Voting Under Pressure: Perceptions of Coercion and Counter-Strategies in Internet Voting

Your N. Here
Your Institution

Second Name
Second Institution

Third Name
Third Institution

Fourth Name
Fourth Institution

Abstract

While internet voting can enhance democratic participation, concerns about voter coercion have emerged due to the uncontrolled voting environment. To mitigate this, researchers have proposed different types of *counter-strategies*, allowing voters to cast their intended vote despite being coerced. The success of the counter-strategies depends on the voter performing the procedure correctly so that their intended vote is cast, while at the same time, the coercer is not alerted to the voter's attempt to circumvent coercion. We conduct semi-structured interviews ($N = 26$) to investigate (1) general perceptions regarding coercion risks in internet voting and (2) voters' perceptions of six types of counter-strategies concerning their effectiveness. Our findings show that perceptions of voter coercion are shaped by societal factors, particularly the political and socio-economic context of a country. Furthermore, our findings reveal that the voter's perception of the effectiveness of counter-strategies depends on both the technical and personal skills of voters, concrete risks, such as last-minute coercion, and ease of use. In particular, memorability appears to be a key factor, as most counter-strategies require voters to remember a secret. Overall, our findings pave the way for future research aimed at developing user-friendly solutions that are effective against voter coercion.

1 Introduction

Internet voting systems are an opportunity to make elections more accessible for disabled voters and for those abroad who have limited access to physical polling places. Moreover, internet voting systems have the potential to increase participation in a world with declining voter turnout [50]. However, implementing internet voting introduces security risks due to the uncontrolled voting environment, as vote secrecy cannot be guaranteed in the same way as it would be ensured in traditional voting booths in polling stations, with poll workers being able to control that voters cannot be observed while being in these booths. One particular risk is voter coercion, where an adversary could force or bribe [1] the voter to cast their vote in a particular manner, undermining the integrity of election results [27]. In order for the coercion to be successful, the adversary furthermore needs to have a possibility to confirm that the voter is complying to avoid situations where the voter lies to the coercer but nonetheless votes according to their own wishes. In internet voting, such confirmation can be achieved through the so-called *over-the-shoulder coercion*, that is, the coercer directly observing the voter during vote casting, either by being physically present next to the voter or employing techniques like monitoring the voting device's screen remotely.

To mitigate the problem of voter coercion, various solutions, referred to as counter-strategies, have been proposed [7, 27, 32]. The main idea behind these counter-strategies is to provide a way for the voter to deceive the coercer – that is, acting during vote casting in a way that looks indistinguishable for the coercer from actual compliance, but at the same time making it possible to vote according to the voter's actual intention. If successful, the voter is thus able to cast a true vote or at least cancel the coerced vote, while the coercer has no possibility of detecting it.

However, the effectiveness of these counter-strategies depends on whether the voters can execute them. Previous research, however, has identified a number of assumptions about the voters' behaviour and capabilities that the currently proposed counter-strategies rely on [29]. The empirical validation of these assumptions has been very limited yet. As such, while a few experiments investigate the usability of specific

[1] For the sake of this work, we consider vote buying as a form of coercion, as a form of illegitimate influence on voters' decision.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2025.
August 10–12, 2025, Seattle, WA, United States.

voting systems implementing a variant of proposed counter-strategies, no in-depth investigation has been conducted of how voters would perceive the feasibility of different types of counter-strategies – that is, the extent to which the counter-strategy would be effective against coercion and its usability for the voters – and the risks connected to them in a real-world election. Additionally, to understand voters' acceptance of voting systems built around these counter-strategies or anti-coercion mechanisms in general, the voters' perception of voter coercion risks, coercer's tactics and capabilities is important to investigate. Yet, little qualitative research has explored how voters perceive the issue and whether they consider it a significant risk. In this work, we address these gaps by investigating the following research questions.

RQ1 How do voters perceive the risk of coercion in internet voting?

RQ2 How do voters perceive the feasibility of counter-strategies to ensure coercion-resistance in internet voting systems?

To address our research questions, we conduct semi-structured interviews with a total of $N = 26$ participants. We present the participants with three scenarios and ask them whether they perceive these scenarios as instances of voter coercion to address **RQ1**. Additionally, we inquire about their concerns and experiences with voter coercion to further address **RQ1**. To address **RQ2**, we introduce participants to six different types of counter-strategies. The six types were selected, extending the taxonomy from previous research [29] with findings from recent literature. For each type of strategy, we ask our participants about their perceptions of these strategies' effectiveness in protecting against voter coercion, along with their assessments of the strategies' usability. We conduct a thematic analysis using an open coding approach to answer our research questions. Our findings are as follows:

RQ1 Our participants perceptions are shaped by societal factors (e.g., hierarchical structures), socio-economic conditions (e.g., their financial situation), and individual aspects (e.g., awareness of coercion or the ability to resist it). While most do not perceive coercion as a concern in their home countries — where, except for one, none has personal experience with it — they are more concerned about coercion risks in less democratic countries, autocracies, and developing nations. Their concerns stem from reports of coercion tactics, such as vote-buying schemes in economically disadvantaged countries and intimidation tactics in places like Russia, highlighting how adversaries exploit economic vulnerability and political structures to exert influence.

RQ2 The participants emphasise key factors that determine the feasibility of the investigated counter-strategies. In particular, they note an issue with *memorability* (e.g., requiring the voter to remember secrets) in the investigated counter-strategies. Other factors include the personal characteristics of the voter (e.g., being able to convincingly lie to a coercer if needed), their environment (e.g., having a trusted person whom they can contact when not being observed by the coercer), and technical skills. At the same time, while voters do find selected counter-strategies sufficiently easy to apply, they are aware of limitations of these counter-strategies, mentioning specific actions the coercer might do to prevent the counter-strategy from being effective. Our findings, therefore, highlight a trade-off between usability and security in voters' perceptions of the counter-strategies.

Overall, we conclude that the participants do not perceive voter coercion as a significant issue in their native countries, which can affect their acceptance of counter-strategies in Internet voting systems, especially for the counter-strategies requiring additional steps even when the voter is not under coercion. The balance between usability, security, and potential risks remains a challenge for the counter-strategies.

2 Related Work

Security of Internet voting. As Internet voting systems became available for real-world elections across the world, security vulnerabilities in these systems have been identified [23, 26, 52]. Correspondingly, security risks of Internet voting have been thoroughly discussed by researchers and policy makers. Following these discussions, a guideline proposed by the Council of Europe specifies such properties as vote secrecy and verifiability that Internet voting systems need to satisfy in order to adhere to principles of democratic elections [42]. Satisfying these properties, however, present a challenge due to the uncontrolled environment in which the voting takes place. As such, since the voters use their own devices and networks to cast their vote, which, as opposed to the environment and infrastructure in polling stations, cannot be easily scrutinised by election officials or observers. As a result, techniques that address the risks of such an uncontrolled environment (e.g., a compromised voting device) have been introduced, enabling voters to verify that their vote has indeed been cast for their intended candidate [13], or to ensure that their cast vote can remain secret even in the presence of an adversary eavesdropping via the voting device [47] or of a coercer capable of directly observing the voter's environment (e.g., by being in the same room as the voter during vote casting) [12]. Our work focuses on the techniques designed to protect against voter coercion.

Empirical studies of human factors in Internet voting systems. Since the aforementioned techniques rely on voters being able to correctly perform these techniques, a number of empirical studies have been conducted that evaluate the usability of Internet voting systems. As such, several studies

investigated the usability and general voters' perceptions of verifiable voting systems [1, 6, 14, 16, 20, 28, 33, 34, 36, 38, 57]. While some of these studies have demonstrated sufficient usability of their investigated solutions, others have revealed issues related to voters' involvement in verifying their vote, such as not being able to complete the verification or to detect vote manipulations, as well as general misconceptions and lack of trust related to verifiability in Internet voting. Further studies focused on investigating the usability of code-voting solutions aimed at protecting vote secrecy against a compromised voting device [30, 37, 54], showing varying levels of usability of the investigated systems; however, they conclude that such systems are unlikely to be usable for complex elections with a large number of candidates and/or complex voting rules. Overall, these studies show that introducing procedures to the voting process that are unfamiliar to voters can be an issue, especially if these procedures are too complicated for the voters to perform or their purpose and their role in protecting the security of the votes is unclear to the voters. In our study, we focus on perceptions and potential usability issues of voters with regards to techniques designed to avoid voter coercion.

