# Human Factors in Coercion Resistant Internet Voting – A Review of Existing Solutions and Open Challenges

Oksana Kulyk[1] and Stephan Neumann[2]

[1] IT University of Copenhagen, Denmark, okku@itu.dk
[2] stephanneumann@tutamail.com

**Abstract.** While Internet voting has a potential of improving the democratic processes, it introduces new challenges to the security of the election, such as the possibility of voter coercion due to voting in uncontrolled environments. Cryptographic research has resulted in a number of proposals for protecting against such coercion with the help of counter-strategies that can be used by the voter to convince the coercer that they obeyed their instructions while secretly voting for another voting option. So far, these proposals have been theoretical, and their usability in terms of ability of the voter to apply the counter-strategies in practice has not been thoroughly investigated. We conducted a literature review to identify the available counter-strategies and assumptions on voters' capabilities. We evaluated the identified assumptions and conclude a number of usability issues. We provide recommendations on further research directions and practical considerations in designing coercion resistant voting systems are provided.

## 1 Introduction

With the ongoing digitalization of society, Internet voting has often been discussed as a way to facilitate democratic processes. These discussions are furthermore more prominent in 2020 given the ongoing pandemic, as many argue, making remote voting a necessary option to protect the population. Several countries, e.g. Estonia and Switzerland, introduced Internet voting as an additional voting channel in order to improve convenience for the voters and support voters who would otherwise be unable to get to a polling station. However, introducing technology in electoral processes also introduced new risks, in particular, risks connected with security and privacy. One of these risks is the possibility of voter coercion, stemming from the fact that the voting occurs in an uncontrolled environment where voter privacy and, correspondingly, the secrecy of the ballot is no longer guaranteed. An adversary who is physically present next to the voter while they cast their vote – for example, a household member or a supervisor at work – would be able to ensure that the voter casts the vote they are instructed to cast. Even a remote coercer could instruct the voter to reveal which voting option they voted for, for example, by requesting the voter to prepare and send a recording of the voting procedure.

In order to prevent such attacks, a number of works in the e-voting community focused on developing schemes for the voting systems with the so-called coercion resistance property, see e.g. [1, 5, 28]. A scheme that is coercion resistant aims to protect voters' privacy even if the adversary can actively communicate with the voter and coerce them to reveal secret information or to behave in a certain way. A related concept is receipt-freeness, which specifically focuses on preventing the voter from creating a receipt that would prove to the adversary how they voted. One of the ways the schemes satisfy coercion resistance and/or receipt-freeness is via the so-called counter-strategy. The idea is, that the voter pretends to follow the coercer's instructions, while secretly following a different procedure that allows them to vote for their preferred voting option. The counter-strategy succeeds if the coercer is not able to tell whether it has been applied, or whether the voter has voted as instructed.

While the underlying cryptographic mechanisms of the proposed schemes can guarantee the success of a counter-strategy under the defined security model, it is still crucial to ensure that the voter is capable of performing them correctly. Usability therefore becomes a fundamental issue. While a number of works have investigated usability and other human factors in e-voting (see e.g. [37, 46]), only a few have considered the actions required by the voter to ensure coercion resistance from the usability point of view [42, 43]. These studies have pointed that the counter-strategies proposed by investigated systems rely on complicated concepts not understandable by the voter and on complex actions required from the voter. As these studies focused on the evaluation of a specific voting scheme and its implementation, no systematic investigation on the available counter-strategies from a variety of systems has been done yet. The general practical issues of coercion resistant voting systems are studied by Krips and Willemson [33], however, their work does not focus on human factors of such systems.

This paper describes the results of a conducted literature review to identify the counter-strategies available in voting literature on the topic of coercion resistance. We study the assumptions regarding the voter capabilities in applying these counter-strategies from the human factors point of view. We identify a number of challenges in designing coercion resistant systems and provide recommendations on addressing these challenges and future work directions.

## 2 Methodology

In order to identify the existing counter-strategies a search using keywords ”coercion resistance voting” and ”receipt-freeness voting” in SpringerLink, IEEE, ACM and USENIX proceedings databases has been conducted. The search was limited to papers in computer science written in English language that are in open access from the authors' institution. Additionally, a search using the same keywords was performed in Google Scholar. From the search results, the papers that propose an Internet voting scheme satisfying some variant of receipt-freeness and/or coercion resistance were identified.

Note, we do not include proposals for polling-place voting, as these assume a controlled environment. We furthermore do not consider the proposals that rely on security mechanisms other than counter-strategies (e.g. rerandomisation of a vote by a voting system component [13] or relying on a tamper-resistant device that does not reveal the encryption randomness to the voter [8]), since these do not protect against an attacker that is either physically present or demands a recording of the voting procedure from the voter. Furthermore, we exclude the papers that focus on improving one specific part of the procedure towards providing better protection against coercion (e.g. such as the individual verification in the original proposal in Selene [49], or preventing disclosure from published tally results in ShuffleSum [10]) without considering other steps of the election procedure such as actual vote casting.

