A Comparative Security Analysis of the German Federal Postal Voting Process

Michael P. Heinl
Fraunhofer AISEC
Germany

Simon Gölz
Ulm University
Germany

Christoph Bösch
Ulm University
Germany

ABSTRACT

The percentage of votes cast by postal voting increases with every election for the German federal parliament (Bundestag). However, especially compared to Internet voting, concerns regarding security, transparency, and trustworthiness of postal voting are rarely discussed. This paper outlines the established process of postal voting in Germany and evaluates it with regard to various security-relevant characteristics. For this evaluation, a methodology originally developed for Internet voting is used in order to ensure comparability. The aim is to identify weaknesses as well as potential for optimization, to compare German postal voting with selected Internet voting schemes, and to derive implications for policy and further research.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; • **Applied computing** → *Voting / election technologies*; • **Social and professional topics** → *Government technology policy*.

KEYWORDS

Remote Voting, Postal Voting, Internet Voting, Security

ACM Reference Format:
Michael P. Heinl, Simon Gölz, and Christoph Bösch. 2021. A Comparative Security Analysis of the German Federal Postal Voting Process. In *DG.O2021: The 22nd Annual International Conference on Digital Government Research (DG.O'21), June 9–11, 2021, Omaha, NE, USA.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3463677.3463679

1 INTRODUCTION

In the fall of 2021, the elections for the 20th German Bundestag will take place. According to the German Federal Returning Officer, 24.3 percent of voters in the 2013 federal elections and as many as 28.6 percent in 2017 have voted by postal voting [5], a type of remote voting largely taking place in uncontrolled environments. Depending on the development of the COVID-19 pandemic caused by the novel coronavirus SARS-CoV-2, it is expected that the percentage of votes cast by postal voting will increase accordingly in 2021.

As depicted in Table 1, another type of remote voting in uncontrolled environments is Internet voting.[1] Not least due to the pandemic and postal voting's increasing popularity, there recently have been discussions regarding the feasibility of Internet voting in the context of German federal elections [13].

A German law enacted in March 2020 to mitigate the consequences of the COVID-19 pandemic in civil, insolvency, and criminal procedure law, among other things, temporarily lowers the hurdles for Internet elections during general assemblies of associations. For general political elections, Internet voting is still not legally feasible though. Primarily, this is due to a Judgment of the German Federal Constitutional Court (*Bundesverfassungsgericht*/BVerfG) [4] requiring comprehensibility without special knowledge of the technical systems used. Technically, this does not only translate into usability dilemmas [12, 19] but also into more fundamental issues such as the *Secure Platform Problem*[2] and the scalability of attacks [3, 18].

But how about the security of Internet voting compared to the established postal voting process? In the context of the 2020 United States elections, there have been a lot of discussions regarding the security and trustworthiness of postal voting. Despite manifold allegations, a preliminary report of the Organization for Security and Co-operation in Europe (OSCE) [33] concludes that "[...] only two cases of alleged fraud with minor impact were publicly reported."

As the implementations of voting procedures in general and of postal voting in particular differ from country to country, this paper comparatively investigates the security of postal and Internet voting for the case of Germany. While Internet voting has been an active field of research with a strong focus on security for several decades, there have been few studies on the security of postal voting so far [3, 8, 17, 18, 26, 35].

The present paper is intended to complement existing literature by describing the German postal voting process, applying an evaluation methodology originally developed for Internet voting by Langer et al. [22, 24], discussing possible attacks as well as recommendations for improvement, and finally drawing a comparative conclusion from the perspective of Internet voting. The evaluation methodology by Langer et al. [22, 24] has been chosen due to its structured and technical approach compared to other frameworks such as the Council of Europe's Recommendation CM/Rec(2017)5 [30].

[1] In the following, *Internet voting* implicitly refers to Internet voting in uncontrolled environments intended to be used from any Internet-capable device, e.g., the voter's personal computer, which is generally not under the technical and organizational control of the electoral authority. The same applies to *postal voting*. Postal voting in controlled environments (such as the premises of the electoral authority), referred to as postal voting *there and then*, is only meant if explicitly mentioned.

[2] The *Secure Platform Problem* means that the device used to cast the vote cannot be trusted because it could be infected with malware [10].

DG.O'21, June 9–11, 2021, Omaha, NE, USA

Table 1: Categorization of different types of remote voting.

Type of Environment	Paper-based	Internet-based
Uncontrolled	*Traditional* postal voting	On voter's own device
Controlled	Postal voting *there and then*	Kiosk-based

The following considerations are based on the authors' direct observations of the Bundestag election 2017, their written correspondence with the Federal Returning Officer[3], and publicly available sources such as press reports [20, 25, 44, 45, 47] or official documents [31].

Section 2 briefly introduces the German postal voting process in order to contribute to the reader's basic understanding needed for the further sections. Section 3 describes the used methodology including assessment criteria and attacker model. The actual evaluation of the German postal voting system is conducted in Section 4, supplemented by additional security concerns presented in Section 5. Recommendations covering the deficiencies discussed in the former two sections are addressed in Section 6. Section 7 briefly discusses a comparative use case based on a limited audience and draws an overall conclusion.

2 THE GERMAN POSTAL VOTING PROCESS

The German postal voting process can be divided into a total of three election phases: pre-election, election, and post-election. Each phase is briefly explained individually in the following sections. Additionally, Figure 1 briefly illustrates the whole process.

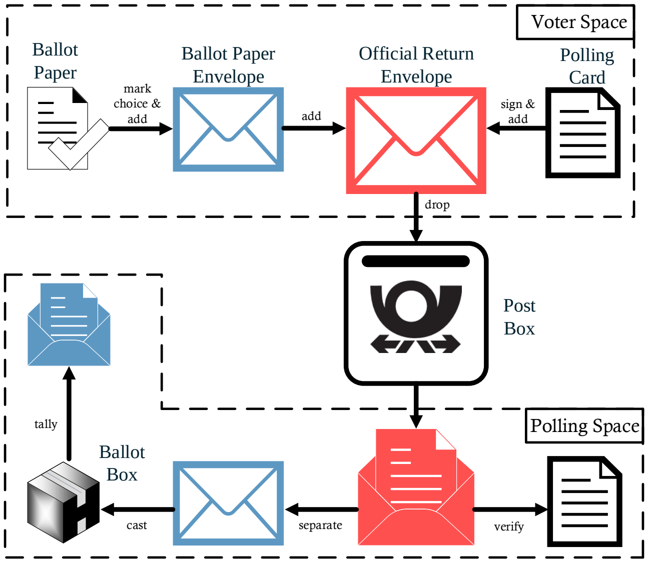

Figure 1: Outline of the German postal voting process.