Coercion resistance in Internet voting. A substantial number of technical solutions, known as counter-strategies, have been offered to address the issue of voter coercion [4, 7–9, 11, 15, 21, 24, 25, 31, 32, 45, 46, 48, 49, 51, 58–61]. These solutions enable voters to deceive coercers by appearing to comply while ensuring that coerced votes are not counted in the final results. A classification of such counter-strategies divides them into three types – namely, *fake credentials*, *masking*, and *deniable vote updating* [29]. Furthermore, the analysis of these types has identified a number of assumptions about the voters' capabilities required to apply these counter-strategies successfully, such as being able to remember secret credentials without writing them down and to enter these credentials correctly without making a mistake. The study concludes that usability issues might prevent these counter-strategies from being effective, however, without conducting an empirical investigation to validate these conclusions. Further works have focused specifically on usability of coercion-resistant voting in proposing their own solutions [19, 40, 41], however, these solutions have not been empirically evaluated.

To the best of our knowledge, only a few user studies have evaluated the usability of counter-strategies in coercion-resistant voting, namely, investigating the counter-strategies based on *fake credentials* [10, 39]. Cristiano et al. [10] report a mean SUS score of 84.9, with all participants managing to complete their tasks within ten minutes. However, the study finds that the participants write down their credentials, reducing the offered protections against coercion resistance. Merino et al. [39] find a mean SUS score of 70.4, with 95% of the participants exposed to fake credentials understanding their use. However, they report that 10% of these participants mistakenly voted using a fake credential, which in a real-world election would result in these votes not being counted.

Only one study has investigated how voters perceive the threat of voter coercion, vote-buying, and their experiences with it in the USA [39]. The study reports that 26% of participants have personal experience with coercion or know someone who has. Participants consider demands for proof of purchase (e.g., a selfie with their ballot containing the coercer's demanded choice) to be the most likely coercion method, while threats of harm are considered least likely. In terms of the source of coercion, the study finds that family members are considered to be the most common, with 21% rating this scenario as extremely likely.

In our study, we extend on the investigation and classification of counter-strategies from previous research [10, 29, 39] and conduct a user study to understand voters' perceptions about usability and risks involved in various types of counter-strategies as well as general perceptions about voter coercion in Internet voting.

3 Counter-strategies

A study conducted a systematic literature review to identify proposed counter-strategies [29]. The paper identified three types of counter-strategies: fake credentials, deniable vote updating, and masking. In this paper, we apply the same methodology to identify counter-strategies proposed between 2020 and the present. We identify three new counter-strategies: *decoy tokens*, *flexible vote updating*, and *signal-based nullification*. This section provides an overview of the six types of counter-strategies to achieve coercion resistance. We describe the counter-strategies on a general level and provide external references for further details.

Fake credentials. Each voter receives a unique secret credential during voter registration in a controlled environment, where the coercer is absent. When voting, the voter uses their true credential to authenticate themselves to the voting system. In the case of coercion, the voter uses a fake credential to authenticate themselves. This fake credential is accepted by the voting system without triggering an authentication error, and the vote cast with the fake credential is excluded from the final tally. This strategy allows the voter to cast a legitimate vote when they are not under observation by the coercer. We refer to [7, 12, 27] for a deeper description of fake credentials.

Masking. Each voter receives a unique secret masking value during voter registration in a controlled environment, where the coercer is absent. When casting their vote, the voter masks their ballot using a function that combines their intended vote with the masking value. In the tallying phase, the voting system can extract the vote from the masked ballot because it knows the voter's masking value. In the case of coercion, the

voter casts the same masked ballot but provides the coercer with a fake masking value. This will make the masked ballot appear to be following the coercer's instructions. We refer to [56, 61] for a deeper description of masking.

Deniable vote updating. The voter follows the instructions of the coercer and casts a vote according to their preference. Once the coercer is gone, the voter casts their true vote and overwrites their coerced vote. We refer to [24, 32] for a deeper description of deniable vote updating.

Decoy tokens. Each voter receives a unique set of secret voting tokens during the voter registration in a controlled environment, where the coercer is absent. One token is valid, and the rest of the tokens are fake. When voting, the voter assigns their valid token to their preferred candidate and the remaining fake tokens to other unique candidates. In the case of coercion, the voter assigns one of the fake tokens according to the coercer's instructions, while they assign their valid token according to their own preference. The fake voting tokens are discarded in the final tally. We refer to [31, 51] for a deeper description of decoy tokens.

Flexible vote updating. The voter has two scenarios with different actions to follow to deceive the coercer. In the first scenario, the voter has not cast a legitimate vote before the coercion happens and follows the instruction of the coercer by casting a coerced vote. Once the coercer is gone, the voter returns to update their vote. However, the voter must provide a list of indexes with references to all their previous cast ballots together with their new vote for the voting system to accept and tally the updated ballot. In the second scenario, the voter has cast a valid vote before the coercion happens. In this scenario, the voter casts a vote according to the coercer's preference, but the voter provides an incorrect list of indexes with references to their previous cast ballots. The voting system will recognize this as a coerced vote and not update this newly cast ballot. We refer to [21] for a deeper description of flexible vote updating.

Signal-based nullification. Each voter registers two public keys, one for YES and one for NO, during a controlled registration phase where the coercer is absent. Further, the voter retains the two corresponding private keys. Until tallying, the voter can recruit one or more helpers, share their private keys, and agree on a signal with them. In case of coercion, the voter or a helper demonstrates knowledge of a private key to the voting system (without revealing it) to cancel the vote. If the voter does not have the option to cancel their vote themselves, they use the agreed signal to instruct the helpers to do so. This strategy allows only vote cancellation. We refer to [8] for a deeper description of signal-based nullification.

4 Methodology

To understand how the participants perceive the problem of voter coercion and the different counter-strategies, we conducted in-person semi-structured interviews. In this section, we describe the interview guide, recruitment, ethical considerations, and the data analysis in our study.

4.1 Interview Guide

The interview guide was prepared in three languages: English, German, and Danish. The English version was prepared first and iterated in three pilot studies. The translations into the other two languages were done by paper authors who were fluent in these languages. To furthermore validate the consistency among the translated versions, the translations were translated back to English using a large language model, and the output was compared with the original interview guide in English to detect any flaws with the translation.

The guide was structured as follows [2]. First, the participants were told about the purpose of the study and asked to read and sign a consent form (see Appendix 8), which stated that they could withdraw at any time. The participants were furthermore provided with a one-sentence description of voter coercion, namely, 'Coercion in voting happens when someone pressures or forces you to vote in a way they want you to vote', to guarantee a common understanding of the research topic we are investigating. The rest of the interview guide consisted of two main parts, each corresponding to one of our research questions.

4.1.1 Part 1: General attitudes towards coercion (RQ1)

Discussion of coercion scenarios. To address **RQ1**, we included three different scenarios that might be interpreted as voter coercion, derived from previous research [39]. The scenarios were chosen to reflect the variety of forms voter coercion might take and different roles the coercer might have [3]. The scenarios were as follows:

- Imagine you're logged into the online voting platform from home. A family member stands beside you and pressures you to vote for a specific candidate.
- Imagine someone offers you money if you can provide proof for voting for a specific candidate.
- Imagine your boss is watching your screen while you cast your vote on your computer, pressuring you to vote for a specific candidate, or you will get fired.

The scenarios were presented in an order determined by the participants picking one paper at a time from a set placed

[2] The full interview guide is provided in the Appendix 8

[3] Note that similar to previous research on voter coercion, we included vote-buying as a form of voter coercion as well.

face down on a table. For each scenario, the participants were asked whether they considered the scenario to be a case of voter coercion and to explain their reasoning. Additionally, we asked participants to assess the likelihood of the scenario occurring to them personally and to someone in general.

General discussion of voter coercion awareness and concerns. After discussing the scenarios, we asked the participants whether they knew of examples of coercion in their native country or elsewhere. Furthermore, we asked them about their concerns regarding voter coercion in both their native country and other parts of the world.

4.1.2 Part 2: Counter-strategies (RQ2)

To address **RQ2**, we included six descriptions in the interview guide, one for each of the counter-strategies described in Section 3 (see also Appendix 8 for the full text of the descriptions). To ensure that these descriptions were understandable to lay people, we had a person without any technical knowledge about the topic read through the descriptions of the counter-strategies and provide us with feedback regarding their understandability. The descriptions were presented to the participants one at a time in random order, and the participants were asked what they thought of the feasibility of each counter-strategy to resist attempts of voter coercion. Moreover, we asked them how doable they considered the counter-strategies to be.