## 3 Results

A total of 51 papers were identified, containing the proposals that can be classified into the following categories: fake credentials, deniable vote updating, vote masking and code voting. Table 1 provides an overview of the number of proposals in each category. We explain the counter-strategies in each category in more detail, considering the following coercion scenario. The adversary wants to coerce the voter to cast a vote for Eve, while the voter attempts to cast a vote for Alice instead[3]. In our description, we focus on human factors challenges and assumptions of the counter-strategies, referring to the work by Krips and Willemson [33] for an overview of more technical assumptions or coercion resistant systems.

| **Counter-strategy** | **Papers** | **Total** |
|---|---|---|
| Fake credentials | [2–6, 12, 15, 16, 18, 19, 22, 24, 27–29, 32, 41, 43, 47, 48, 52–55, 57, 58, 61, 65, 66] | 29 |
| Deniable vote updating | [11, 14, 20, 25, 34, 36, 38, 39, 44, 45, 56] | 11 |
| Masking | [7, 17, 26, 30, 31, 50, 59, 62–64] | 11 |

**Table 1.** Classification of scientific papers into counter strategies against voter coercion.

### 3.1 Fake credentials

By far the most popular counter-strategy relies on the existence of so-called fake credentials. The idea behind the counter-strategy is as follows. Given a space of available credentials $\mathcal{C}$, the voter is provided with a unique and secret credential

[3] Note, while other possible combinations of goals for both adversary and the voter exist (for example, the voter might want to avoid voting for Eve without necessarily casting a ballot for another candidate, or adversary might want to force the voter to abstain instead of voting for a specific candidate), these are only briefly discussed and are not in the focus of this paper.

$\hat{c} \in \mathcal{C}$ during voter registration, so that the credential is distributed before the election via an untappable channel. When voting, the voter uses the credential $\hat{c}$ to authenticate themselves to the voting system. If the voter is coerced, instead of authenticating themselves with their real credential, they generate and use a so-called fake credential $c' \neq \hat{c}$. The fake credential is indistinguishable from the real one by the adversary, and is accepted by the voting system without outputting an authentication error. The votes submitted with the fake credential are, however, are excluded from tallying. The voter then can cast a valid vote for their preferred candidate when they are not being observed by the adversary. In case the voter only wants to prevent voting for an adversarial candidate, no further actions are required.

While some of the described schemes do not specify how the credentials are stored, providing only a description of the protocol without going into practical implementation aspects (e.g. [28]), others rely on storing various values such as cryptographic secret keys on a tamper-resistant trusted device (see e.g. [43, 47]. The purpose of this device is to ensure, that neither an adversary nor the voter themselves can get access to the information stored on it.

**Human factors assumptions** The success of the fake credential counter-strategy depends on how secure these credentials are managed. This results in the assumptions on voters' behaviour as described below.

*Inputting real credentials.* The first assumption is crucial, first and foremost, for the case when no coercion occurs and the voter simply wants to cast a vote for their preferred candidate. In that case, they have to enter their real credential into the system. They, however, would not be provided with any feedback from the system, whether the credential is actually correct – after all, a potential coercer who observes the voting would otherwise be able to tell whether the voter obeys the adversary's instructions or applies a counter-strategy. This assumption is especially crucial in systems where any credential $c \in \mathcal{C}$ is admissible by the system and treated as fake as long as $c' \neq \hat{c}$ – in such a case, any typo or other mistake in entering the credential will result in casting an invalid vote, without the voter knowing it.

One approach to facilitate this assumption relies on the so-called panic passwords [15]. The idea is to use a separate type of credential that would allow the voter to signal being coerced. Thus, each voter is assigned a set $I \subset \mathcal{C}$ of admissible credentials, of which $\hat{c} \in I$ is the only real credential that allows casting a valid ballot. Whenever the voter authenticates themselves using any value $c \in \mathcal{C}/I$, the system outputs an authentication error. If the voter uses $c' \in I$, $c' \neq \hat{c}$, the system treats $c'$ as a fake credential and the voter as coerced, and accepts $c'$ without outputting any error. Using such an approach it is crucial to define $I$ in such a way that makes it unlikely that the voter mistakenly enters another credential $c' \in I$ instead of $c$. The authors of [15] propose to define $I$ as any passphrase that consists of a given number of dictionary words. Such a system is likely to protect against typos (especially if one excludes dictionary words that differ from each other by a single letter, and hence, prone to being mixed up due to typos). However, it will not protect voters who do not remember the passphrase exactly, for example, not being sure about the order of the words in a passphrase. One can furthermore argue that panic passwords introduce further usability issues: as such, it is crucial to ensure that the voters understand the concept of panic passwords, namely, that out of many admissible passwords available to them, only one can be used for casting a valid ballot. Finally, if the voters are expected to generate their passwords themselves, it should be taken into account that humans often find it difficult to come up with passwords that are secure enough.

*Generating fake credentials.* A related assumption is required to ensure that the coerced voters are capable of applying a counter-strategy without alerting the adversary. This assumption might be easier to fulfill if the system accepts any credential $c' \in \mathcal{C}$ as a fake credential without outputting a warning. Still, the voters need to be explained how and when they should do it. As with panic passwords, generating a convincing fake credential would also get more complicated if the voters are required to understand the rules of how panic passwords are constructed and generate one accordingly.