2.1 Pre-election Phase

Eligible persons can request postal voting documents in different ways. These include personal and written requests in the form of a letter or the correspondingly completed official election notification, by e-mail or fax and, depending on the constituency, by online platform. The request must in any case contain the first name and surname, date of birth, as well as the residential and in certain circumstances a differing shipping address. The request for another person is possible with a written authorization (with original signature of the authorizing person). This authorization along with the corresponding request can be filed either in person or in writing. However, it is not allowed to file it electronically [6].

These postal voting documents will then be sent to those eligible to vote. This happens at the earliest after the entry of all registered persons in the voters' register. In accordance with Section 16 Paragraph 1 of the German Federal Electoral Regulations (*Bundeswahlordnung*/BWO), this happens 42 days before the election. The documents contain a polling card[4] (to confirm the identity of the person eligible to vote), a ballot paper, an information sheet on correct usage, a blue envelope (ballot paper envelope) for the ballot paper, and a larger red envelope (official return envelope) for the blue ballot paper envelope as well as the polling card. For persons who have requested postal voting, a `W` is printed in the corresponding line of the voters' register [32]. On election day, they may only vote by presenting their valid polling card in order to ensure that they have not already voted in advance by employing postal voting.

2.2 Election Phase

In order to participate in the election, the filled in ballot paper must be placed in the blue ballot paper envelope which then has to be sealed. Together with the completed polling card containing an affidavit, the sealed blue ballot paper envelope is then placed in the red official return envelope which then in turn has to be sealed as well. The red official return envelope with the election documents[5] can then either be handed in at the responsible electoral authority or sent to them by postal mail free of charge within Germany. Persons with German citizenship living abroad can be included into the voters' register upon request and then cast their ballot by postal voting as well. For this, they can either hand in the completed election documents to a representation of the Federal Republic of Germany (embassy/consulate) or send them by postal mail. In the latter case, the postage has to be paid by the voter.

[3] The original written correspondence is not attached to this publication due to the fact that it is in German language. However, for everyone interested nevertheless, it is freely available online [12].

[4] The term *polling card* ("Wahlschein" in German) is misleading because in Germany, the election notification often times comes in the form of a postcard whereas the actual polling card is a letter-sized document.

[5] Referred to as *ballot letter.*

2.3 Post-election Phase

After the ballot letter has been received by the electoral authority, it is kept under lock and key until distributed to the responsible postal ballot board on election day. The postal ballot boards consist of five to nine eligible voters and are meant to control each other. At 3:00 p.m., three hours before the end of the official election period, the postal ballot boards begin to open the red ballot letters in order to check the validity of the polling cards and the blue ballot paper envelopes.

Provided the polling card has been signed according to the regulations and the blue ballot paper envelope containing the ballot paper is sealed and untampered with, the two are separated by throwing the blue ballot paper envelope unopened into the ballot box. Once all blue ballot paper envelopes are in the ballot box and the voting period has expired, the ballot box is opened and the votes in the blue ballot paper envelopes are counted.

During both the opening of the red official return envelope and the filling of the ballot box, at least three members of the postal ballot board must be present. During the subsequent tallying, at least five postal ballot board members must be present. As in regular polling station-based presence voting, the entire process is public and can be observed from beginning to end.

3 EVALUATION METHODOLOGY

For the systematic evaluation of the postal voting process, a methodology is used which has first been developed by Langer et al. [22, 24] and was originally meant for Internet voting. In subsequent work [12], the methodology has been extended to include the criteria of *robustness* and *usability* since those are indispensable for practical election procedures.

3.1 Criteria

Although many of today's common requirements for Internet voting are not explicitly mentioned therein, they can all be derived directly or indirectly [12] from the German Basic Law (*Grundgesetz*), the Federal Elections Act (*Bundeswahlgesetz*/BWahlG), the BWO, or fundamental decisions of the Federal Constitutional Court [4]. Depending on the granularity of the used taxonomy, there are about 20 criteria which can be used to identify different areas of security and trustworthiness of Internet voting. A list of five core criteria implying many of the other requirements has been derived to evaluate the different Internet voting schemes [12]:

- In general, **verifiability** enables the voter to convince themselves of the election's integrity. While *individual verifiability* means the voter's possibility to verify the integrity her own vote, *universal verifiability* means the possibility of anyone to verify the election's correctness. This guarantees immediacy, equal voting power, and public traceability of the election. The characteristic of fulfilling both individual as well as universal verifiability is referred to as *end-to-end verifiability*. It is further elaborated in Section 4.1.
- By making it impossible for third parties to find out the voter's actual choice, **secrecy of the ballot** is maintained and the election is therefore secret. Thanks to **receipt-freeness**, voters cannot prove which choice they have actually made. In order to fulfill this characteristic, the requirement of secrecy of the ballot must be met. Considered to be a stronger notion of secrecy, receipt-freeness improves secrecy in the sense that the voter could not even prove her choice afterwards if she wanted to. Vote-buying is thus made more difficult and the electoral freedom is strengthened. The nuances of secrecy and receipt-freeness are further explained in Section 4.2.
- **Coercion-resistance** enables the voter to cast her ballot freely and secretly even in case of coercion. In order to not give the coercer any indication of the plausibility of a choice made, receipt-freeness must be given as described in Section 4.3.
- **Robustness** ensures that the election can be held and will lead to a valid result even under adverse conditions. It is a prerequisite for a successful election and further detailed in Section 4.4.
- The **usability** of the voting scheme is a requirement ensuring that eligible persons are able and willing to use it to cast their ballot. Furthermore, it is important to keep the inhibition threshold for participation in the election as low as possible so that practically all eligible voters can actually vote. This contributes to generality and equality of the election. Furthermore, as described in Section 4.5, the process of individual verifiability has to be usable as well which contributes to the integrity of the election.

3.2 Attacker Model

Previous work [12] provides a guideline to choose between several pre-defined attacker models for elections of different order or to create an individual attacker model. In the following evaluation, an attacker model for first-order elections *with* the ability to attack the production of tools is assumed. This is due to the fact that Bundestag elections are first-order elections [14]. Consequently, it has to be assumed that Bundestag elections are potentially targeted by nation-state attackers with sophisticated capabilities such as supply chain compromise.