Demographics. Finally, we included questions on sociodemographic information, such as gender, age, and level of education. Additionally, we included a scale-based question to assess participants' IT skills.

4.2 Recruitment and Ethics

For recruitment, we used a combination of purposive and convenience sampling [5]. The study was conducted between July and early September 2024, shortly after the EU election, which took place between June 6 and 9, 2024. For convenience, we distributed flyers at two universities, one in Denmark and one in Germany (see Appendix 8). Additionally, we used Facebook to share posts in public student groups associated with three universities, one in Germany and two in Denmark (see Appendix 8). Finally, we used snowball sampling for the recruitment by asking recruited participants whether they knew about other potential participants for the study [5]. We stopped recruiting new participants when data saturation was reached [22].

We coordinated the process alongside the ethical guidelines and received approval by the ethical committee of the German institution. At the Danish institution, ethical approval is not mandatory. However, we completed a privacy impact assessment for the project, which was approved by the institution's legal department. Participants from Germany received ten euros as reimbursement, aligning with the minimum wage. Denmark has no minimum wage, so the participants from Denmark received a gift card worth 13.41 euros (100 DKK) for an ice cream shop or a chocolate shop. For the Danish participants, the higher compensation is due to generally higher living costs, and the choice of providing gift cards instead of direct payment is due to institutional regulations. Prior to the interview, participants were asked to sign a consent form outlining the study's purpose, withdrawal options, and data handling procedures. Contact details for the researchers were also provided for any inquiries.

4.3 Data Analysis

All interviews were auto-recorded, and they were transcribed using Amberscript and WhisperAI, which are tools approved for use by our institutions. Afterwards, the two interviewers reviewed the transcripts to ensure alignment with the original recordings. We used MAXQDA to support a coded thematic analysis of the interviews, employing an open coding approach to address the research questions. We coded the interviews at the question level and to analyse RQ1 and RQ2 with separate sets of codes to ensure that the results for the two research questions remained separate. The two researchers who conducted the interviews also carried out the coding in their respective languages. To develop the initial codebook, the two coders independently coded a randomly selected interview translated into English and discussed their findings. Subsequently, they each coded two interviews in their respective languages to identify additional codes, recognising that a single interview would not capture all potential codes. Based on these interviews, they discussed and revised the codebook. To ensure agreement between the coders, four interviews were translated into English and coded independently. An iterative process of discussion and refinement of the codebook followed, ultimately reaching a Cohen's Kappa of 0.76, suggesting substantial agreement between the coders [44]. After the acceptable level of agreement was reached, the rest of the interviews were coded by each coder separately in their native language. To identify the themes, we grouped the codes using post-its to visualise patterns and connections. We refer to Appendix 8 for the codebook.

5 Results

In this section, we present the results of our study. We recruited 26 participants in total, with 14 participants from Denmark and 12 from Germany. We refer to Appendix 8 for demographics of the participants. In the following, we refer to the participants using the notation P# (e.g. P1 says: "quote").

5.1 RQ1: General attitudes towards coercion

Table 1 provides an overview of how many participants consider the three scenarios to be voter coercion. All participants considered the third scenario (*boss coercion*) to be voter coercion. For the second (*vote-buying*) and first (*family coercion*) scenario, the participants provided a mix of responses, with a few participants expressing conditional views. Overall, none of the participants had personal experience with voter coercion or knew someone who had experience with it. Through our analysis, we identified three themes: societal influences, individual influences, and influence and pressure tactics. Below we present the findings for each theme.

Scenario	Yes	No	Depends
Scenario 1 - Family	23	0	3
Scenario 2 - Vote-buying	23	1	2
Scenario 3 - Boss	26	0	0

Table 1: Participants responses to whether they consider the different scenarios to be coercion.

5.1.1 Societal Influences on Perceptions of Coercion

One theme is societal influences, which encompasses the following aspects: socio-economic-cultural context, country examples, public information, political manipulation and electoral influence, legality, and availability and transparency of information.

The **socio-economic-cultural context** is what participants mentioned most frequently, with a total of 198 mentions. In particular, they elaborated on the differences between democracies and autocracies and how the economic and cultural situation in a country affects the likelihood of an attacker trying to coerce a voter. This also relates to the specific **country examples**, which they provided in the interviews. They mentioned countries 61 times in total, such as Russia, China, and the USA. In general, the participants described these countries as less democratic, more autocratic, or less economically developed. P26 says: *"I would be more concerned about it, not just the USA. I believe there are many places, like the UAE and other poorer countries, that might struggle to manage it. In some places, like dictatorships such as Russia, it is even more likely. There are many things that can happen in countries where democracies are already unstable."* [4]. For the first scenario (*family coercion*), the participants elaborated on how certain cultures have more conservative family structures, which could increase the likelihood of a family member trying to coerce a voter. Additionally, they expressed concerns about family coercion in the case of younger adults living at home with their parents. P14 says: *"I can imagine that if it is a young voter, say someone in their late teens or early twenties, unsure of who to vote for, a father or family member might try to influence them."* For the second scenario (*vote-buying*), the participants highlighted how the socio-economic context influences the likelihood of someone offering a voter money, as people are in need of money. P17 says: *"I am half Pakistani, and it is a typical thing among poor people to give them money to vote for a certain party."* Further, P1 states that *"It depends on whether you are economically dependent on taking the money. If I tell a millionaire that I will give you 10 euros to vote for X, then he probably wouldn't do it. But if I tell a poor person that I will give you 1000 euros and you have to vote for X, then he would probably do it a lot more."* This emphasizes how economic hardship can make individuals more vulnerable to financial incentives, such as being paid to vote for a particular party.

The **public information** aspect covers shared or widely accessible information, such as news, social media, word-of-mouth, or general social awareness. Twelve different participants mentioned this 24 times. They perceived public information as a reason for not being concerned about coercion, as they did not know of any examples of coercion in their native countries from public coverage. Moreover, they believed that public coverage would discourage attackers from attempting coercion because such attempts would be published and result in reputation loss. Especially for the second scenario (*boss coercion*), the participants considered it unlikely that a party would offer money because of public information. P23 says: *"If it were a party, everyone would know about it fairly quickly because word spreads fast. So if someone was paid, others would find out. That would put them in a position where they could not really go through with it."*

Furthermore, the participants also perceived **political manipulation and electoral influence** as forms of voter coercion. 23 participants mentioned this 63 times, covering a range of tactics from political targeting through advertisements to the illegal manipulation of ballots. P26 says: *"It could be small things like closing a polling station or issues with digital voting machines. There has been tampering, or people being told to vote on a specific machine instead."* Stressing this different perception of voter coercion, P7 says that *"I have the feeling that sometimes it doesn't really come to direct voter coercion, but instead the cast votes are being altered or not tallied at all."* Similarly, even the way in which election outcomes can be altered based on voting districts is seen as forms of coercion, as P1 states *"The thing with gerrymandering in the US, that would also apply for me here."*

Twelve participants mentioned **legality** 20 times, which influences whether they perceived the scenarios as voter coercion. P14 says: *"I would find that extremely uncomfortable and downright illegal because I know that no one is allowed to look over your shoulder when you're casting your vote."*

Finally, **availability and transparency of information** covers access to information and issues related to the availability and transparency of information. Four participants

[4] This and other quotes were translated from their respective language in English for the paper.

mentioned this aspect seven times. P12 explains why influencing the availability and transparency of information could be some form of coercion: *"I would even go so far to say that some Social Media Posts and Reels and things like that. Depending on how they are designed and how the algorithm behind them works and in what intensity and frequency and which messages that can also have an influence, which is more so unconsciously. But yes, still a certain degree of coercion because you are led towards an opinion."*

5.1.2 Individual Influences on Perceptions of Coercion

Another theme is individual influences, which encompasses the following aspects: individual context and the voter's capabilities.