### 3.2 Deniable vote updating

Another method of resisting coercion is the so-called deniable vote updating. The idea is simple: while the voter might be coerced to cast a particular vote in presence of an adversary, they can cast another vote, overwriting their previous one, when the adversary is gone. This method, in particular, is relied upon in real-world Internet voting in Estonia and was deployed in the Norwegian Internet voting system between 2011 and 2013. The coercion resistance property, in particular, is achieved due to deniability of vote updating – the adversary should be unable to tell whether the voter has cast another vote, even if the voter would try to prove that they did not do it. This deniability is achieved either via restricting access to the election information, or via cryptographic solutions that enable deniability while also publishing the cast ballots for verifiability. As opposed to fake credentials-based systems, where the voting credentials are generated and distributed as a part of the voting system and specifically designed to be coercion resistant, systems based on deniable vote updating assume that an existing infrastructure is used for authenticating the voters. Such an infrastructure can be implemented via tamper-resistant trusted hardware tokens, such as smart cards in Estonia. Forwarding those types of authentication material could have severe impact to voters beyond the voting process, which lowers the risk of forwarding voting materials.

A variant of deniable vote updating is a so-called flexible vote updating. As opposed to simple vote updating that follows the last-vote-counts policy, the final ballot that is included in the tally is calculated as a function of all the ballots cast by the voter in the election, expressed by a function $F(v_1, ..., v_n)$. One example of such function is the proposal in [11,36], which sets $F(v_1, ..., v_k) = \sum_{i=1}^{k} v_i$. In this way, the system ensures protection against last-minute attacks that might occur if the adversary demands that the voter casts their vote during the very last minute of the voting phase of the election, either observing the voter while they do so (including remote observation or recordings of the voting procedure provided by the voter), or checking the public election information for the ballots posted by the voter. In that case, if the voter is coerced to cast a vote for $v_{Eve}$ using the system with flexible vote updating, they cast a ballot for $v' = v_{Alice} - v_{Eve}$ beforehand, so that their final ballot is computed as $v' + v_{Eve} = v_{Alice}$.

**Human factors assumptions** An advantage of the deniable vote updating strategy is its initial simplicity: if the voter is not coerced, the vote casting process is no different from simpler voting systems that do not ensure coercion resistance. Even in case of coercion, the concept of voting again in order to overwrite the vote cast under coercion would most probably fit into the mental models of the voters. The simple vote updating strategy therefore only relies on one assumption:

*Make sure to vote after (or before) coercion.* As opposed to fake credentials approach, the deniable vote updating strategy requires the voter to take additional action in order to make sure that the adversarial vote will not be counted. Thus, in addition to ensuring that the voter has such a possibility by being free from adversarial observation, the voter should also keep in mind that they need to go through the voting process again at some point. More complexity, however, is introduced if the flexible vote updating is used. Namely, the following assumptions becomes of crucial importance:

*Remember all the votes cast in the election.* At the moment of casting their vote, the voter should keep track of all the votes cast in the election, including votes that they might be coerced to cast in the future.

*Calculate values to cast.* The voter should be able to calculate the value they should cast in order to get their preferred vote to be counted; that is, given $v_1, ..., v_{k-1}$ as the votes cast in the election, the voter should be able to calculate $v_k$ so that $F(v_1, ..., v_k) = v_{Alice}$.

*Input $v_k$.* Once the value $v_k$ is calculated, the voter has to input it without making any errors.

Similar to the fake credentials strategy, the system would not be able to output all the previously cast votes on voter's request or provide any feedback on the resulting value $F(v_1, ..., v_k)$ upon casting $v_k$ without violating coercion resistance. Note, that the consequences in making a mistake in inputting $v_k$ are even more severe than in the fake credential counter-strategy when voting in absence of coercion. While failing to input a correct credential can only in casting an invalid ballot that will not be counted, choosing a wrong value $v_k$ can in worst case result in a final ballot $v = F(v_1, ..., v_k)$ that will be counted as a valid vote for one of the candidates in the election other than Alice.

Note also, that much of this complexity can be hidden behind the user interface of the voting client; as such, the system with flexible vote updating can be modified into the system with simple vote updating, if the voting client stores all the votes $v_1, ..., v_{k-1}$ cast so far, and casts a value $v_k$ so that $F(v_1, ..., v_k) = v_{Alice}$ if the voter inputs "Alice" as their choice in the user interface. Such a modification, however, will make the system vulnerable to last-minute coercion. A possible solution would be to let the voter choose between simple and flexible vote updating in an election, by offering to download two different voting clients; this, however, would require further computer literacy from the voter, as well as the ability to understand the difference between the offered choices.