The ability to attack the production of tools originally meant the production of complex electronic devices, such as tokens or cryptographic code sheets, which might have to be produced in a trustworthy way on a massive scale in the context of widespread Internet voting. A comparable "tool" in the context of postal voting could for example be the paper used for polling cards and ballot papers. However, the paper currently used in German elections is just plain paper without any additional security features as mentioned in Section 5.3.[6] Compared to the manipulation of electronic devices or cryptographic code sheets, no sophisticated attacks, such as hiring insiders or compromising supply chains, are needed to counterfeit election documents printed on plain paper. Due to its low hurdles, such counterfeit is consequently not considered to be an *attack on the production of tools* in the context of this paper. Hence, for the evaluation of the German postal voting process the results are the same, no matter if the attacker model for first-order elections *with* or *without* the ability to attack the production of tools is applied.

Although counter-intuitive in the first place, there are scenarios, such as voting from abroad, for which applying the mentioned

[6] The usage of security paper is encouraged in Section 6.3 and Table 3 though.

attacker model *without* the ability to attack the production of tools (see Table 4) can make sense in the context of Internet voting. This implies that the needed electronic tools can be produced and delivered in a trustworthy way at least for a limited amount of people as discussed in a concluding comparative use case in Section 7.

4 ANALYSIS OF THE GERMAN FEDERAL POSTAL VOTING PROCESS

In this section, the postal voting process currently established in Germany will be evaluated. For the sake of comprehensibility, the used methodology is successively presented alongside. The methodology [12, 22, 24] was originally developed for the evaluation of Internet voting schemes in uncontrolled environments and is therefore adjusted and shortened to a certain degree in order to better adapt to the context of postal voting. Table 2 summarizes the evaluation's results assuming the attacker model for first-order elections with the ability to attack the production of tools along with two of the most promising Internet voting schemes according to a preliminary evaluation [12].

4.1 Verifiability

As described in Section 3.1, (end-to-end) verifiability [37] can be divided into individual and universal verifiability. The assessment scheme takes this fact into account by providing separate criteria for both.

4.1.1 Individual Verifiability. Individual verifiability can be distinguished into inner [9, 39] and outer [21, 41] verifiability [22, 24]:

- **(IV.1) Inner individual verifiability:** The voter can verify that the ballot letter was received by the electoral authority and that it contains the correct vote.
- **(IV.2) Outer individual verifiability:** The voter can verify that the ballot letter was received by the electoral authority, but cannot verify if it contains the correct vote.

Both forms of individual verifiability can in turn be differentiated according to whether the corresponding verification is possible only after or already before tallying [23]:

- **(IV.x.1) Individual verifiability after tallying:** The voter can verify whether her ballot (IV.2.1)/vote (IV.1.1) has been correctly included in the result.
- **(IV.x.2) Individual verifiability before tallying:** The voter can verify whether her ballot (IV.2.2)/vote (IV.1.2) was correctly submitted to the electoral authority.

Evaluation. The German postal voting process does not provide inner individual verifiability since the ballot paper envelope in which the ballot paper is located is not opened again until before the ballot is going to be tallied. At this point in time (and assuming that both the red and the blue envelopes are correctly separated), it can no longer be linked to the voter in order to guarantee the secrecy of the ballot.

According to the Federal Returning Officer, there is currently no legally binding possibility for voters to inquire about the whereabouts of the ballot letter after it has been sent. It is also not possible to inspect the corresponding voters' register of the postal ballot boards. Hence, not even outer verifiability and therefore no individual verifiability is provided at all.

4.1.2 Universal verifiability. In contrast to individual verifiability, universal verifiability is about each person being able to verify the overall result of the votes cast [9]. In the ideal case, the election's correctness can be verified which apart from the accuracy of the individual votes (accuracy verifiability) includes the fact that only eligible persons have voted (*eligibility verifiability*) [24, 39] and for each of these eligible persons exactly one vote is included in the election result (*uniqueness verifiability*) [22]:

- **(AV.1) Continuous accuracy verifiability:** Everybody can verify that no errors occurred during the entire tallying process.
- **(AV.2) Discrete accuracy verifiability:** Everybody can verify that no errors occurred during a specific part of the tallying process.
- **(EV.1) Unconditional eligibility verifiability:** Everybody can verify (without trusting a party involved in the process) that only eligible voters cast their vote.
- **(EV.2) Conditional eligibility verifiability:** Everybody can verify that only eligible voters have cast their votes. This requires the verifier to trust certain parties involved in the authentication process.
- **(QV.1) Unconditional uniqueness verifiability:** Everybody can verify (without trusting any party involved in the process) that all voters have cast only one tallied vote.
- **(QV.2) Conditional uniqueness verifiability:** Everybody can verify that all voters have cast only one tallied vote. This requires the verifier to trust certain parties involved in the authentication and voting process.

Evaluation. Due to the given possibility of critically observing every single step of the tallying process from beginning to end, *discrete accuracy verifiability* (AV.2) is met. All other types of universal verifiability cannot be guaranteed since it cannot be checked whether the election documents are actually filled in by an eligible person (no *eligibility verifiability*) and whether each eligible person has only cast one vote (*uniqueness verifiability*) or, for example, bought votes from other people or even received them "as a gift" due to political apathy.

4.2 Secrecy and Receipt-Freeness

In order to ensure that the voter is eligible and that her vote is included in the election's result only once, it is necessary to authenticate her at least at one point in the process. However, this requirement is opposed by the mandatory secrecy of the ballot, which is intended to categorically exclude any link between the vote and the voter's identity. Due to this link which has to be prevented, this requirement is also referred to as *unlinkability* [22, 39]:

- **(UL.1) Unlinkability between voter's identity and vote:** An attacker is not able to establish a link between a voter's identity and her vote.
- **(UL.2) Unprovability of link between voter's identity and vote:** An attacker is able to establish a link between a voter's identity and her vote. However, the attacker is not able to prove this link to third parties.

Table 2: Assessment of German postal voting and selected Internet voting schemes assuming an attacker model for first-order elections *with* the ability to attack the production of tools ("/" ≙ requirement not met). Polling station-based presence voting is added for reference.

	Verifiability		Secrecy	Coercion-Resistance	Robustness	Usability	
	Individual	Universal				Voting	Verif.
Presence Voting	IV.1.1	AV.2, EV.2, QV.2	RF	AA.2, RA, SA	RI	UV.1.1	UY.1
Postal Voting	/	AV.2	/	AA.1, RA, SA	RI	UV.1.1	/
Du-Vote [11]	IV.1.1	AV.1, EV.1, QV.1	/	/	/	UV.3.2	UY.2
PGD [38]	IV.2.1	AV.1, QV.1	/	/	RI	UV.2.2	UY.2

Receipt-freeness implicitly includes the secrecy of the ballot which leads to the following definitions based on but stronger than the secrecy of the ballot:

- **(RF) Receipt-freeness:** The attacker is not able, even with the help of the voter, to establish a verifiable link between the voter's identity and her vote.