The **individual context** of the voter is an aspect that encompasses the voter's financial circumstances, family situation, and relationship with the coercer. This is similar to the socio-economic-cultural context code (see section 5.1.1). However, this aspect focuses on the individual voter, whereas the other focuses on voters on a more general level. 25 participants highlighted this aspect with a total of 141 mentions. For the first scenario (*family coercion*), eleven participants believed that it depends on the individual context of the voter whether the scenario is coercion or not. They highlighted that for some voters, it will feel like coercion, while it will not for others. Moreover, the participants highlighted that it can be difficult to withstand coercion if the voter has a close relationship with the coercer. P19 says: *"I can feel that it is somehow more important for me to agree with my family member than it might be to agree with my boss."* P4 explains that *"It depends on how politically informed you are. I know it from people who are not politically informed or even interested. Their parents vote for something, so they also vote for it. [...] So I believe, if their parents would pressure them, they would be easy to influence."*

The **voter's capabilities** deal with the specific capabilities of the voter, and 24 participants highlighted this 79 times. This aspect includes voters' ability to move freely or the strength to withstand coercion attempts. The participants emphasised that they have the ability to not cast a vote while at work to avoid coercion in the third scenario (*boss coercion*). Additionally, they mentioned how their technical skills can help them avoid family coercion in the first scenario. P18 says: *"Because I simply believe that I would withdraw in such a scenario."* P1 says: *I think if you feel that this could happen, you would be able to vote somewhere else because work is not the only place where you could vote.*

5.1.3 Influence and pressure tactics

One theme is influence and pressure tactics, which refer to situations where participants perceived voters as being influenced, coerced, or pressured. This theme specifically focuses on external pressures or influences, involving concrete techniques or actions that affect voter behaviour. All participants mentioned tactics with a total of 146 times.

For the first (*family coercion*) and third (*boss coercion*) scenario, the participants perceived it as coercion because someone is **physically looking over the voter's shoulder** while they cast their vote. P22 says: *"But yes, because your boss is standing there, looking over your shoulder while you are voting."*

For the second scenario (*vote-buying*), the participants perceived it as coercion because it includes the **use of money** as a pressure tactic. P25 says: *"I feel it is about exchanging value — vote for us, get money. This creates pressure to vote a certain way, especially for those who don't care much about their vote."* However, one participant does not perceive it as coercion. P21 says: *"Because you are not being forced. You have a choice here, where you do not really risk anything."*

For the third scenario (*boss coercion*), the participants also perceived it as coercion because the pressure tactic exploits the **power imbalance** between a boss and an employee. Furthermore, this tactic **threatens the voter's livelihood**, as a lay-off could result in the loss of their financial income. P16 says: *"Because it is a boss who has the power to fire me. That makes it have a greater consequence."*

Additionally, the participants perceived **blackmailing, and hacking and monitoring of the voter's device**, as coercion. P26 says: *"If you are on a mobile device and the hacker can see your screen, then it is very easy to step in and say, 'Now you go in and vote here and here, or else it disappears."*

5.2 RQ2: Counter-strategies

In our analysis, we identified four key themes: voter capabilities, risks, security and privacy considerations, and system attributes. Below, we present the findings for each theme.

5.2.1 Voter's Capabilities

One theme is the voter's capabilities, which encompasses the following capabilities: cognitive skills, such as memorability and understandability, assertiveness, and technical skills. Table 2 provides an overview of the required capabilities of the voter for each counter-strategy.

The success of almost every counter-strategy relies on the voter's ability to remember specific elements such as credentials, tokens, or other components. 25 participants mentioned **memorability** with a total of 119 times. Moreover, they considered alphanumerical passwords harder to recall than visual symbols (e.g., coloured shapes). P13 says: *"Remembering symbols is easier for people; I think it is better than the password. It is easier for people to remember whether it was a triangle, an orange triangle, or a blue circle."*

Some strategies are considered difficult to understand by the participants (e.g., masking). 14 participants mentioned

	Memorability	Understandability	Lying	Technical skills
Fake credentials	+	-/+	+	-
Decoy tokens	+	-/+	+	-/+
Flexible vote updating	+	-/+	+	-
Deniable vote updating	-	-	-	-
Masking	+	+	+	
Signal-based nullification	+	+		

Table 2: Voter's capabilities required for the different counter-strategies according to participants. Green cells with (-) are when a skill is not required for a counter-strategy to work. Red cells with (+) are when a skill is required for a counter-strategy to work. Yellow cells with (-/+) are when a skill is required/not required for a counter-strategy to work according to different participants. Empty cells indicate that no participants mentioned the aspect for the counter-strategy.

understandability 35 times, 14 of which are about masking. P19 says: *"Well, I have a hard time fully understanding the addition of numbers; maybe others will too."*

The success of most counter-strategies relies on the voter's assertiveness, especially the deceptive skill of the voter. 20 participants mentioned **assertiveness**, as the ability to convincingly lie under pressure, 64 times. P14 says: *"But I also think it requires a bit of the person who votes. They also have to be good at lying or just be able to think clearly and say, 'no, I haven't,' or say 'I haven't voted,' even if you have already voted."*

Finally, participants considered some strategies as easy to do (e.g., deniable vote updating), while other strategies raised mixed perceptions (e.g., decoy tokens). 12 participants mentioned **technical skills** 23 times. P23 says: *"Most people can manage drag-and-drop."* P6 states that *"You only have to put in an arbitrary password, which is not hard because you just press random buttons."*

5.2.2 Risks

Another theme is concrete risks, which the participants referred to as risks affecting the effectiveness of the counter-strategies. This theme encompasses the following risks: typo mistake, casting a wrong vote, last-minute coercion, and cancelling a vote by mistake.

The risk of a **typo mistake** is associated with fake credentials, which nine participants mentioned 13 times. P20 says: *"You think you voted, but you entered the information incorrectly, so you did not vote anyway."*

The risk of **casting a wrong vote** is associated with decoy tokens, masking and flexible vote updating, which 14 participants mentioned 34 times (15 mentions for decoy tokens, 15 for masking, and four for flexible vote updating). P23 says: *"But it could be risky to have the possibility of voting incorrectly — even just by mistake. If you forget which symbol was correct...and you could also vote incorrectly without necessarily being coerced."* Moreover, specifically for flexible vote updating, the participants identified the risk that they may accidentally cast a wrong vote if they submit the wrong time when trying to change their vote in an uncoerced case. For example, P7 states: *"I see some potential here, that you accidentally forget to add the right time, and your new vote will be recognized as a coerced vote."*

The risk of **last-minute coercion** is associated with deniable and flexible vote updating, and 16 participants mentioned this 26 times (19 mentions for deniable vote updating, seven for flexible vote updating). This occurs when the coercer waits until the voting phase ends to pressure the voter, leaving no chance to update their vote. P21 says: *"You cannot ensure that people won't be pressed just before the election closes."* P10 states that *"If the coercer stays with you until the end of the election and you can't change your vote, it is problematic."*

The risk of **cancelling a vote** covers several risks associated with the signal-based nullification strategy, which 15 participants mentioned 29 times. This includes the potential to cancel another person's vote by mistake because voters might fail to create a unique code or because a signal is misinterpreted. P14 says: *"I also think you can be like, 'Oh, okay, should I take this as a signal, or wasn't it a signal?' There will definitely be situations where you consider something to be a signal without it being a signal."* Moreover, this code also encompasses situations in which participants addressed dissatisfaction with the fact that it is only possible to revoke your vote without being able to recast it again, resulting in the risk of one's intended choice not being represented in the election. P9 states that this strategy *"It is difficult, as it could lead to certain voters or voter groups always being forced and then a complete group of voters almost virtually disappears.*

5.2.3 Security and Privacy Considerations

One theme is security and privacy considerations regarding the counter-strategies. It encompasses the following aspects: coercer's capabilities and knowledge, security of knowledge-based secrets, writing down knowledge-based secrets, system feedback, security of authentication, depending on others, and security of voting several times.

The **coercer's capabilities and knowledge** are security considerations associated with all counter-strategies, and 25

participants mentioned it with a total of 122 times. The participants considered it to be public knowledge how the counter-strategies work, independently of the type of counter-strategies, which they believed the coercer will use to their advantage. This could be by pressuring the voter to reveal their knowledge-based secret (e.g., masking value) or waiting until the last minute to coerce (e.g., deniable vote updating). Additionally, they believed that the coercer is likely to suspect the voter of using a counter-strategy. P16 says: *"I think if this is a system that is known to everyone, then if it is a manipulative partner, then it might not work as well because they would know that you are getting that code, and then they would start trying to pressure you to give this code to them as well."*

The **security of knowledge-based secret** is an aspect associated with fake credentials, decoy tokens, and masking, and 18 participants mentioned this 37 times. The participants considered a strategy to be effective because the voter is the only one knowing their secret (e.g., credential). P23 says: *"Well, again, here you have something that only you know. I think that has proven to be a reasonably secure solution. If you are the only one who knows it, then you can make the others believe many things and then vote for the one you want to vote for."*