### 3.3 Masking

As opposed to fake credentials and deniable vote updating counter-strategies that are aimed at nullifying the vote cast in presence of an adversary (with a possibility to change it to a vote for the voter's preferred candidate), masking enables the voter to cast their preferred vote for Alice while letting the adversary think that the same cast vote is a vote for Eve. The idea is, that before the election, the system commits to a secret masking value $b \in \mathcal{B}$ and shares it with the voter. When casting the vote, the voter utilises a function $M : \mathcal{B} \times \mathcal{V} \to \mathcal{V}$ to submit a masked ballot $v_M = M(b, v_{Alice})$, from which the value $v_{Alice} = M^{-1}(v_m, b)$ will be extracted by the voting system. A voter who is coerced would, correspondingly, cast the same masked ballot $v_M$ and provide the coercer with a fake masking value $b'$ selected such as $v_M = M(b', v_{Eve})$. Different variants of masking strategy have been proposed, such as using $\mathbb{Z}_n$ as a set of possible votes $v_m$ and using a one time pad $b \in \mathbb{Z}_n$ with $M(v, b) := v + b$, using permutation $\pi$ of candidate list $v_1, ...v_L$, with $b = (\pi(1), ..., \pi(L))$ and $M(v_i, b) := \pi(i)$ or using a code list $b = x_1, ..., x_L$ with a unique code assigned to each one of the candidates $v_1, ..., v_L$ and $M(v_i, b) := x_i$ (the so-called code voting).

**Human factor assumptions** The main assumption crucial for the masking counter-strategy is the voter being able to calculate the value $v_m$ that results in a vote for an intended candidate (i.e. so that $M^{-1}(v_m, b) = v_{Alice}$). This results in the following assumptions:

*Recalling $b$.* While the voter does not have to manually input the masking value during vote casting, they are expected to recall it correctly in order to perform the calculation of $M(v_{Alice}, b)$.

*Calculating $M(v_{Alice}, b)$.* Even if the voter remembers $b$, they are still expected to calculate the masked ballot that corresponds to their intended vote $b$.

*Input $v_m$.* Finally, once the value $v_m = M(v_{Alice}, b)$ is calculated, the voter has to input it without making any errors.

Similar to the fake credential counter-strategy, the voting system would not output any feedback regarding $M^{-1}(v_m, b)$ for a cast $v_m$. Similar to the deniable vote updating strategy, failing to cast a correct masked ballot, due to mistakes either in recalling $b$ or in calculating or inputting $v_m$ can in worst case result in a vote being cast for another candidate that will be counted in the tally.

As one way to mitigate this assumption, the scheme in [7] proposes to use a mobile app that receives and outputs the value $b$ from the voting system as the voter starts the voting process. As discussed above, such an approach requires a trusted mobile device and does not protect against a physically present coercer. Another solution is the code voting approach that uses paper code sheets containing printed codes for each candidate, e.g. with $x_{Alice}$ and $x_{Eve}$ corresponding to votes for Alice and Eve respectively. The idea is that the voter reads the code of their chosen candidate during vote casting, without having to recall it from memory. Similar to the app approach, the voter would be vulnerable against physically present adversary. However, assuming that the voter can print fake code sheets by themselves and expects the coercer to force them to vote for Eve, they could switch the codes on the fake sheets, setting $x'_{Alice} = x_{Eve}$ and $x'_{Eve} = x_{Alice}$. Yet another way to ensure that the cast masked ballot is the same vote that the voter intended to cast is the use of so-called return codes. The idea is to assign a code $r_1, ..., r_L$ to each candidate, and provide the return code sheets with codes printed on paper to the voter. After receiving a ballot with a vote for a candidate $v_i$, the voting system outputs a code $r_i$ to the voter, which they should compare to the code on their return code sheet. While the use of return codes is commonly used to protect against malicious voting device, it can also be used as a help for the voter to ensure that they input the correct masked ballot. In order to avoid coercion, however, the voter would have to fake the return code sheet, assuming a certain level of computer skills.

## 4 Discussion

Following the description of counter-strategies and their related assumptions, we discuss the human factors related with applying the counter-strategies and make recommendations on designing coercion resistant systems.

### 4.1 Identified human factors and challenges

As the discussion of different counter-strategies revealed, there is a number of issues related to human factors that need to be addressed for ensuring proper use of coercion resistant voting systems, with some of these issues known from usable security research in other domains (see e.g. [51, 60]). These issues can be clustered as follows.

**Unrealistic assumptions** The complexity of the proposed counter-strategies is a significant issue that could potentially prevent the voters from applying these counter-strategies correctly. As such, they tend to require capabilities that are difficult or impossible to attain, such as being able to remember long, random-looking credentials or to input them on their first try without any errors.

While these limitations have been acknowledged in previous research, often by the authors of the proposed schemes, the suggested methods to aid the voters in their task either had to rely on additional security assumptions such as trusted hardware, or introduced further complexity for the voters.

**Self-efficacy issues** Even if the voters are actually capable to apply a counter-strategy, a seeming complexity of the process might still discourage them from it. This leads to lack of self-efficacy: even if the system actually provides ways for the voters to protect themselves against coercion, the voters might still feel helpless and unable to do so. Such lack of self-efficacy has been identified as an issue in other aspects of electronic voting that require actions from the voter that are unfamiliar to them from paper-based voting, such as verifying the integrity of one's cast vote [37]). This issue, however, might be even more crucial for coercion resistance, since the voter is under additional stress from coercion and the consequences of failure are potentially higher. If the voter tries to apply a counter-strategy and fails, they might face repercussions from the adversary. Even in the vote buying scenario, where the voter does not suffer any negative repercussions, but instead does not get his pay from the adversary, the voter might consider it a more rational decision to obey the adversary, if they do not see their vote as valuable enough.