Evaluation. Due to the fact that the entire election process up to the point of dropping the ballot letter in the postbox or dropping it off at the election authority usually takes place in an uncontrolled environment, it cannot be ensured that the secrecy of the ballot is not already broken during the former steps of the voting process.

Furthermore, the blue ballot paper envelope and the polling card containing the name of the voter are transported in the same red official return envelope. The red official return envelope/ballot letter is not secured against third parties opening it and thus allowing the violation of the secrecy of the ballot. Although only postal and administrative staff should have physical access to the ballot letters after they have been dropped in the postbox, even this represents a potential risk as relevant press reports show [20, 25, 44, 45, 47]. Additionally, there is the possibility of a more sophisticated attack aiming to link a voter's identity and her actual vote without opening the ballot letter based on fingerprinting the used paper [7] in the pre-election as well as post-election phases.

The individual secrecy of the ballot and receipt-freeness can therefore not be guaranteed - especially when considering the very strict rules applied to cryptographic schemes. However, the size of the group of people potentially capable and the scalability of such a physical attack is considered to be much smaller than for Internet voting [3, 18].

4.3 Coercion-Resistance

Contrary to the long-held opinion that coercion-resistance automatically goes hand in hand with receipt-freeness, Juels et al. [16] specify forced-abstention (the attacker coerces the voter to refrain from voting), randomization (the attacker coerces the voter to submit a random vote), and simulation attacks (the attacker coerces the voter to let the attacker vote on behalf of the voter) that are all possible even without knowledge of the vote cast.

Assuming that the voter is unobserved for at least a sufficient period of time during both the registration and voting phases, the following nuances of coercion-resistance exist [24]:

- **(AA.1):** There is a way to circumvent *forced-abstention attacks*, so attackers cannot decide whether their instructions have been followed.
- **(AA.2):** Attackers can't decide whether the voter has voted based on the information provided by the system.
- **(RA):** There is a way to circumvent *randomization attacks*, so attackers cannot decide whether their instructions have been followed.
- **(SA):** There is a way to circumvent *simulation attacks*, so attackers cannot decide whether their instructions have been followed.

Evaluation. Except for the affidavit stating that the ballot has been filled in by oneself and without any external influence, there are no explicit mechanisms to prevent such attacks. The affidavit itself does not represent a significant obstacle for potential coercers. However, in principle it is possible to request a new polling card from the electoral authority within a certain period of time. This implies that the old polling card is going to be invalidated and will no longer be accepted by the responsible postal ballot board at the point of tallying. It is therefore to a limited extent possible to pretend having (finally) cast a vote, e.g., by dropping the ballot letter in the postbox under observation, but then requesting a new polling card from the electoral authority. This kind of "re-voting" is in principle a timely limited measure against absence (AA.1), randomization (RA), and simulation attacks (SA).

4.4 Robustness

It can be differentiated between two types of robustness. External robustness describes a voting system's capability to resist external attacks targeting its availability. Since this property depends on the actual implementation as well as corresponding security measures and capacities of the underlying infrastructure, it is not included in the formal evaluation of Internet voting but rather has to be considered during implementation and realization of such systems. Due to the distributed approach of German postal voting, a broad external attack endangering its availability at scale seems to be rather unrealistic. Another attack vector is trying to internally prevent the tally without attacking the availability of the system itself, e.g., by having an election official refusing to provide the key to decrypt the election result or by pretending to provide allegedly plausible evidence of fraud. The ability to prevent such insider attacks on the system is called internal robustness:

- **(RI) Internal robustness:** The robustness against attacks trying to prevent the tally without attacking the availability of the voting system itself.

Evaluation. Since the ballot letters contained in the ballot box can be opened by any authorized person without any special knowledge, internal robustness (RI) of the postal vote is not endangered in this very context. Due to its already mentioned distributed approach, also an increased internal robustness can be assumed. This is due to the fact that a systematic manipulation by insiders, such as members of the electoral boards, across constituencies is very difficult and even (alleged or not) manipulations in some constituencies do not result in the repetition of the entire election at scale but rather only in those affected constituencies according to Section 83 of the BWO.

4.5 Usability

For electoral procedures to be accepted by the overall population, their usability is an important factor. In the case of Internet voting, too much abstraction of the underlying cryptographic methods is critical due to the requirement of comprehensibility set by the German Federal Constitutional Court [4]. This means that in this context a special focus must be placed on the comprehensibility of the technical-mathematical foundations. The actual level of usability is then assessed based on the complexity and quantity of the inputs needed to successfully vote. These inputs can include simple clicks but also complex cryptographic codes and multiple iterations.

As there are no such obstacles in postal voting, the assessment scheme for the usability of Internet voting is not directly applicable to postal voting and consequently omitted at this point for the sake of brevity and clarity. While UV.x.x describes the usability of the actual voting process, UY.x applies to the usability of the individual verifiability process. It can, however, be generalized that the higher the number, the more complex the input, meaning that for example UV.3.2 is more complex than UV.2.2.

Evaluation. Since the actual process of postal voting is quite user-friendly and comprehensible compared to most advanced approaches of Internet voting, it is evaluated with the best possible criterion, namely single-run click-voting without tools (UV.1.1).

Actually, a distinction is also made between the usability of the voting process itself and the usability of the verification [28]. As already mentioned, the German postal voting process does currently not provide individual verifiability. Consequently, its usability cannot be evaluated.

5 FURTHER SECURITY CONCERNS

This section describes further security concerns regarding postal voting in Germany that arose during participation in the actual process as a voter.

5.1 Registration

The election documents including the polling card can be requested in various ways, e.g., by e-mail. There is no identity verification of the person filing the request. It is furthermore possible to specify a shipping address that differs from the registration address. Section 28 Paragraph 4 BWO actually states that in the case of a deviating shipping address, a notification is sent to the residential address in order to enable the affected person to detect an unauthorized request and to undertake corresponding countermeasures. The practical usage of this possibility to state a differing shipping address during the 2017 Bundestag election showed the authors that there is a risk of incorrect implementation of this control mechanism. Although the notification was sent, it was not sent to the actual residential address but to the shipping address differing from the residential address. A concerned person would therefore no longer be able to detect possible fraud. The circumstances outlined above would allow attackers to request voting documents on behalf of another person.

By their unauthorized request for election documents to be shipped to an attacker-controlled mailbox, attackers can hinder eligible voters who actually plan to vote on election day. This is possible due to the fact that these eligible voters are marked by a W in the voters' register and are therefore only allowed to vote providing their valid polling card. Since the attacker rather than the eligible voter possesses the corresponding polling card, the voter is denied to vote at the polling station according to Section 56 Paragraph 6 Number 2 BWO. Thus, the abstention of an actually eligible voter can be forced by attackers if the notification is not properly implemented. Based on the method presented by Sweeney et al. [42] to obtain addresses and other data via address dealers or from Internet platforms, this attack could be scaled up to a certain extent.

