Combatting electoral traces: the Dutch tempest discussion and beyond*

Wolter Pieters

Faculty of Electrical Engineering, Mathematics and Computer Science
University of Twente

Abstract. In the Dutch e-voting debate, the crucial issue leading to the abandonment of all electronic voting machines was compromising radiation, or tempest. Other countries, however, do not seem to be bothered by this risk. In this paper, we use actor-network theory to analyse the socio-technical origins of the Dutch tempest issue in e-voting, and its consequences for e-voting beyond the Netherlands. We introduce the term *electoral traces* to denote any physical, digital or social evidence of a voter's choices in an election. From this perspective, we provide guidelines for risk analysis as well as an overview of countermeasures.

1 Introduction

In the Netherlands, electronic voting machines were introduced in the 1990s without much controversy. A major debate was started by an activist group in 2006. As in the US, the discussion seems to revolve around correctness and verifiability.

In the Dutch e-voting debate, however, the crucial issue leading to the abandonment of all electronic voting machines was tempest (also written TEMPEST, supposedly being an acronym for Telecommunications Electronics Material Protected from Emanating Spurious Transmission or something similar), related to the secrecy of the ballot. Tempest involves listening to so-called "compromising emanations", i.e. radio emission from the device, in this particular case the display. In this way, it would be possible to eavesdrop on the information shown, and thereby deduce a relation between the vote cast and the identity of the voter. Whereas the secrecy of the ballot is anchored in law in many other countries, they generally do not seem to be bothered much by this risk. The issue has only been mentioned incidentally, and without implementation details [7,13,3].

In this paper, we ask the question why tempest became so prominent in the Dutch debate. We analyse the emergence of the Dutch tempest issue from the point of view of actor-network theory, and discuss its possible consequences for e-voting beyond the Netherlands. As far as we are aware, this is the first systematic account of this discussion. In order to place it in a broader scientific context, we introduce the term *electoral traces* to denote any physical, digital

[*] All the information in this article is based on publicly available documents and scientific analysis thereof.

or social evidence of a voter's choices in an election. From this perspective, we provide guidelines for risk analysis as well as an overview of countermeasures.

In section 2, we provide an overview of the electronic voting controversy in the Netherlands. In section 3, we zoom in on the tempest issue from the point of view of actor-network theory [16]. We investigate how the tempest issue was constructed in the debate, and why the issue could not be resolved. In section 4, we place the tempest issue in the context of electoral traces, and suggest guidelines for analysing such risks in different voting systems. In section 5, we discuss the possible consequences of the tempest issue for e-voting beyond the Netherlands, in terms of means to combat vote traces. The final section draws conclusions from the presented analysis.

2 The electronic voting controversy in the Netherlands

2.1 Background

The Netherlands are a constitutional monarchy, and have a system of proportional representation for local and national elections. Since 1928, the option of "stemmen bij volmacht" (voting by proxy) exists: one can authorise other people to cast one's vote. The possibilities for authorisation have been restricted over time, because, especially in local elections, there had been cases of active vote gathering. By now, one is only allowed to have two authorisations. Since 1983, Dutch citizens living abroad, or having job duties abroad during the elections, are allowed to vote by postal ballot. Postal voting is not allowed within the country.

The Netherlands have been ahead in electronic voting for some time. In 1965, a legal provision was put in place to allow the use of machines, including electronic ones, in voting. In the late 1980s, attempts were made to automatise the counting, and the first electronic voting machines appeared. From 1994, the government actively promoted the use of electronic voting machines in elections. Since then, voting machines have been used extensively. The most widely used voting machines were produced by the company Nedap. These were so-called full-face DREs, with a button for each candidate. There was no paper trail. More recently, touch-screen based systems marketed by the former state press Sdu were also used, notably in Amsterdam.