**Limited interactive feedback** As opposed to voting in general, the system cannot provide feedback on the status of vote casting (e.g. whether the voter is applying a counter-strategy or not). All the explanations and voter instructions have to be provided in a non-interactive form, that is, they should not depend on the actions of the voter and whether they apply the counter-strategy.

**Trust and acceptance** Even in absence of coercion, the voters have to change their vote casting procedure, often to incorporate non-intuitive elements, such as entering a masked value instead of their vote, having to remember all the previously cast votes when updating, or remembering and distinguishing between different kinds of credentials. If explicit instructions to avoid coercion are provided, the voter might be altered and distrust the system. On the other hand, mentions of increased security of the system might make the voters accept the system more, once they are provided an explanation of the risks that are present in Internet voting and that the system is designed to protect against (see [35, 40] for related studies on the concept of cast-as-intended verifiability).

### 4.2 Recommendations

Considering the identified human factors and challenges, we propose a set of recommendations for future implementations of coercion resistant voting systems.

**Involve the user** Involving the user in the development of security-critical systems has been widely recommended in usable security research, including research on usability of electronic voting systems [46]. This is especially relevant when the assumptions on voters' capabilities are inherent in the cryptographic protocol, and any improvements after the system is implemented will most likely come with a change to the security model assumed in the initial scheme. Considering usability from the beginning of the development, including getting iterative feedback for the system prototypes from the users, would therefore help to identify potential issues early. This feedback can furthermore be used to design new counter-strategies that are more aligned with mental models of potential voters.

**Provide aids** The counter-strategies presented above rely on the voter *remembering certain secrets*, be it their real credential, votes cast previously in the election, or masking value. While the voter could write them down and use as a reference during vote casting, this could be an issue with over-the-shoulder coercion, where the adversary can observe the whole voter environment. For such a scenario, the secrets should be explicitly designed easy to remember (but at the same time, not easy to guess to the adversary). The voter should furthermore be provided with guidelines on how to remember these secrets, e.g. based on memorisation strategies for PINs [23].

In addition to secrets individual to each voter, there is also a need to remember the *steps of counter-strategy*, e.g. the rules of generating panic passwords, or general instructions on how and when the counter-strategy can be applied. A number of counter-strategies furthermore require the voter to perform some calculations, such as generating a panic password according to a set list of rules, or performing mathematical calculations, such as the XOR-function with the masking value or the sum of all the ballots cast within election so far. Moreover, several of these calculations also have to be performed during coercion-free voting. As the system can only provide limited feedback, the voter will not notice if they make a mistake in these calculations and thereby accidentally cast a ballot for a wrong candidate.

In case the secrets such as credentials or masking values are sent to the voter as voting materials, either via email or paper post, the voter should be able to *fake these materials* in case the coercer demands access to them.

As mentioned above, aids to these fundamental components of coercion resistant voting systems cannot be presented in an interactive way to the voter. Furthermore, in a scenario with the physical presence of the adversary, even non-interactive supplementary materials (e.g. paper-based instructions) cannot be used, as the adversary will demand the voter to put them away. We therefore propose that early in the development process, user studies are carried out in order to align voting system specifics and requirements with voter capabilities. The introduction of new voting systems, possibly related to new concepts such as coercion resistance, shall be conducted by incorporating accompanying awareness and education campaigns. One should, however, be careful in ensuring that the inclusion of this additional information will not overwhelm the voter or make them distrust the system. It shall be emphasized here that previous research has proven that voters tend to accept and manage slightly more complex processes if this results in an increase of voting security [35]. By involving voters early in the process and providing them continuous support throughout the election, we mitigate the risks that come with the limited voter feedback of coercion resistant voting systems.

**Do not over-rely on technology** The unrealistic assumptions of the coercion resistant schemes show that the problem of coercion in remote voting is unlikely to be solved only by technology. Even if a usable solution is found, it is not guaranteed that the voter is capable of actually applying the solution, especially given the high-stress situation of coercion. When implementing the internet voting system, even the one that is designed to provide coercion resistance protection, one needs to be of the limitations of such protection, and include non-technological measures to prevent voter coercion and vote buying.

**Consider implementing means for detecting coercion** For some of the counter-strategies, the information available to the election officials might reveal some insights on whether coercion was attempted. This would include presence of votes with invalid credentials (for the fake credentials counter-strategy), unusually frequent vote updating (for deniable vote updating) or invalid ballots (for deniable vote updating or masking). The concept of coercion evidence [21] was designed to provide this feature specifically. Such a feature could be a valuable tool in enabling the coerced voters to signal abuse to the authorities. At the same time, it can lead to false positives, such as voters making mistakes during coercion-free voting e.g. by entering an invalid credential, or malicious voters who misuse the coercion detection mechanisms to undermine the legitimacy of the election and the trust of the electoral system. One way to resolve this would be enabling to track the potential coercion attempts back to the individual voters. In that case, however, potential privacy issues have to be considered.