Furthermore, by using the fraudulently obtained postal voting documents themselves, attackers could cast a vote under someone else's name. Although it is necessary for attackers to make a false affidavit, this is a negligible obstacle due to the criminal energy required for this attack anyway and the low risk of detection.

Due to the fact that the notification sent to the residential address is actually legally mandatory, the described circumstance of a wrongly implemented control is not considered during the assessment conducted in Section 4.3. Nevertheless, it is worth mentioning because it indicates the need to regularly audit the implemented processes.

5.2 Return/Verification

As soon as the election documents are successfully delivered to the eligible voter, she can exercise her right to vote and return the sealed ballot letter by postal mail to the responsible electoral authority. Once the ballot letter is dropped in the postbox, the voter loses all active and passive control over it. Neither BWahlG nor BWO provide a process that enables the voter to inquire about the whereabouts of her ballot letter.

A field test during the 2017 Bundestag election in form of an exemplary call with the corresponding electoral authority of one of the authors' constituencies resulted in the same insight, namely that no information about the whereabouts of the ballot letter could be inquired. It is therefore not possible to trace whether the ballot letter was received in time by the electoral authority if it was sent close to election day. Schreiber [40] assumes the responsibility for having the ballot letter dispatched in time with the respective voter which is reasonable due to the fact that the election documents shall be dispatched already six weeks before election day. However, a more serious problem also affects voters who have sent their ballot letter long before the actual election day. Letters can either get lost while being shipped or be deliberately stolen [25, 44, 45]. Both cases cannot be detected by the voter due to the missing legal possibility of verification. On written consultation with the German Federal Returning Officer [12], the authors were informed that voters have the following voluntary options to keep track of the whereabouts of the ballot letter:

- Dispatch of the ballot letter by registered mail with return receipt,
- personal submission of the ballot letter at the electoral authority, and
- if voter collects the election documents at the electoral authority, postal voting there and then.

When sending the ballot letter by registered mail or a similar, traceable form of dispatch, there will be non-negligible costs which must be paid by the voter. The two latter possibilities reduce the risk substantially. However, it is also questionable, how well they are actually accepted by voters due to the comfort losses connected with them. Furthermore, the overall conditions of postal voting there and then at the electoral authority have in fact more similarities to the regular polling station elections than to actual postal voting and are therefore out of scope of this paper.

The three options mentioned can serve to lower the individual risk for voters. However, due to the associated costs or loss of comfort, it is questionable whether they significantly increase the overall security of the entire postal voting process. Furthermore, for voters who have doubts only after sending their ballot letter it should also be possible to determine its whereabouts. According to the principle of *security by design* [15], the legally defined postal voting process should be secure and verifiable rather than transferring responsibility to the individual voter through optional measures.

Irrespective of the probability that the election letter will be successfully delivered to the electoral authority, the question arises how the voter can determine whether her vote actually ended up in the ballot box during the tally on election day. This is another issue regulated neither by the BWO nor the BWahlG. A possible solution is going to be discussed in Section 6.

5.3 Counterfeit Resistance

Several factors contribute to the fact that electoral fraud is difficult to detect and even harder to trace by observers as well as election officials [43]. For example, when the ballot letters are opened, the polling cards are not matched against the complete voters' register. Instead, only a list of invalidated polling cards is employed (*denylisting*) according to Section 75 Paragraph 1 Number 2 BWO. This opens a vector for attackers by forging deceptively real looking election documents and equip them with fictional names and numbers. Since these forged polling cards do not appear on the lists of invalidated polling cards, they cannot be detected this way.

The main reason why documents can be forged deceptively real looking is that they contain no security features. This is astonishing, since these security features (as well as a more thorough verification mechanism for polling cards as the one described above) already existed but had been abolished in 1989 by the First Ordinance to Amend the Federal Election Regulations (*Erste Verordnung zur Änderung der Bundeswahlordnung* [1]). Both the stamped official seal (which is now only printed) and the official signature on the polling card as well as sealing stamps for the envelopes were abolished without replacement in 1989, thereby worsening the security of postal voting.

Due to the lack of seal stamps, voting letters can be opened by employees of the administration or the post office who are then able to tamper with the content. The missing official seals and signatures make it easier for fraudsters to forge election documents and potentially influence the election results by casting illegitimate votes.

6 RECOMMENDATIONS FOR IMPROVEMENT

The postal voting process established in the Federal Republic of Germany has some of the typical problems of remote voting systems in common with their digital counterparts for Internet voting, especially with regard to secrecy/receipt-freeness. These deficits are difficult to overcome without fundamentally changing the character of postal voting as it is employed today. Nevertheless, the following paragraphs provide some approaches that would make postal voting in Germany less prone to errors as well as more comprehensible and secure. Supplementally, Table 3 maps the security deficiencies identified in Sections 4 and 5 onto the recommendations presented in the present section as well as the requirements defined in Section 3.1 and elaborated in Section 4.

6.1 Registration

The risks related to registration described in Section 5.1 could be significantly reduced if the request for postal voting documents required the presentation of a valid identity card when made in person or the voter's notification number[7] (and for additional security a copy of the identity card) when submitted in written or electronic form. In the case of electronic submittal, a portal providing encrypted communication via https, as for example offered by the City of Munich, is preferable.

6.2 Return/Verification

Deficits of the postal voting process with regard to verifiability could be compensated by a legally prescribed obligation of the electoral authority to provide information to the voter. For this, the voter could be given the right to determine the whereabouts of her ballot letter by calling the electoral authority and authenticating herself by stating her name, voter's notification number, and any other information known by the electoral authority but not mentioned in the voter's notification. Furthermore, voters could be granted access to an excerpt of their individual voters' register entry of the corresponding postal ballot board after the election, so that they can determine whether their polling card has been checked on election day and the ballot subsequently has found its way into the ballot box.

In addition, the existing process based on paper trail can be enriched by digital complements. As suggested by Reichmann [36], a QR or barcode could be printed on the official return envelope. It could then be scanned by the electoral authority upon arrival and

[7] Whereby the voter's notification number should be as random as possible.

Table 3: Mapping of security deficiencies, corresponding improvement recommendations, and addressed requirements.