In 1997, regulation on voting machines was introduced, including an extensive list of requirements that voting machines have to meet ("Regeling voorwaarden en goedkeuring stemmachines"). The full requirements specification, consisting of 14 sections, existed as an appendix to the regulation. We quote and translate some items from section 8: Reliability and security of the voting machine:

- The storage of the cast votes is made redundant. The vote is stored in such a redundant way in the vote memory, that it can be proved that the failure rate is 1 x 10E-6. If there is a discrepancy in the redundant storage, the machine will report this to the voter and the voting station;

- The voting machine is able to avoid or reduce the possibilities for accidental or intended incorrect use as much as is technically feasible in fairness;
- The way of vote storage does not enable possibilities to derive the choice of individual voters;
- The voting machine has features which help to avoid erroneous actions during repair, maintenance and checks, for example by mechanical features which preclude assembly in wrong positions or in wrong places.

The possibility of recount or other forms of verification are not mentioned. Furthermore, most of the requirements in section 8 concern correctness under normal circumstances, and not especially security against possible election fraud.

An experiment with Internet voting took place during the European elections in 2004. Participation was intended for expatriates, who had the option to vote by mail before. This possibility is typically used by 20,000 - 30,000 people, of the about 600,000 potential participants. They were given the opportunity to vote via Internet or phone. For this purpose, the KOA system was developed in 2003–2004, and a law regulating the experiment was passed through parliament [18].

The main setup of the system was as follows [6]. Voters registered by ordinary mail, and chose their own access code as password. In return they received a vote code as "login", together with a list of candidates, each with her own candidate code. There were 1000 different lists in the experiment. Combining login and candidate code, one could then cast a vote.

A somewhat more sophisticated system, called RIES, was developed by the water board of Rijnland together with two companies cooperating under the name TTPI. A water board (Dutch: hoogheemraadschap or waterschap) is a regional government body for water management. Its officials are usually elected via ordinary mail, but voter participation for these elections is typically fairly low. An experiment with election via the Internet was conducted in the regions Rijnland and Dommel in 2004, with 1 million eligible voters. 120,000 people voted online, but turnout did not increase.

The RIES system uses cryptographic operations to protect votes and at the same time offer good transparency, at least in principle. It is possible for voters to verify their vote after the elections, and for independent institutions to do a full recount of the results [11]. RIES was also used in the second remote voting experiment for expats during the national elections in 2006, instead of the KOA system from 2004.

2.2 "We don't trust voting computers"

Criticism of the obscurity of the election procedure when using voting machines increased after 2000. Main reasons were the secrecy of the source code and the evaluation reports, and the lack of verifiability. After Ireland had insufficient confidence to use the Nedap machines they bought in the elections [5], Dutch politicians started asking questions about the safety and verifiability of such machines. At first, the government responded that everything was OK and not much happened.

In Fall 2006, the pressure group “Wij vertrouwen stemcomputers niet” (“We don’t trust voting computers”), founded around June, managed to get hold of a couple of Nedap voting machines. They took them apart and reverse-engineered the source code. They made the results of their analysis public in a national television programme on October 4, with the general elections scheduled for November 22 [9]. The first main problem they identified was the easy replacement of the program chips, allowing the attacker to have the machine count incorrectly, or execute any other desired task. The second one was the possibility to eavesdrop on the voting machine and the choice of the voter via a tempest attack. Also, they found problems with the security of the storage facilities where the machines were kept in between elections.

The tempest attack was particularly successful because there is a special (diacritical) character in the full name of one of the parties. This required the display to switch to a different mode with a different refresh frequency, which could easily be detected. The minister responded to the findings of the activists by having all the chips replaced with non-reprogrammable ones (a questionable solution, because the chips had been *replaced*, not *reprogrammed*), seals on all the machines, and having the intelligence agency look into the tempest problem.

The fix for the diacritical character problem was easy (don’t use special characters). With that implemented, the signal emitted from the Nedaps was fairly limited. However, the intelligence agency also looked into the other type of voting machine, the touch-screen based system produced by the former state press Sdu. They found that the tempest issue was much worse there, and someone outside the polling station might be able to reconstruct the whole screen from the signal.

The technical requirements only stated that voting machines should maintain the secrecy of the vote *in storing the vote*, not in casting. Nonetheless, the minister suspended the certification for the Sdu machines three weeks before the elections. This affected about 10% of the voter population, including Amsterdam. Some districts got spare Nedaps, but others had to use paper ballots, especially because the certification of one of the older Nedap types was suspended later.