Another security consideration associated with several strategies is about **writing down knowledge-based secrets**, and the participants mentioned it 35 times (19 mentions for fake credentials, five for masking, four for decoy tokens, and two for each of the remaining strategies). The participants perceived a strategy to be less secure if the voter is writing down their knowledge-based secret as they connects this with the coercer's capabilities: P8 says: *"Remembering a unique password is difficult, so I believe you would write it down somewhere. When you are not prepared and someone comes in while you are voting and the password is there, the coercer could just vote for you directly."*

16 participants mentioned **System feedback** as a security consideration 29 times. It is associated with fake credentials, masking, and deniable and flexible vote updating. The participants argued that the voting system should not display any feedback to ensure the effectiveness of the counter-strategies and is therefore somewhat related to the **security of knowledge-based secret**, as P1 explains that *"You have a secret that the attacker does not have, and the attacker has to trust you because the system does not give any feedback"*. Further, P20 says: *"As long as you do not get confirmation emails or have a browser history that someone can follow."*

The **security of authentication** is a security consideration associated with deniable and flexible vote updating, according to five participants, which they mentioned seven times. The participants perceived flexible vote updating as more secure compared to deniable vote updating because the voter needs to prove their identity by referring back to a previous vote to update their vote. P25 says: *"Then there is deniable vote updating. I actually think that's generally okay. I just think there is some security missing in that part. Then I have flexible vote updating, and I think that might is the best because I feel like you have to log in differently, where you can't just go back and forth. There's also an awareness that when you change your choice, I think that might make it a little more secure."*

Depending on others is considered to be a privacy and security concern related to the signal-based nullification strategy. 23 participants mentioned this concern 57 times. The participants expressed concerns that not everyone trusts others, and the coercers could be family members. P20 says: *"The thing about including family members and friends. I actually think that voting is a very private matter. It may also be that there are people who have neither family members nor friends."*

The **security of voting several times** is associated with deniable and flexible vote updating, which 12 participants mentioned 105 times. The participants expressed concerns about overloading the server and the possibility of coercion happening over a longer time period. P24 says: *"There is another problem that if we say all five million Danes think it is super fun to vote all the time, it could overload the system, and then it collapses."* However, they also perceived it positively that the voter has the opportunity to have a more secure situation later in the voting process to cast their intended vote because they can vote several times. P23 says: *"You go home and change it when you have a more secure situation."*

5.2.4 System Attributes

One theme is system attributes, which encompass the following attributes: convenience, closeness to established practices, flexibility, non-coercive cases, and general feasibility in practice. Table 3 provides an overview of the identified attributes for each counter-strategy.

The system attribute that the participants mentioned most frequently, with a total of 230 mentions, is **Convenience**. All participants highlighted this attribute. The participants perceived strategies requiring physical visits (e.g., fake credentials) or multiple complex steps to complete them (e.g., masking) as inconvenient. P18 says: *"Well, because there are too many steps involved. It requires too much for people to bother voting, I would say."*

Closeness to established practices is an attribute that covers how close the strategy is to the established voting practices and digital platforms. Eight participants mentioned this attribute 17 times. Among the strategies, deniable vote updating has the highest frequency, as the participants mentioned this nine times. P16 says: *"Because it seems like something you would normally do in connection with public authorities, that you log in with your ID. These are procedures that you have gone through before for something similar."*

Flexibility covers whether a counter-strategy is flexible to different scenarios of coercion. Seven participants men-

	Convenience	Flexibility	General feasibility in practice	Closeness to established practices	Non-coercive cases
Fake credentials	-/+	-		+	
Decoy tokens	-/+		-	-	-
Flexible vote updating	-/+	+	-	+	+
Deniable vote updating	+			+	+
Masking	-	-/+	-	-	-
Signal-based nullification	-/+	-	-		

Table 3: System attributes for the different counter-strategies. Green cells with (+) are when an attribute is fulfilled positively for a counter-strategy. Red cells with (-) are when an attribute is not fulfilled for a counter-strategy. Yellow cells with (-/+) are when an attribute is both fulfilled/not fulfilled for a counter-strategy. Empty cells indicate that no participants mention the attribute for the counter-strategy.

tioned this 14 times. The participants perceived flexible vote updating as flexible. P26 says: *"It gives you the flexibility to vote both before and after someone has blackmailed you into voting. And you can always come back and correct it."* In contrast, fake credentials and signal-based nullification are perceived as less flexible to different scenarios of coercion. 16 says: *"I might not think it works as well for some who could be very manipulative. But if it is for your boss, who just looks over your shoulder and tries to convince you, then it might work."*

The feasibility of a counter-strategy when the voter casts their ballot without being under any coercion is captured with **Non-coercive cases**. Nine participants mentioned this 13 times and perceived some strategies negatively and others positively in non-coercive cases. P16 says: *"If you are not subjected to pressure, then you only need to vote once."* Contrary, P7 states that *"I could imagine that lead to wrong cast votes. So, unintentionally it is from people who are not being coerced simply because they miscalculated.*

General feasibility in practice is an attribute that covers how participants perceived the general feasibility of the counter-strategies in practice. It encompasses factors such as the presence of significant gaps or pitfalls, as well as strategies that may appear effective in theory but fail to deliver in practice. Ten participants mentioned this 17 times, and they especially perceived signal-based nullification as incomplete, with 12 mentions. P24 says: *"So, it sounds like it was developed somewhat in an academic setting. It sounds great, but it doesn't work in practice."*

6 Discussion

6.1 RQ1: General attitudes towards coercion

Lack of concern about coercion. Our participants neither experienced voter coercion themselves nor were concerned about voter coercion happening in their home countries of Denmark and Germany, believing that it mostly happens in autocracies, weaker democracies, and developing countries. This lack of concern could be due to normalcy bias, which is the tendency to believe that things will remain as they have always been, making it difficult to imagine threats or changes in democracies [43]. Such lack of concern might be a barrier towards acceptance of voting systems that offer protection against voter coercion in case this protection comes at a price of more complicated voting procedures. While this might be a lesser issue for counter-strategies such as **deniable vote updating** that do not modify the voting process for voters not under coercion, counter-strategies such as **masking** might require additional voter education to facilitate their acceptance. On the other hand, if Internet voting is being discussed as an option to be used in large-scale elections, a country-wide risk assessment would be beneficial in understanding whether such counter-strategies need to be implemented at all, or whether the costs of a potentially more complicated and error-prone voting procedure outweigh the benefits of an additional protection against coercion.

Furthermore, as the lack of concern about voter coercion among our participants stemmed from their lack of personal experience with voter coercion and beliefs that their home countries are strong democracies where voter coercion is unlikely, these results are not generalisable worldwide. As such, a study with U.S. citizens finds that 26% of participants have experienced or know someone who has experienced at least one form of voter coercion, with family members being the most common source [39]. This highlights national differences and is consistent with the participants in our study mentioning the USA as an example of a country where they would be concerned about voter coercion. An important direction for future research would therefore be conducting further studies about perceptions of voter coercion in the USA and in other countries where voter coercion is perceived to be an issue.

Voter's personal circumstances. The influence of personal circumstances, such as the voter's financial situation or family relationships, also plays a role in how coercion is per-

ceived. While our participants, who are well-educated people living in bigger cities, might not be subject to voter coercion, individuals from another demographic background could be more vulnerable to it. Our participants elaborate on this, as they believe that possession of resources makes it easier to resist coercion, which is why they might not be subject to voter coercion. Furthermore, they can easily imagine how individuals with other circumstances are vulnerable to coercion. Thus, the question is whether a voting system should provide extra protection to those few who are potentially vulnerable to coercion or should focus on providing an easier solution for the majority.

Lack of internet voting-specific concerns. None of our participants pointed at increased risks of coercion introduced specifically by technology used in online elections. Instead, their concerns are rooted in broader societal attitudes and personal experiences rather than the online nature of the voting process itself. Such an absence of discussions of technology-specific risks can be explained by the fact that neither Denmark nor Germany uses Internet voting in large-scale elections; hence, most of the voters do not have personal experience with this technology. Yet, in case internet voting is introduced in either of these countries, the risks of voter coercion introduced by an uncontrolled environment might be underestimated by voters.

6.2 RQ2: Counter-strategies

Usability vs. security. Our participants' opinions on the presented counter-strategies revealed a conflict between the usability and security of these counter-strategies. As such, while they mention memorability as a potential issue for the success of almost every counter-strategy, they nonetheless emphasise the importance of keeping a **knowledge-based secret** (e.g., credential, or masking value) only known to the voter themselves for security reasons. This trade-off is a known issue in usable security, e.g., in usable authentication research focusing on passwords. However, the issue is exacerbated for coercion-resistant voting due to potential issues with storing the secret somewhere where the coercer can demand access, excluding solutions such as password managers. This issue has furthermore been noted by our participants: as such, while our participants suggested writing down or taking a picture of their knowledge-based secret (e.g., tokens) to remember it, they also consider this as a security issue if the attacker accesses the stored secret by finding or obtaining it through coercion.