## 5 Conclusions

It is difficult to ensure coercion resistance in e-voting systems, as even the solutions that propose cryptographic protocols are hard to implement in a way that the voters are able to used them effectively. This is evidenced e.g. from the real-world applications of Internet voting systems, where it is either assumed that no coercion takes place (i.e. there are other safeguards in society that protect against this), or some form of protection against coercion is implemented at the cost of verifiability (e.g. deniable vote updating in Estonia and Norway). Given the issues outlined in the paper, designing a practical and usable coercion resistant scheme is a challenge.

It, however, has to be noted, that coercion cannot be fully excluded via traditional in polling-place voting as well, including traditional paper ballots. The possibility of so-called ”ballot selfies”, which would be even harder to prevent as new devices such as smart watches and other wearables that are capable of recording and are harder to detect are becoming wide-spread. For these reasons, Benaloh in particular argued [9] that the techniques to achieve coercion resistance in Internet voting might be of greater help in preventing coercion than simply relying on safety of voting booths. An important direction of future work is therefore developing solutions for the aforementioned human factor-related challenges, including implementations of existing cryptographic schemes, their evaluation via empirical studies and development of new schemes that allow for counter-strategies more suitable for practical use.

A particular challenge is to integrate the coercion resistant property with verifiability, ensuring that the voters can also verify that their vote has been counted correctly. Such an integration is particularly challenging, as the voter should not be able to use the results of verification to construct a proof of how they voted to the adversary. While a few works consider providing verifiability in coercion resistant voting (see e.g. [49]), further investigation into the investigation of human factors involved in ensuring both of these properties is needed.

An interesting further direction of future work is studying the perception of the voters of risk and benefit trade-offs that come from applying coercion resistant strategies, as well as cross-cultural studies investigating the perceptions of these trade-offs in different societies. We furthermore did not consider other technical issues with implementing coercion resistant systems, such as the need to implement an untappable channel between the voter and the voting server (see [33] for an overview and discussion of such issues), which would have to be considered in relation to the human factors as well.

## References

1. Achenbach, D., Kempka, C., Löwe, B., Müller-Quade, J.: Improved coercion-resistant electronic elections through deniable re-voting. JETS: USENIX Journal of Election Technology and Systems **3**(2), 26–45 (2015)
2. Araújo, R., Barki, A., Brunet, S., Traoré, J.: Remote electronic voting can be efficient, verifiable and coercion-resistant. In: International Conference on Financial Cryptography and Data Security. pp. 224–232. Springer (2016)
3. Araujo, R., Foulle, S., Traoré, J.: A practical and secure coercion-resistant scheme for internet voting. In: Towards Trustworthy Elections, pp. 330–342. Springer (2010)
4. Araújo, R., Rajeb, N.B., Robbana, R., Traoré, J., Youssfi, S.: Towards practical and secure coercion-resistant electronic elections. In: International Conference on Cryptology and Network Security. pp. 278–297. Springer (2010)
5. Araújo, R., Traoré, J.: A practical coercion resistant voting scheme revisited. In: International Conference on E-Voting and Identity. pp. 193–209. Springer (2013)
6. Aziz, A.: Coercion-resistant e-voting scheme with blind signatures. In: 2019 Cybersecurity and Cyberforensics Conference (CCC). pp. 143–151. IEEE (2019)
7. Backes, M., Gagné, M., Skoruppa, M.: Using mobile device communication to strengthen e-voting protocols. In: Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society. pp. 237–242. ACM (2013)