2.3 Commissions and reports

On September 27, the Election Process Advisory Commission reported on the future of the electoral process in the Netherlands [1]. The report stated that the primary form of voting should be voting in a polling station. Internet voting for the whole population would not be able to guarantee transparency, secrecy and freedom of the vote sufficiently. It was advised to equip polling stations with “vote printers” and “vote counters” instead of electronic voting machines, providing a paper vote in between the two stages. Vote printers would only print the voter’s choice, which would then be verified by the voter and put in a ballot box. After the close of the polls, the vote counter would scan the votes and calculate the totals.

The American solution of a paper trail was not advised. It was argued that registering the vote twice, electronically and on paper, could lead to different outcomes, depending on which registration would have priority in case of a dispute. Significantly, systems without a paper copy of the vote were not considered as alternatives, for reasons of transparency.

A technical expert group was formed to investigate the practical issues involved in the commission's proposal. Because of research into the tempest issue [15], the option of a vote printer was judged not to be feasible. Machine counting of manually cast paper votes was not considered, for unclear reasons. It might be that the government did not want to reconsider the design of the ballot for this purpose (the huge present Dutch ballots are impossible to feed automatically into a machine). Besides, problems in the United Kingdom with this type of e-counting were a reason for the Election Process Advisory Commission not to recommend this option. It was tried to propose to use machines similar to the Nedaps for counting by the poll workers. They would then enter the paper votes manually into the machine. Because of the separation between the voter and the electronic processing of the vote, this would resolve the tempest issue. However, parliament could not be convinced that this would reduce the other security problems involved in electronic voting, and rejected the option.

Finally, the planned Internet voting for the water boards in 2008 was also cancelled after independent investigations reported security problems [8]. Electronic counting of postal ballots for the water boards was continued, though.

3 The construction of tempest

In this section, we investigate how tempest came to be the crucial factor in the Dutch electronic voting controversy. We take the perspective of actor-network theory (ANT) [16], which focuses on social dynamics in terms of the forming of associations between different entities, both human and nonhuman. The first part of the section discusses how a coalition emerged supporting the seriousness of the tempest problem in electronic voting. The second part analyses how the Netherlands ended up with a norm stating that the radiation should not reach beyond 5 metres from the machine. The final part discusses the emergence of consensus about the impossibility of solving the problem.

3.1 The association of tempest supporters

It is important to start the analysis with the observation that there did not exist any social means to support the tempest issue before the start of the activist group's campaign. In the requirements, it was stated that the secrecy of the ballot needed to be ensured in storing the vote, not in casting. The risk of compromising radiation had thus been hidden in the requirements. Only from 2006, a social coalition emerged to support the tempest issue.

From the perspective of ANT, the tempest issue is a complex association between different types of beings. First of all, there is the activist group, trying to put e-voting on the political agenda. Secondly, there is a seemingly innocent design feature of the Nedap machines, allowing special characters to be displayed. Thirdly, there is a major Dutch political party which actually has a special character in its name. Fourthly, there is another type of electronic voting machine, using a much larger screen (touchscreen). Fifthly, there is a legal framework demanding a secret ballot, but not verifiability of election results. Sixthly, there is an intelligence service with all kinds of measurement equipment for radiation.

The forming of a coalition between these apparently incompatible entities goes roughly as follows. First of all, the possibility of special characters in names of political parties forces Nedap to enable the display of these characters in their machines. This feature is actually used in Dutch elections, because one of the Dutch parties has such a character. Here, the naming of the party and the design of the machine form an alliance.

Since the activist group wants to put e-voting on the political agenda, they are looking for problematic features of the machines to be demonstrated to the public and politicians. Accidentally, they find out that a radio antenna receives signals from the Nedap machines, which sound differently depending on the party selected. An alliance now forms between the name, the design, and the intention of the pressure group to *demonstrate* problems. Enter the TV programme, which is interested in news that can be easily showed to the public. The tempest issue meets this criterion,[1] and is therefore included in the programme on the activist group's findings.