Deficiency	Recommendation(s)	Requirement(s)
Unauthorized opening and/or **dropping** of ballot letters by postal and administrative staff	Systematical mailing of dummy ballot letters in order to detect both deliberate and accidental interference in transit	Secrecy, individual verifiability, universal verifiability
Unauthorized request for polling card	Need to demonstrate knowledge of randomly generated voter's notification number	Universal verifiability, robustness
Wrongly implemented control mechanisms such as the letters sent to residential addresses meant to notify eligible voters of polling cards being sent to a differing shipping address	Regularly audit the practical implementation of control mechanisms	Generally applicable; coercion-resistance for the given example
No possibility to inquire about **the ballot letter's whereabouts**	Legally prescribed and technically supported [36] (e.g., QR or barcode) obligation of the electoral authority to provide information to the voter (authenticated by credentials including a randomly generated voter's notification number) such as arrival of the ballot letter and the corresponding voters' register entry having been checked off	Outer individual verifiability
No possibility to verify whether the ballot was **counted as cast**; i.e., stated the correct voting option when tallied	Enrich the existing postal voting system by digital complements making use of cryptographic procedures [2]	Inner individual verifiability
Polling card **denylisting**; i.e., checking the polling card in question against a list of invalidated polling cards	Polling card allowlisting; i.e., checking the polling card in question against a list of valid polling cards or the voters' register, respectively	Universal verifiability
Election documents easily **forgeable**	Usage of security paper with first line inspection features such as watermarks [46]	Universal verifiability

when the polling card is checked on election day. This would allow the voter to track the whereabouts of her ballot letter (although this raises new questions regarding the security of the system used for this purpose of course). Employing this automated mechanism, the two questions whether the ballot letter arrived at the electoral authority and whether the ballot actually landed in the ballot box on election day and was thus included in the election results could then be answered with at least a certain probability. Benaloh et al. [2] even propose some supplementary yet easy to use cryptographic procedures aiming to provide inner individual verifiability.

In order to be able to initially detect and, if necessary, prosecute systematic manipulation, an independent authority could send dummy ballot letters to the electoral authorities which are not recognizable as such without additional knowledge. They could then be sorted out again based on a corresponding characteristic. This would allow to obtain meaningful statistics on how many election letters are really lost while in transit by mail.

6.3 Counterfeit Resistance

The lamented fact that postal voting documents are too easy to forge could be partially counteracted by reintroducing the security features that were abolished in 1989, i.e., the official seal and official signature on the ballot paper as well as sealing stamps to close the envelopes. An even more effective measure would be the usage of security paper (which is also used for banknotes) with first line inspection features such as watermarks [46]. However, according to the Federal Returning Officer, there are currently no such considerations [12]. The comparison of the received polling cards with the voters' register (*allowlisting*) would also increase the detection rate of forged postal voting documents on election day.

7 CONCLUSION

Security concerns still outweigh the question whether paper-based voting could be replaced by Internet voting. Considering the current state of the art, a large-scale replacement of postal voting or even polling station-based presence voting by Internet voting is not justifiable from the authors' point of view. There are indeed sophisticated Internet voting schemes, such as the code voting-based Pretty Good Democracy (PGD) [38] or the hybrid approach Du-Vote [11] which (with the exception of coercion-resistance) are comparable to the postal voting process under the assumption of the attacker model for first-order elections without the ability to attack the production of tools (see Table 4). They even fulfill additional requirements, such as individual verifiability. Applying an attacker model for first-order elections *with* the ability to attack the production of tools (see Table 2), the secrecy of these Internet

Table 4: Assessment of German postal voting and selected Internet voting schemes assuming an attacker model for first-order elections *without* the ability to attack the production of tools ("/" ≙ requirement not met). Polling station-based presence voting is added for reference.

	Verifiability		Secrecy	Coercion-Resistance	Robustness	Usability	
	Individual	Universal				Voting	Verif.
Presence Voting	IV.1.1	AV.2, EV.2, QV.2	RF	AA.2, RA, SA	RI	UV.1.1	UY.1
Postal Voting	/	AV.2	/	AA.1, RA, SA	RI	UV.1.1	/
Du-Vote [11]	IV.1.1	AV.1, EV.1, QV.1	RF	/	/	UV.3.2	UY.2
PGD [38]	IV.2.1	AV.1, QV.1	RF	/	RI	UV.2.2	UY.2

voting schemes is at stake though since they rely on the trustworthy production of hardware tokens (Du-Vote) or code sheets (PGD).

However, due to the deficiencies in the postal voting process that have been identified, the question arises whether Internet voting should at least be considered as an alternative to postal voting for German citizens living abroad who cannot directly submit their ballot letters to German diplomatic missions and are therefore dependent on the use of infrastructure either controlled by foreign governments or unreliable [27]. This is particularly relevant in light of the fact that elections have recently become increasingly close and could be decided by postal votes as, for example, shown in the 2020 United States presidential elections or the 2016 runoff for the presidential elections in Austria [29]. As described in Section 3.2 and Table 4, for this scenario, a slightly weaker attacker model could be assumed implying that the trustworthy production and provision of tools is possible for the correspondingly limited audience.

Considering the hypothetical effort of safeguarding the corresponding production and provision on such a huge scale to be able to supply all potential voters with trustworthy tools, postal voting seems to be the more viable approach overall. Apart from its obvious practicability and comprehensibility compared to Internet voting, postal voting also has the decisive advantage that attacks on it are not scalable or at least not without great effort [3, 18].

Admittedly, there are risks such as postal or administrative personnel illegitimately opening ballot letters [20, 25, 44, 45, 47]. However, due to the distributed approach of Germany's postal voting system, the severity of such an attack would be rather limited. In order to increase its impact, the amount of conspiring people would have to at least linearly correlate with the amount of compromised constituencies. This in turn increases the difficulty of such a plot to stay undetected, especially compared with the stealthy exploitation of an Internet voting scheme's potential vulnerability unknown to the electoral authority and the public. From an adversary's perspective, attacks based on the forgery of election documents have the advantage that they do not require hiring or infiltrating insiders. Therefore, the probability of such an attack being detected as well as of prosecution in case the attack got detected are lower compared to an attack requiring insiders. This estimation is emphasized by the described denylisting approach which is only capable of detecting polling cards previously declared invalid. Due to this and the severity of smuggling in forged ballots, the authors highly recommend establishing the allowlisting approach described in Table 3.

Although the polling station-based presence voting has a difficult stand in times of COVID-19, it is the first choice from both the perspective of the German Basic Law itself [34] as well as from the mostly security-related criteria derived from it and discussed in this paper. From the authors' point of view, it would be gratifying if in the context of the current situation, which stimulates the discussion regarding alternative models of voting, not only the percentage of votes cast by postal voting continued to increase, but also the inherent security of the postal voting process. For instance, in the form of individual verifiability by employing digital complementary functions while simultaneously maintaining the comprehensibility and the resilience caused by the distributed nature of the paper-based approach [2, 36]. Therefore, future work could include partnerships with electoral authorities surveying their perspective, deriving requirements, and implementing proof of concepts which could then ideally be tested in the field. Concluded, both the analogues as well as the digital world have their advantages. Hence, it's important not to play them off against each other but rather to combine the best of both worlds.