8. Basin, D., Radomirovic, S., Schmid, L.: Alethea: A provably secure random sample voting protocol. In: 2018 IEEE 31st Computer Security Foundations Symposium (CSF). pp. 283–297. IEEE (2018)
9. Benaloh, J.: Rethinking voter coercion: The realities imposed by technology. In: Presented as part of the 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (2013)
10. Benaloh, J., Moran, T., Naish, L., Ramchen, K., Teague, V.: Shuffle-sum: coercion-resistant verifiable tallying for stv voting. IEEE Transactions on Information Forensics and Security **4**(4), 685–698 (2009)
11. Bernhard, D., Kulyk, O., Volkamer, M.: Security proofs for participation privacy, receipt-freeness and ballot privacy for the helios voting scheme. In: Proceedings of the 12th International Conference on Availability, Reliability and Security. p. 1. ACM (2017)
12. Bursuc, S., Grewal, G.S., Ryan, M.D.: Trivitas: Voters directly verifying votes. In: International Conference on E-Voting and Identity. pp. 190–207. Springer (2011)
13. Chaidos, P., Cortier, V., Fuchsbauer, G., Galindo, D.: Beleniosrf: A non-interactive receipt-free electronic voting scheme. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 1614–1625. ACM (2016)
14. Chen, G., Wu, C., Han, W., Chen, X., Lee, H., Kim, K.: A new receipt-free voting scheme based on linkable ring signature for designated verifiers. In: 2008 International Conference on Embedded Software and Systems Symposia. pp. 18–23. IEEE (2008)
15. Clark, J., Hengartner, U.: Selections: Internet voting with over-the-shoulder coercion-resistance. In: International Conference on Financial Cryptography and Data Security. pp. 47–61. Springer (2011)
16. Clarkson, M.R., Chong, S., Myers, A.C.: Civitas: Toward a secure voting system. In: 2008 IEEE Symposium on Security and Privacy (sp 2008). pp. 354–368. IEEE (2008)
17. Dossogne, J., Lafitte, F.: Mental voting booths. In: Nordic Conference on Secure IT Systems. pp. 82–97. Springer (2011)
18. Essex, A., Clark, J., Hengartner, U.: Cobra: Toward concurrent ballot authorization for internet voting. In: EVT/WOTE. p. 3 (2012)
19. George, V., Sebastian, M.: An efficient homomorphic coercion resistant voting scheme using hierarchical binary search tree. In: 2009 WRI World Congress on Computer Science and Information Engineering. vol. 1, pp. 502–507. IEEE (2009)
20. Gjøsteen, K.: The norwegian internet voting protocol. In: International Conference on E-Voting and Identity. pp. 1–18. Springer (2011)
21. Grewal, G.S., Ryan, M.D., Bursuc, S., Ryan, P.Y.: Caveat coercitor: Coercion-evidence in electronic voting. In: 2013 IEEE Symposium on Security and Privacy. pp. 367–381. IEEE (2013)
22. Grontas, P., Pagourtzis, A., Zacharakis, A.: Coercion resistance in a practical secret voting scheme for large scale elections. In: 2017 14th International Symposium on Pervasive Systems, Algorithms and Networks & 2017 11th International Conference on Frontier of Computer Science and Technology & 2017 Third International Symposium of Creative Computing (ISPAN-FCST-ISCC). pp. 514–519. IEEE (2017)
23. Gutmann, A., Renaud, K., Volkamer, M.: Nudging bank account holders towards more secure pin management. International Journal of Internet Technology and Secured Transactions **4**(2), 380–386 (2015)

24. Haghighat, A.T., Dousti, M.S., Jalili, R.: An efficient and provably-secure coercion-resistant e-voting protocol. In: 2013 Eleventh Annual Conference on Privacy, Security and Trust. pp. 161–168. IEEE (2013)
25. Heiberg, S., Martens, T., Vinkel, P., Willemson, J.: Improving the verifiability of the estonian internet voting scheme. In: International Joint Conference on Electronic Voting. pp. 92–107. Springer (2016)
26. Hirt, M., Sako, K.: Efficient receipt-free voting based on homomorphic encryption. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 539–556. Springer (2000)
27. Iovino, V., Rial, A., Rønne, P.B., Ryan, P.Y.: Using selene to verify your vote in jcj. In: International Conference on Financial Cryptography and Data Security. pp. 385–403. Springer (2017)
28. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Proceedings of the 2005 ACM workshop on Privacy in the electronic society. pp. 61–70. ACM (2005)
29. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Towards Trustworthy Elections, pp. 37–63. Springer (2010)
30. Kiayias, A., Zacharias, T., Zhang, B.: End-to-end verifiable elections in the standard model. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 468–498. Springer (2015)
31. Kim, S., Oh, H.: A new universally verifiable and receipt-free electronic voting scheme using one-way untappable channels. In: Advanced Workshop on Content Computing. pp. 337–345. Springer (2004)
32. Koenig, R., Haenni, R., Fischli, S.: Preventing board flooding attacks in coercion-resistant electronic voting schemes. In: IFIP International Information Security Conference. pp. 116–127. Springer (2011)
33. Krips, K., Willemson, J.: On practical aspects of coercion-resistant remote voting systems. In: International Joint Conference on Electronic Voting. pp. 216–232. Springer (2019)
34. Krzywiecki, Ł., Kutyłowski, M.: Lagrangian e-voting: Verifiability on demand and strong privacy. In: International Conference on Trust and Trustworthy Computing. pp. 109–123. Springer (2010)
35. Kulyk, O., Neumann, S., Budurushi, J., Volkamer, M.: Nothing comes for free: How much usability can you sacrifice for security? IEEE Security & Privacy (2017)
36. Kulyk, O., Teague, V., Volkamer, M.: Extending helios towards private eligibility verifiability. In: International Conference on E-Voting and Identity. pp. 57–73. Springer (2015)
37. Kulyk, O., Volkamer, M.: Usability is not enough: Lessons learned from human factors in security research for verifiability. E-Vote-ID 2018 p. 66 (2018)
38. Kutyłowski, M., Zagórski, F.: Verifiable internet voting solving secure platform problem. In: International Workshop on Security. pp. 199–213. Springer (2007)
39. Locher, P., Haenni, R., Koenig, R.E.: Coercion-resistant internet voting with everlasting privacy. In: International Conference on Financial Cryptography and Data Security. pp. 161–175. Springer (2016)
40. Marky, K., Kulyk, O., Renaud, K., Volkamer, M.: 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. p. 176. ACM (2018)
41. Neji, W., Blibech, K., Rajeb, N.B.: Incoercible fully-remote electronic voting protocol. In: International Conference on Networked Systems. pp. 355–369. Springer (2017)