As previous research on the usability of **fake credentials** avoided this problem either by letting the participants write down their credentials [10]. Hence, future work needs to focus on designing and evaluating other techniques either for the voters to remember their secrets without writing them down or for developers of the system to provide storage options not accessible to the attacker even in case of coercion. Such studies can furthermore be beneficial for counter-strategies other than *fake credentials* that rely on memorability – which, according to our participants, is every counter-strategy with the exception of deniable vote updating. A further potential usability issue mentioned by our participants for *fake credentials* is the possibility of a typo mistake, as the voting system will not provide any errors as feedback because of security reasons. While solutions have been proposed that are flexible enough to allow the voters at least some kind of mistakes (such as a single wrong digit) [18], the full range of mistakes voters can make when using *fake credentials* is still to be investigated. Further investigation is required for the usability of techniques such as panic passwords [11] that distinguish between real credentials, "panic" credentials that the voting system seemingly accepts as real while discarding the votes from the tally, and invalid credentials (which might include e.g., real credentials with a typo) that the voting system immediately declines, providing corresponding feedback to the voter.

A further example of the conflict between usability and security has been discussed in relation to the **deniable vote updating**. Most of our participants find this strategy to be the easiest to apply, and it has the advantage of leaving the voting process unchanged for non-coerced voters. At the same time, our participants note risks present within this counter-strategy, namely, a possibility for the coercer to wait until the last minute to coerce the voter, making it impossible to update the vote. Since this risk would not be an issue for the other investigated counter-strategies, the effectiveness of the deniable vote strategy in protecting against coercion can be seen as weaker compared to the rest of the counter-strategies. For real-world elections, decisions, therefore, need to be made on a case-to-case basis to determine whether the last-minute coercion risk outweighs the benefits of an overall simplicity of the counter-strategy. An open question that furthermore remains is how to communicate the relevant risks, in particular, the capacities of a potential coercer both to voters and to the decision-makers (e.g., election officials), particularly in relation to the scalability of an attack. The risk of last-minute coercion is furthermore mentioned as an issue for the **flexible vote updating** counter-strategy, despite this counter-strategy actually having mechanisms available to protect against this attack. Such a misconception highlights an issue with the strategy's understandability, and it remains an open question of how to explain the strategy without misrepresenting the risks.

Voter's personal circumstances. In addition to usability issues, our participants pointed to the personal circumstances of the voter regarding their environment, social circle, personality, and skills. As such, the participants are concerned about having to rely on others in **signal-based nullification** to be effective against coercion – either because the voters might be socially isolated and lack close trusted contacts or because the helpers themselves could potentially be the coercers.

The participants are particularly concerned about the lack of trusted helpers in the family coercion scenario. Consequently, they perceive signal-based nullification as ineffective against voter coercion in such situations. Deciding to use a particular counter-strategy should, therefore, take into account such personal circumstances – as such, studies need to be conducted to get a thorough understanding of the population that is of particularly high risk of coercion.

Participants further emphasise the resources and the skills required from the voter, especially for the counter-strategies that, according to the participants' perceptions, lack in convenience. Of particular note is a skill that, according to our participants, would be required in most cases of coercion, namely, the ability of the voter to lie to a coercer. As such, when discussing counter-strategies that rely on using a **knowledge-based secret** in front of the coercer (e.g., by authenticating with fake credentials), the participants highlight that individuals who are not comfortable with deception might struggle in convincing the coercer that they are indeed using the right secret. This raises an important point about the psychological and social challenges of implementing such counter-strategies, suggesting that personal traits, such as the ability to lie convincingly under pressure, could influence the effectiveness of knowledge-based secrets in preventing coercion. Still, it remains an open question of how the voter's assertiveness impacts the effectiveness of counter-strategies in practice.

Role of public information. Applicable to all counter-strategies, the participants consider publicly available information about the procedures voters have to perform to apply these counter-strategies to be a problem for their effectiveness in protecting against coercion. As such, our participants note that for counter-strategies implementing a knowledge-based secret, the coercer might try to be present during the disclosure of the knowledge-based secret or use extreme threats to make the voter reveal it. For counter-strategies vulnerable to last-minute coercion, the coercer might attack right before the deadline, making it impossible to update the vote. In general, the coercer might suspect that the voter is trying to deceive them if they know that an Internet voting system has implemented a counter-strategy, making it harder for the voter to convincingly deceive a coercer. On the other hand, information about available counter-strategies might discourage the coercer from attempting coercion. Namely, as the coercer will have no way of knowing for sure whether the voter complied with the coercer's instructions, they might decide that the risks they face attempting coercion are not worth the uncertainty of the result. Furthermore, making information about the voting system publicly available aligns with recommendations from experts [3, 35, 42, 55] and is perceived as improving election transparency and trust by the voters [2]. The specific trade-offs introduced by public information about counter-strategies therefore remain an open question, and an open challenge is how to design Internet voting systems that maintain transparency without making counter-strategies ineffective.

6.3 Limitations

Our findings may be subjected to bias due to the participants' lack of experience with Internet voting and the fact that they are only from Denmark and Germany. To partially address this bias, future studies should explore how voters from countries such as Estonia, with an Internet voting system utilising deniable vote updating, perceive the counter-strategies and the problem of voter coercion in Internet voting. Another limitation is that all the participants are between 22 and 30 years old with a university-level degree or are in the process of completing one. This limits the generalisability of our findings, but since younger people with high education are more likely to be first adopters of digital technologies; hence, in case Internet voting is introduced, this demographic is likely to be among the first ones using it [17, 53]. Additionally, the structure of the interview guide may have influenced participants' responses. Asking them to assess different scenarios for potential coercion may have led them to assume that vote buying was inherently considered a form of coercion. Furthermore, providing a clear definition of coercion might have constrained participants' ability to conceptualise possible coercion scenarios. However, our pre-study indicated that without a clear definition, participants also struggled to articulate precisely what constitutes coercion, highlighting the challenge of balancing guidance with open-ended exploration.

7 Conclusion

We conducted 26 semi-structured interviews to explore how voters perceive the issue of voter coercion as well as the usability and security of counter-strategies designed to resist coercion in Internet voting.

From our findings, we conclude that there is a general lack of awareness and concern about coercion among our participants, leading them to prefer a counter-strategy that is easy to use, namely, the **deniable vote updating**, which leaves the voting process in the absence of coercion unchanged. For this reason, this counter-strategy seems to be the most promising one from a voter's perspective. However, *deniable vote updating* also introduces the risk of last-minute coercion. Thus, for elections with a high risk for voter coercion, a more complex counter-strategy should be used. Future work should therefore focus on studying the effects of awareness about the risk of voter coercion on voters' acceptance of specific counter-strategies. Furthermore, future work should focus on improving and evaluating the usability of counter-strategies.

References

[1] Claudia Z. Acemyan, Philip Kortum, Michael D. Byrne, and Dan S. Wallach. Users' Mental Models for Three End-to-End Voting Systems: Helios,

Prêt à Voter, and Scantegrity II. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 463–474. Springer, 2015. Available at: https://dl.acm.org/doi/10.1007/978-3-319-20376-8_41.

[2] Samuel Agbesi, Jurlind Budurushi, Asmita Dalela, Christina Nissen, and Oksana Kulyk. How to increase transparency and trust in internet voting systems: An experimental study. In *Proceedings of the 13th Nordic Conference on Human-Computer Interaction*, NordiCHI '24, New York, NY, USA, 2024. Association for Computing Machinery. Available at: https://dl.acm.org/doi/10.1145/3679318.3685362.

[3] Samuel Agbesi, Asmita Dalela, Jurlind Budurushi, and Oksana Kulyk. "What Will Make Me Trust or Not Trust Will Depend Upon How Secure the Technology Is": Factors Influencing Trust Perceptions of the Use of Election Technologies. *E-Vote-ID 2022*, page 1, 2022. Available at: https://pure.itu.dk/ws/portalfiles/portal/91508344/Trust_and_Risk_Perceptions_Final_3.pdf.

[4] Diego F. Aranha, Michele Battagliola, and Lawrence Roy. Faster coercion-resistant e-voting by encrypted sorting. Cryptology ePrint Archive, Paper 2023/837, 2023. https://eprint.iacr.org/2023/837.

