbourhood: Migration and Environment Reforms in Ukraine and Moldova in 2010–2015. Tartu 2017, 218 p.
17. **Kats Kivistik.** Relevance, Content and Effects of Left-Right Identification in Countries with Different Regime Trajectories. Tartu 2017, 204 p.
18. **Lukas Pukelis.** Informal mutual oversight mechanisms in coalition governments: Insights from the Baltic states for theory building. Tartu 2018, 145 p.
19. **Shota Kakabadze.** "The Caucasian Chalk Circle": Georgia's Self at the East/West Nexus. Tartu 2020, 186 p.

20. **Maksim Kulaev.** Trade unions, transformism and the survival of Russian authoritarianism. Tartu 2020, 151 p.
21. **Juhan Saharov.** From Economic Independence to Political Sovereignty: Inventing "Self-Management" in the Estonian SSR. Tartu 2021, 161 p.
22. **Andrii Nekoliak.** 'Memory Laws' and the Patterns of Collective Memory Regulation in Poland and Ukraine in 1989–2020: A Comparative Analysis. Tartu 2022, 263 p.
23. **Ivan Ulises Kentros Klyszcz.** How Does Violent Conflict Affect Para-diplomacy? An Exploratory Research with Cases from the North Caucasus. Tartu 2022, 200 p.
24. **Lelde Luik.** Re-evaluating the Role of Representative Institutions in Radical Democratic Theory: Lessons from Democratic Identity Construction in Latvia. Tartu 2023, 149 p.
25. **Ionut Chiruta.** Triadic Nexus Relationships in an Age of Populism: Interactions between Hungary, Romania and the Hungarian Minority in Szeklerland. Tartu 2023, 201 p.
26. **Sanshiro Hosaka.** Nothing but Politics? Explaining the Reproduction of Russian Narratives About the Events in Ukraine Among Japanese Scholars and Intellectuals 2014–2019. Tartu 2025, 224 p.
27. **Eoin Micheál McNamara.** The Risk Society's Stabilisation Failure? An Analysis of NATO and the International Security Assistance Force in Afghanistan. Tartu 2025, 370 p.
28. **Butrint Berisha.** Exploring the Role of Civil Society Organisations (CSOs) in Foreign Relations of De Facto States: A Comparative Analysis of Kosovo, Palestine and Taiwan. Tartu 2025, 236 p.
29. **George Spencer Terry.** Demanding Subjectivity: The Radical Right's Use of Discursively Empty Referent Objects within a Post-Foundational Logics Framework. Tartu 2025, 139 p.
30. **Michael Cole.** The People, the Elites and the Russia Factor: A Comparative Study of Populist Discourses in Georgia and Ukraine. Tartu 2025, 242 p.
31. **Logan Carmichael**. Cybersecurity Governance Responses in the Estonian Digital Governance Model, 2007–2023. Tartu 2026, 170 p.
32. **Stefan Dedović**. European Union Digital Integration: Exploring the development and governance of cross-border digital public services. Tartu 2026, 161 p.
33. **Sandra Hagelin**. Speaking Borders, Speaking Europe: Entangled Borders in Governmental Discourse Across the Baltic and Nordic Spaces. Tartu 2026, 265 p.