REFERENCES

[1] 1989. Erste Verordnung zur Änderung der Bundeswahlordnung. https://dejure.org/BGBl/1989/BGBl._I_S._1981

[2] Josh Benaloh, Peter Y. A. Ryan, and Vanessa Teague. 2013. Verifiable Postal Voting. In *Security Protocols XXI*, Bruce Christianson, James Malcolm, Frank Stajano, Jonathan Anderson, and Joseph Bonneau (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 54–65. https://doi.org/10.1007/978-3-642-41717-7_8

[3] Katharina Bräunlich and Grimm Rüdiger. 2016. *Einfluss von Wahlszenario auf Geheimheit, Privatheit und Öffentlichkeit der Wahl.* Arbeitsberichte FB Informatik 2016/2. Universität Koblenz-Landau. https://kola.opus.hbz-nrw.de/opus45-kola/frontdoor/deliver/index/docId/1316/file/Einfluss_von_Wahlszenario_auf_Geheimheit_Privatheit_und_Oeffentlichkeit_der_Wahl.pdf

[4] Bundesverfassungsgericht. 2009. Judgment of the Second Senate of 3 March 2009 - 2 BvC 3/07 -, paras. 1-166. (03 2009). https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html;jsessionid=393F8F7CF286625A3FE9E633FFDF7691.1_cid386l

[5] Der Bundeswahlleiter. 2017. Anteil der Briefwählerinnen und Briefwähler bei den Bundestagswahlen 1994 bis 2017 nach Ländern (auf Grundlage des amtlichen Endergebnisses. https://www.bundeswahlleiter.de/dam/jcr/b4aeabb8-7fac-473e-8581-cd718cb7a007/BTW_ab94_briefwahl.pdf

[6] Der Bundeswahlleiter. 2017. Bundestagswahl 2017 - Briefwahl. https://www.bundeswahlleiter.de/bundestagswahlen/2017/informationen-waehler/briefwahl.html

[7] William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman, and Edward W. Felten. 2009. Fingerprinting Blank Paper Using Commodity Scanners. In *2009 30th IEEE Symposium on Security and Privacy.* 301–314. https://doi.org/10.1109/SP.2009.7

[8] Véronique Cortier, Jérémie Detrey, Pierrick Gaudry, Frédéric Sur, Emmanuel Thomé, Mathieu Turuani, and Paul Zimmermann. 2011. Ballot stuffing in a postal voting system. In *2011 International Workshop on Requirements Engineering for Electronic Voting Systems.* 27–36. https://doi.org/10.1109/REVOTE.2011.6045913

[9] Stéphanie Delaune, Steve Kremer, and Mark Ryan. 2009. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security* 17, 4 (2009), 435–487. http://www.lsv.fr/Projects/anr-avote/PUBLIS/DKR-jcs08.pdf

[10] Ed Gerck, C. Andrew Neff, Ronald L. Rivest, Aviel D. Rubin, and Moti Yung. 2002. The Business of Electronic Voting. In *Financial Cryptography*, Paul Syverson (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 243–268. https://doi.org/10.1007/3-540-46088-8_21

[11] Gurchetan S. Grewal, Mark D. Ryan, Liqun Chen, and Michael R. Clarkson. 2015. Du-Vote: Remote Electronic Voting with Untrusted Computers. In *2015 IEEE 28th Computer Security Foundations Symposium*. 155–169. https://doi.org/10.1109/CSF.2015.18

[12] Simon Gölz, Michael P. Heinl, and Christoph Bösch. 2019. *Trustworthy Elections? Eine Übersicht aktueller Verfahren & Probleme von Internetwahlen in unkontrollierten Umgebungen.* Technical Report. https://doi.org/10.18725/OPARU-22691

[13] Christian Haase. 2020. Pressestatement | Höhere Wahlbeteiligung dank Briefwahl. https://haasechristian.de/kpv/artikel/news/pressestatement-hoehere-wahlbeteiligung-dank-briefwahl/

[14] Jörg Helbach. 2010. *Eingrenzung des Secure Platform Problems bei Internetwahlsystemen mit Hilfe von Code Voting.* Ph.D. Dissertation. Ruhr-Universität Bochum. https://hss-opus.ub.ruhr-uni-bochum.de/opus4/frontdoor/index/index/year/2018/docId/2648

[15] Michael Howard and Steve Lipner. 2006. *The security development lifecycle.* Microsoft Press, Redmond, WA, USA. http://download.microsoft.com/download/C/8/F/C8FF968E-91C6-4E91-BF4E-00352917169D/11_Microsoft_Security_Development_Lifecycle.pdf

[16] Ari Juels, Dario Catalano, and Markus Jakobsson. 2005. Coercion-Resistant Electronic Elections. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (Alexandria, VA, USA) *(WPES '05)*. Association for Computing Machinery, New York, NY, USA, 61–70. https://doi.org/10.1145/1102199.1102213

[17] Robert Krimmer and Melanie Volkamer. 2005. Bits or Paper? Comparing Remote Electronic Voting to Postal Voting. In *Electronic government: workshop and poster proceedings of the Fourth International EGOV Conference 2005, August 22 - 26, 2005, Copenhagen, Denmark. Ed.: Kim V. Andersen*, Vol. 13. Univ.-Verl. Trauner, Linz, 225–232.

[18] Robert Krimmer and Melanie Volkamer. 2005. Wählen auf Distanz: Ein Vergleich zwischen elektronischen und nicht elektronischen Verfahren. In *Effizienz von e-Lösungen in Staat und Gesellschaft: aktuelle Fragen der Rechtsinformatik; Tagungsband des 8. Internationalen Rechtsinformatik-Symposions.* Boorberg, Stuttgart, 256–262.

[19] Oksana Kulyk, Stephan Neumann, Jurlind Budurushi, and Melanie Volkamer. 2017. Nothing Comes for Free: How Much Usability Can You Sacrifice for Security? *IEEE Security & Privacy* 15, 3 (2017), 24–29. https://doi.org/10.1109/MSP.2017.70

[20] Thomas Kutschbach. 2014. Ärger mit der Post: Briefe, die nie ankommen. *Berliner Zeitung* (05 03 2014). https://www.berliner-zeitung.de/panorama/aerger-mit-der-post-briefe--die-nie-ankommen-3219438

[21] Costas Lambrinoudakis, Dimitris Gritzalis, Vassilis Tsoumas, Maria Karyda, and Spyros Ikonomopoulos. 2003. Secure Electronic Voting: the Current Landscape. In *Secure Electronic Voting.* 101–122.