[5] Thomas Bjørner. *Why 'Qualitative Methods for Consumer Research'?*, pages 11–15. Hans Reitzels Forlag, Denmark, 2015.

[6] Jurlind Budurushi, Karen Renaud, Melanie Volkamer, and Marcel Woide. An investigation into the usability of electronic voting systems for complex elections. *Annals of Telecommunications*, 71:309–322, 2016. Available at: https://doi.org/10.1007/s12243-016-0510-2.

[7] Mohamed Chaieb and Sabrine Yousfi. Loki vote: A blockchain-based coercion resistant e-voting protocol. In Marinos Themistocleous, Marios Papadaki, and Mostafa M. Kamal, editors, *Information Systems. EMCIS 2020*, volume 402, pages 151–168, Cham, 2020. Springer. Available at: https://doi.org/10.1007/978-3-030-63396-7_11.

[8] David Chaum, Richard T. Carback, Jeremy Clark, Chao Liu, Mahdi Nejadgholi, Bart Preneel, Alan T. Sherman, Mario Yaksetig, Zeyuan Yin, Filip Zagórski, and Bingsheng Zhang. VoteXX: A solution to improper influence in voter-verifiable elections. Cryptology ePrint Archive, Paper 2022/1212, 2022. Available at: https://votexx.org/votexx-whitepaper.pdf.

[9] Nusrat Jahan Khan Chowdhury, Shinsuke Tamura, and Kazi Masudul Ryan Alam. Preliminary conceptions of a remote incoercible e-voting scheme. In Rajkumar Doriya, Bhavesh Soni, Abhishek Shukla, and Xinzheng Gao, editors, *Machine Learning, Image Processing, Network Security and Data Sciences*, volume 946, Singapore, 2023. Springer. Available at: https://doi.org/10.1007/978-981-19-5868-7_58.

[10] Laura Christiano, Riccardo Longo, and Chiara Spadafora. Click and cast: Assessing the usability of vote app. In *Electronic Voting: 9th International Joint Conference, E-Vote-ID 2024, Tarragona, Spain, October 2–4, 2024, Proceedings*, 2024.

[11] Jeremy Clark and Urs Hengartner. Selections: Internet voting with over-the-shoulder coercion-resistance. In George Danezis, editor, *Financial Cryptography and Data Security*, pages 47–61, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[12] Michael R. Clarkson, Stephen Chong, and Andrew C. Myers. Civitas: Toward a secure voting system. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 354–368, 2008. Available at: https://ieeexplore.ieee.org/document/4531164.

[13] Véronique Cortier, David Galindo, Ralf Küsters, Johannes Müller, and Tomasz Truderung. Sok: Verifiability notions for e-voting protocols. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 779–798. IEEE, 2016. Available at: https://ieeexplore.ieee.org/document/7546535.

[14] Véronique Cortier, Pierrick Gaudry, Anselme Goetschmann, and Sophie Lemonnier. Belenios with cast-as-intended: Towards a usable interface. In *Electronic Voting: 9th International Joint Conference, E-Vote-ID 2024, Tarragona, Spain, October 2–4, 2024, Proceedings*, page 1–19, Berlin, Heidelberg, 2024. Springer-Verlag. Available at: https://doi.org/10.1007/978-3-031-72244-8_1.

[15] Véronique Cortier, Pierrick Gaudry, and Quentin Yang. Is the jcj voting system really coercion-resistant? Cryptology ePrint Archive, Paper 2022/430, 2022. https://eprint.iacr.org/2022/430.

[16] Verena Distler, Marie-Laure Zollinger, Carine Lallemand, Peter B. Roenne, Peter Y. A. Ryan, and Vincent Koenig. Security - visible, yet unseen? how displaying security mechanisms impacts user experience and perceived security. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–13, New York, NY, USA, 2019. Association for Computing Machinery. Available at: https://dl.acm.org/doi/pdf/10.1145/3290605.3300835.

[17] Piret Ehin, Mihkel Solvak, Jan Willemson, and Priit Vinkel. Internet voting in estonia 2005–2019: Evidence from eleven elections. *Government Information Quarterly*, 39(4):101718, 2022. Available at: https://www.sciencedirect.com/science/article/pii/S0740624X2200051X.

[18] Ehsan Estaji, Thomas Haines, Kristian Gjøsteen, Peter B. Rønne, Peter Y. A. Ryan, and Najmeh Soroush. Revisiting practical and usable coercion-resistant remote e-voting. page 50–66, Berlin, Heidelberg, 2020. Springer-Verlag. Available at: https://doi.org/10.1007/978-3-030-60347-2_4.

[19] Christian Feier, Stephan Neumann, and Melanie Volkamer. Coercion-resistant internet voting in practice. In *Informatik 2014*, pages 1401–1414. Gesellschaft für Informatik e.V., Bonn, 2014. Available at: https://subs.emis.de/LNI/Proceedings/Proceedings232/1401.pdf.

[20] Kristin Skeide Fuglerud and Till Halbach Røssvoll. An evaluation of web-based voting usability and accessibility. *Universal Access in the Information Society*, 11:359–373, 2012. Available at: https://doi.org/10.1007/s10209-011-0253-9.

[21] Rosario Giustolisi, Maryam Sheikhi Garjan, and Carsten Schuermann. Thwarting last-minute voter coercion. Cryptology ePrint Archive, Paper 2023/1876, 2023. Available at: https://eprint.iacr.org/2023/1876.pdf.

[22] Greg Guest, Arwen Bunce, and Laura Johnson. How many interviews are enough? an experiment with data saturation and variability. *Field Methods*, 18:59–82, 02 2006.

[23] Thomas Haines, Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. How not to prove your election outcome. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 644–660. IEEE, 2020. Available at: https://ieeexplore.ieee.org/document/9152765.

[24] Thomas Haines and Johannes Mueller. How not to VoteAgain: Pitfalls of scalable coercion-resistant e-voting. Cryptology ePrint Archive, Paper 2020/1406, 2020. https://eprint.iacr.org/2020/1406.

[25] Thomas Haines, Johannes Müller, and Iñigo Querejeta-Azurmendi. Scalable coercion-resistant e-voting under weaker trust assumptions. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, SAC '23, page 1576–1584, New York, NY, USA, 2023. Association for Computing Machinery. Available at: https://doi.org/10.1145/3555776.3578730.

[26] J Alex Halderman and Vanessa Teague. The new south wales ivote system: Security failures and verification flaws in a live online election. In *E-Voting and Identity: 5th International Conference, VoteID 2015, Bern, Switzerland, September 2-4, 2015, Proceedings 5*, pages 35–53. Springer, 2015. Available at: https://doi.org/10.1007/978-3-319-22270-7_3.

[27] Ari Juels, Dario Catalano, and Markus Jakobsson. *Coercion-Resistant Electronic Elections*, pages 37–63. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010. Available at: https://doi.org/10.1007/978-3-642-12980-3_2.

[28] Fatih Karayumak, Maina M. Olembo, Michaela Kauer, and Melanie Volkamer. Usability analysis of helios — an open source verifiable remote electronic voting system. In *2011 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 11)*, San Francisco, CA, August 2011. USENIX Association. Available at: https://www.usenix.org/legacy/event/evtwote11/tech/final_files/Karayumak.pdf.

[29] Oksana Kulyk and Stephan Neumann. Human factors in coercion resistant internet voting – a review of existing solutions and open challenges. 2020. Available at: https://pure.itu.dk/ws/portalfiles/portal/85567889/Human_factors_in_coercion_resistant_voting_13_2.pdf.

[30] Oksana Kulyk, Stephan Neumann, Jurlind Budurushi, and Melanie Volkamer. Nothing comes for free: How much usability can you sacrifice for security? *IEEE Security & Privacy*, 15(3):24–29, 2017. Available at: https://ieeexplore.ieee.org/document/7945211.

[31] Riccardo Longo and Chiara Spadafora. Amun: Securing e-voting against over-the-shoulder coercion. Cryptology ePrint Archive, Paper 2021/851, 2021. Available at: https://eprint.iacr.org/2021/851.pdf.

[32] Wouter Lueks, Iñigo Querejeta-Azurmendi, and Carmela Troncoso. VoteAgain: A scalable coercion-resistant voting system. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1553–1570. USENIX Association, August 2020. Available at: https://www.usenix.org/conference/usenixsecurity20/presentation/lueks.