42. Neto, A.S., Leite, M., Araújo, R., Mota, M.P., Neto, N.C.S., Traoré, J.: Usability considerations for coercion-resistant election systems. In: Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems. p. 40. ACM (2018)
43. Neumann, S., Volkamer, M.: Civitas and the real world: problems and solutions from a practical point of view. In: 2012 Seventh International Conference on Availability, Reliability and Security. pp. 180–185. IEEE (2012)
44. Nguyen, T.A.T., Dang, T.K.: A practical solution against corrupted parties and coercers in electronic voting protocol over the network. In: Information and Communication Technology-EurAsia Conference. pp. 11–20. Springer (2013)
45. Nguyen Thi, A.T., Dang, T.K.: Enhanced security in internet voting protocol using blind signatures and dynamic ballots. In: Proceedings of the 14th International Conference on Information Integration and Web-based Applications & Services. pp. 278–281. ACM (2012)
46. Olembo, M.M., Volkamer, M.: E-voting system usability: Lessons for interface design, user studies, and usability criteria. In: Human-Centered System Design for Electronic Governance, pp. 172–201. IGI Global (2013)
47. Patachi, Ş., Schürmann, C.: Eos a universal verifiable and coercion resistant voting protocol. In: International Joint Conference on Electronic Voting. pp. 210–227. Springer (2017)
48. Rønne, P.B., Atashpendar, A., Gjøsteen, K., Ryan, P.Y.: Short paper: Coercion-resistant voting in linear time via fully homomorphic encryption. In: International Conference on Financial Cryptography and Data Security. pp. 289–298. Springer (2019)
49. Ryan, P.Y., Rønne, P.B., Iovino, V.: Selene: Voting with transparent verifiability and coercion-mitigation. In: International Conference on Financial Cryptography and Data Security. pp. 176–192. Springer (2016)
50. Sako, K., Kilian, J.: Receipt-free mix-type voting scheme. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 393–403. Springer (1995)
51. Sasse, M.A., Flechais, I.: Usable security: Why do we need it? how do we get it? O'Reilly (2005)
52. Schläpfer, M., Haenni, R., Koenig, R., Spycher, O.: Efficient vote authorization in coercion-resistant internet voting. In: International Conference on E-Voting and Identity. pp. 71–88. Springer (2011)
53. Shirazi, F., Neumann, S., Ciolacu, I., Volkamer, M.: Robust electronic voting: Introducing robustness in civitas. In: 2011 International Workshop on Requirements Engineering for Electronic Voting Systems. pp. 47–55. IEEE (2011)
54. Smart, M., Ritter, E.: Remote electronic voting with revocable anonymity. In: International Conference on Information Systems Security. pp. 39–54. Springer (2009)
55. Smart, M., Ritter, E.: True trustworthy elections: remote electronic voting using trusted computing. In: International Conference on Autonomic and Trusted Computing. pp. 187–202. Springer (2011)
56. Sodiya, A.S., Onashoga, S., Adelani, D.: A secure e-voting architecture. In: 2011 Eighth International Conference on Information Technology: New Generations. pp. 342–347. IEEE (2011)
57. Souheib, Y., Stephane, D., Riadh, R.: Watermarking in e-voting for large scale election. In: 2012 International Conference on Multimedia Computing and Systems. pp. 130–133. IEEE (2012)

58. Spycher, O., Koenig, R., Haenni, R., Schläpfer, M.: A new approach towards coercion-resistant remote e-voting in linear time. In: International Conference on Financial Cryptography and Data Security. pp. 182–189. Springer (2011)
59. Storer, T., Duncan, I.: Two variations to the mcesg pollsterless e-voting scheme. In: 29th Annual International Computer Software and Applications Conference (COMPSAC'05). vol. 1, pp. 425–430. IEEE (2005)
60. Volkamer, M., Renaud, K., Kulyk, O., Emeröz, S.: A socio-technical investigation into smartphone security. In: International Workshop on Security and Trust Management. pp. 265–273. Springer (2015)
61. Weber, S.G., Araujo, R., Buchmann, J.: On coercion-resistant electronic elections with linear work. In: The Second International Conference on Availability, Reliability and Security (ARES'07). pp. 908–916. IEEE (2007)
62. Wen, R., Buckland, R.: Masked ballot voting for receipt-free online elections. In: International Conference on E-Voting and Identity. pp. 18–36. Springer (2009)
63. Xia, Z., Tong, Z., Xiao, M., Chang, C.C.: Framework for practical and receipt-free remote voting. IET Information Security **12**(4), 326–331 (2018)
64. Yi, X., Okamoto, E.: Practical mobile electronic election. In: 2011 IEEE/SICE International Symposium on System Integration (SII). pp. 1119–1124. IEEE (2011)
65. Zaghloul, E., Li, T., Ren, J.: Anonymous and coercion-resistant distributed electronic voting. In: 2020 International Conference on Computing, Networking and Communications (ICNC). pp. 389–393. IEEE (2020)
66. Zhang, Y.: An open framework for remote electronic elections. In: International Conference on Cryptology and Network Security. pp. 304–316. Springer (2008)