[22] Lucie Langer. 2010. *Privacy and Verifiability in Electronic Voting.* Ph.D. Dissertation. Technische Universität Darmstadt. https://tuprints.ulb.tu-darmstadt.de/2313/2/Dissertation_Langer.pdf

[23] Lucie Langer, Axel Schmidt, Johannes Buchmann, and Melanie Volkamer. 2010. A Taxonomy Refining the Security Requirements for Electronic Voting: Analyzing Helios as a Proof of Concept. In *2010 International Conference on Availability, Reliability and Security.* 475–480. https://doi.org/10.1109/ARES.2010.106

[24] Lucie Langer, Axel Schmidt, Johannes Buchmann, Melanie Volkamer, and Alexander Stolfik. 2009. Towards a Framework on the Security Requirements for Electronic Voting Protocols. In *Proceedings of the 2009 First International Workshop on Requirements Engineering for e-Voting Systems (RE-VOTE '09).* IEEE Computer Society, Washington, DC, USA, 61–68.

[25] Raphael Moritz. 2013. Pannen bei der Briefwahl. *Handelsblatt* (09 10 2013). http://www.handelsblatt.com/8908552.html

[26] Robert Müller-Török. 2019. The Principles Established by the Recommendation CM/Rec(2017)5 on Standards for E-voting Applied to Other Channels of Remote Voting. *Masaryk University Journal of Law and Technology* 13 (06 2019), 3. https://doi.org/10.5817/MUJLT2019-1-1

[27] Robert Müller-Török and Arne Pautsch. 2015. Stochastische Verfälschung von Wahl ergebnissen bei grenzüberschreitender Briefwahl? *Verwaltung & Management* 21 (01 2015), 192–197. https://doi.org/10.5771/0947-9856-2015-4-192

[28] Stephan Neumann and Melanie Volkamer. 2014. *A Holistic Framework for the Evaluation of Internet Voting Systems.* IGI Global, Hershey, PA, USA, 76–91. https://doi.org/10.4018/978-1-4666-5820-2.ch004

[29] Erich Neuwirth and Walter Schachermayer. 2016. Some Statistics concerning the Austrian Presidential Election 2016. *Austrian Journal of Statistics* 45 (09 2016). https://doi.org/10.17713/ajs.v45i3.596

[30] Council of Europe. 2017. Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. https://rm.coe.int/0900001680726f6f

[31] The German Federal Returning Officer. 2020. Essential legal bases of Bundestag elections. https://www.bundeswahlleiter.de/en/bundestagswahlen/2021/rechtsgrundlagen.html

[32] Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) - Office for Democratic Institutions and Human Rights (ODIHR) Wahlexpertenteam (Election Expert Team). 2009. Abschlussbericht: Bundesrepublik Deutschland - Wahl zum Deutschen Bundestag am 27. September 2009. http://www.osce.org/de/odihr/elections/germany/40879?download=true

[33] Organization for Security and Co-operation in Europe (OSCE) - Office for Democratic Institutions and Human Rights (ODIHR) International Election Observation Mission. 2020. United States of America - General Elections, 3 November 2020: Statement of preliminary findings and conclusions. https://www.osce.org/files/f/documents/9/6/469437.pdf

[34] Frederik Orlowski and Simon Pohlmann. 2020. Die Briefwahl: Ein scharfes Schwert im Kampf gegen Epidemien? *Zeitschrift für Parteienwissenschaften* 2020, 1. https://doi.org/10.25838/oaj-mip-202038-43

[35] Jordi Puiggali and Victor Morales-Rocha. 2007. Remote Voting Schemes: A Comparative Analysis. In *E-Voting and Identity*, Ammar Alkassar and Melanie Volkamer (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 16–28. https://doi.org/10.1007/978-3-540-77493-8_2

[36] Emilie Reichmann. 2016. Einwurf - Zukunft der Demokratie: Mehr Briefwahl wagen! Ausgabe 3. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/ZD_EINWURF_03_2016.pdf

[37] Ronald L. Rivest. 2006. *The ThreeBallot voting system.* VTP Working Paper 56. Caltech/MIT Voting Technology Project (VTP). https://dspace.mit.edu/handle/1721.1/96593

[38] Peter Y. A. Ryan and Vanessa Teague. 2009. Pretty Good Democracy. In *Security Protocols XVII, 17th International Workshop, Cambridge, UK, April 1-3, 2009. Revised Selected Papers.* 111–130.

[39] Krishna Sampigethaya and Radha Poovendran. 2006. A Framework and Taxonomy for Comparison of Electronic Voting Schemes. *Computers and Security* 25, 2 (March 2006), 137–153.

[40] Wolfgang Schreiber. 2017. *BWahlG: Kommentar zum Bundeswahlgesetz* (10 ed.). Carl Heymanns.

[41] Warren D. Smith. 2005. New cryptographic election protocol with best-known theoretical properties. In *Proc. of Workshop on Frontiers in Electronic Elections.* 1–14.

[42] Latanya Sweeney, Ji Su Yoo, and Jinyan Zang. 2017. Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections. *Technology Science* (05 09 2017). https://techscience.org/a/2017090601

[43] Jörg Thoma. 2013. Wahlbetrug leicht gemacht. *Golem.de* (05 07 2013). https://www.golem.de/news/hacking-wahlbetrug-leicht-gemacht-1307-100234.html

[44] Jan Thomsen. 2013. 64.000 Wahlscheine beantragt: Verfassungsrechtler kritisieren Briefwahl. *Berliner Zeitung* (18 08 2013). http://www.berliner-zeitung.de/4464084

[45] Lina Timm. 2013. Briefwahl-Skandal: Bleiben Tausende Wähler ohne Stimme? *Focus* (21 09 2013). http://www.focus.de/politik/deutschland/bundestagswahl-2013/tid-33649/stimmzettel-verschwunden-briefwahl-skandal-bleiben-tausende-waehler-ohne-stimme_aid_1107824.html

[46] Rudolf L. van Renesse. 1997. Paper based document security - a review. In *Proceedings of the European Conference on Security and Detection - ECOS97 Incorporating the One Day Symposium on Technology Used for Combatting Fraud.* Institution of Engineering and Technology (IET). https://digital-library.theiet.org/content/conferences/10.1049/cp_19970425

[47] Fabian Wahl. 2011. Tausende Briefe und Pakete kommen nie an. *Die Welt* (22 08 2011). https://www.welt.de/wirtschaft/article13558939/Tausende-Briefe-und-Pakete-kommen-nie-an.html