[33] Damien MacNamara, Ted Scully, J. Paul Gibson, Francis Carmody, Ken Oakley, and Elizabeth Quane. Dualvote: Addressing usability and verifiability issues in electronic voting systems. 05 2011. Available at: https://jpaulgibson.synology.me/

~jpaulgibson/TSP/Research/Publications/E-Copies/MacNamaraSGCOQ11.pdf.

[34] Karola Marky, Nina Gerber, Henry John Krumb, Mohamed Khamis, and Max Mühlhäuser. Investigating voter perceptions of printed physical audit trails for online voting. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 3458–3477, 2024.

[35] Karola Marky, Paul Gerber, Sebastian Günther, Mohamed Khamis, Maximilian Fries, and Max Mühlhäuser. Investigating State-of-the-Art practices for fostering subjective trust in online voting through interviews. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 4059–4076, Boston, MA, August 2022. USENIX Association. Available at: https://www.usenix.org/conference/usenixsecurity22/presentation/marky.

[36] Karola Marky, Oksana Kulyk, Karen Renaud, and Melanie Volkamer. What did i really vote for? on the usability of verifiable e-voting schemes. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–13, New York, NY, USA, 2018. Association for Computing Machinery. Available at: https://dl.acm.org/doi/10.1145/3173574.3173750.

[37] Karola Marky, Verena Zimmermann, Markus Funk, Jörg Daubert, Kira Bleck, and Max Mühlhäuser. Improving the usability and ux of the swiss internet voting interface. CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery. Available at: https://dl.acm.org/doi/10.1145/3313831.3376769.

[38] Karola Marky, Marie-Laure Zollinger, Peter Roenne, Peter Y. A. Ryan, Tim Grube, and Kai Kunze. Investigating usability and user experience of individually verifiable internet voting schemes. 28(5), September 2021. Available at: https://doi.org/10.1145/3459604.

[39] Louis-Henri Merino, Alaleh Azhir, Haoqian Zhang, Simone Colombo, Bernhard Tellenbach, Vero Estrada-Galiñanes, and Bryan Ford. E-vote your conscience: Perceptions of coercion and vote buying, and the usability of fake credentials in online voting. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 3478–3496, 2024. Available at: https://link.springer.com/chapter/10.1007/978-3-642-12980-3_2.

[40] Stephan Neumann, Christian Feier, Melanie Volkamer, and Reto Koenig. Towards a practical JCJ / civitas implementation. Cryptology ePrint Archive, Paper 2013/464, 2013. Available at: https://eprint.iacr.org/2013/464.pdf.

[41] Stephan Neumann and Melanie Volkamer. Civitas and the real world: Problems and solutions from a practical point of view. In *2012 Seventh International Conference on Availability, Reliability and Security*, pages 180–185, 2012. Available at: https://publikationen.bibliothek.kit.edu/1000081877.

[42] Council of Europe. Recommendation cm/rec(2017)5[1] of the committee of ministers to member states on standards for e-voting. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f#globalcontainer, last visited 24.05.2022.

[43] Haim Omer and Nahi Alon. The continuity principle: A unified approach to disaster and trauma. *American Journal of Community Psychology*, 22(2):273–287, 1994.

[44] Cliodhna O'Connor and Helene Joffe. Intercoder reliability in qualitative research: Debates and practical guidelines. *International Journal of Qualitative Methods*, 19:1609406919899220, 2020.

[45] Iñigo Querejeta-Azurmendi, David Arroyo, José Luis Hernández-Ardieta, and Luis Hernández Encinas. Netvote: A strict-coercion resistance re-voting based internet voting scheme with linear filtering. *Mathematics*, 8(9):1618, 2020. Available at: https://www.mdpi.com/2227-7390/8/9/1618.

[46] Iñigo Querejeta-Azurmendi, Luis Hernández Encinas, David Arroyo Guardeño, and José Luis Hernández-Ardieta. An internet voting proposal towards improving usability and coercion resistance. In Francisco Martínez Álvarez, Álvaro Troncoso Lora, Javier Sáez Muñoz, Héctor Quintián, and Emilio Corchado, editors, *International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019)*, volume 951, pages 155–164, Cham, 2020. Springer. Available at: https://link.springer.com/chapter/10.1007/978-3-030-20005-3_16.

[47] Peter YA Ryan and Vanessa Teague. Pretty good democracy. In *Security Protocols XVII: 17th International Workshop, Cambridge, UK, April 1-3, 2009. Revised Selected Papers 17*, pages 111–130. Springer, 2013. Available at: https://doi.org/10.1007/978-3-642-36213-2_15.

[48] Neyire Deniz Sarier. Efficient and usable coercion-resistant e-voting on the blockchain. Cryptology ePrint Archive, Paper 2023/1509, 2023. https://eprint.iacr.org/2023/1509.

[49] Cristina Satizábal, Rafael Páez, and Jordi Forné. Secure internet voting protocol (sivp): A secure option for electoral processes. *Journal of King Saud University - Computer and Information Sciences*, 34(6, Part B):3647–3660, 2022. Available at: https://www.sciencedirect.com/science/article/pii/S1319157820306248.

[50] Abdurashid Solijonov. *Voter Turnout Trends around the World*. International Institute for Democracy and Electoral Assistance (International IDEA), Stockholm, Sweden, 2016. Available at: https://www.idea.int/sites/default/files/publications/voter-turnout-trends-around-the-world.pdf.

[51] Chiara Spadafora, Riccardo Longo, and Massimiliano Sala. Coercion-resistant blockchain-based e-voting protocol. Cryptology ePrint Archive, Paper 2020/674, 2020. Available at: https://eprint.iacr.org/2020/674.pdf.

[52] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J Alex Halderman. Security analysis of the estonian internet voting system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 703–715, 2014. Available at: https://dl.acm.org/doi/10.1145/2660267.2660315.

[53] Kristjan Vassil, Mihkel Solvak, Priit Vinkel, Alexander H. Trechsel, and R. Michael Alvarez. The diffusion of internet voting. usage patterns of internet voting in estonia between 2005 and 2015. *Government Information Quarterly*, 33(3):453–459, 2016. Available at: https://www.sciencedirect.com/science/article/pii/S0740624X1630096X.

[54] Melanie Volkamer, Oksana Kulyk, Jonas Ludwig, and Niklas Fuhrberg. Increasing security without decreasing usability: A comparison of various verifiable voting systems. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 233–252, Boston, MA, August 2022. USENIX Association. Available at: https://www.usenix.org/conference/soups2022/presentation/volkamer.

[55] Melanie Volkamer, Oliver Spycher, and Eric Dubuis. Measures to establish trust in internet voting. In *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance*, pages 1–10, 2011. Available at: https://dl.acm.org/doi/pdf/10.1145/2072069.2072071.

[56] Roland Wen and Richard Buckland. Masked ballot voting for receipt-free online elections. In Peter Y. A. Ryan and Berry Schoenmakers, editors, *E-Voting and Identity*, pages 18–36, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg. Available at: https://doi.org/10.1007/978-3-642-04135-8_2.

[57] Marco Winckler et al. Assessing the usability of open verifiable e-voting systems: a trial with the system prêt à voter. In *Proceedings of ICE-GOV*, pages 281–296, 2009.

[58] Zeyuan Yin, Bingsheng Zhang, Andrii Nastenko, Roman Oliynykov, and Kui Ren. A scalable coercion-resistant blockchain decision-making scheme. Cryptology ePrint Archive, Paper 2023/1578, 2023. https://eprint.iacr.org/2023/1578.

[59] Ehab Zaghloul, Tongtong Li, and Jian Ren. Anonymous and coercion-resistant distributed electronic voting. In *2020 International Conference on Computing, Networking and Communications (ICNC)*, pages 389–393, 2020. Available at: https://ieeexplore.ieee.org/document/9049653.

[60] Ehab Zaghloul, Tongtong Li, and Jian Ren. d-bame: Distributed blockchain-based anonymous mobile electronic voting. *IEEE Internet of Things Journal*, 8(22):16585–16597, 2021. Available at: https://ieeexplore.ieee.org/document/9409949.

[61] Zhang Zhaoju, Luo Hanbo, and Di Hong. Verifiable receipt-free electronic voting system based on mask ballot. In *2021 IEEE 9th International Conference on Smart City and Informatization (iSCI)*, pages 47–52, 2021. Available at: https://ieeexplore.ieee.org/document/9724582.

8 Appendix

Due to the extensive length, all appendices (recruitment materials, interview guide, consent form, codebook, and demographics) are provided in a single external link, accessible here: https://osf.io/3cd2r/?view_only=cfa43eae0e00457fb144c56e7ae6ca5c. The recruitment materials have been removed to ensure anonymisation.