At this point, had there been no expertise, the issue might have been resolved by just ignoring the special character in the name. However, there is both an intelligence agency with expertise on this matter, as well as a different type of voting machine. An extended alliance is created here, where the intelligence service can show that even if the Nedap special character issue can be resolved, there are still problems with the other type of machine. Moreover, both the government and the activist group are looking for legal foundations for taking action against the machines: the activist group to enforce the abolishing of the machines, the government to respond to public pressure. Since there is nothing in the law about verifiability, which was the main topic of the activists, it is convenient for both to turn to the secret ballot instead. The coalition is now complete.

This coalition stands for the now undeniable fact that e-voting machines cause trouble with compromising emanation. The question now becomes what the consequences should be, especially in terms of which levels of radiation are acceptable and which are not. At some point, the consensus seems to be that it should not be possible to capture radiation from beyond 5 metres distance [10]. From a measurement perspective, this still does not solve the question, as radiation decreases quadratically with the distance, but only reaches zero asymptotically. Everything thus depends on the size of the antenna used, but the 5 metre norm does not specify this. Where, then, did this norm come from?

[1] See `http://www.youtube.com/watch?v=B05wPomCjEY`

3.2 The association of 5 metre measurers

Let us quote some longer fragments by the responsible minister from the parliamentary reports on the issue:

> "The possibility that the choice of a voter can be assessed outside of the voting booth is a source of concern, and all possible efforts will be made to find a solution. The possibility can never be completely excluded though, even when voting with paper and pencil. After all, with a small camera in the voting booth observation of the voter's choice is also possible. This can never be prevented completely, but if there were any indication of such a thing happening, extra supervision is of course possible. Something similar must happen now as well. The problem consists of two parts. Radiation can be captured up to tens of metres of distance from the voting machine, i.e. outside the polling station too. This is not the first concern, for someone outside only knows which vote has been cast, but not by whom. That does not diminish the necessity of investigating possibilities for prevention. The greatest concern, however, is the possibility of someone inside the polling station finding out who casts the vote. The question is if, with whichever advanced technical means, it is possible to capture radiation within the polling station without somebody noticing. This is now being investigated." [20, p. 7, translation by the author]

The first step in the construction of the 5 metre norm is the drawing of a distinction between outside and inside of the polling station. In the above statement, the radiation *inside* the polling station is seen as the most dangerous. However, now that this distinction has been mobilised as a member of the tempest issue, it can also be used differently:

> "The radiation range of the Sdu machines is 40 metres. With relatively simple equipment, the voting behaviour can even be read from the screen of the voting machine within this distance. The radiation range of the three Nedap machines that have been tested is approximately five metres at maximum, the dimension of a polling station itself. [...] The radiation, however, does not only concern the diacritics, but is also about the intensity of the radiation and the equipment necessary for capturing the signal. Weak radiation can indeed be captured by advanced equipment within a distance of five metres, but this implies that one would have to stay in the polling station with this equipment for a longer period. Such behaviour will draw attention in a polling station, and will be acted against. A 100 % guarantee can not be given though. The actions and measures taken must be seen within the proportions of the reliability that can be offered." [21, p. 5, translation by the author]

In this more recent comment of the minister, the inside/outside distinction has been translated into a radiation range. From a technical point of view, this is understandable, since this is more amenable to standardised measurement, using the devices the intelligence agency possesses. Note, however, that the distance of 5 metres is introduced here as the *actual radiation range of the Nedap machines.* This range is thus descriptive rather than normative. Also note that, as opposed to the earlier statement, the problem of capturing *outside* the polling station is now considered the most important one, because this is less likely to draw attention. In the earlier statement, capturing *inside* the polling station was considered more dangerous. This may be a reversal in the problem perception based on what can be physically measured: a maximum range can be tested against, but a minimum range ("only outside the polling station") does not make sense from what physicists know about radiation. Here, a new alliance forms between the radiation expertise of the intelligence agency and the political formulation of the problem. This formulation of the problem is reconfirmed in a later statement by the minister:

> "As I said before in parliament, there remains as a residual risk the possibility that radiation from the machine can be captured and the display reproduced within a range of maximum 5 metres. This, however, requires very advanced devices. As I stated in the AO [discussion with parliament] of 31 October 2006, I hold the opinion that this residual risk is acceptable." [17, p. 1, translation by the author]

In this statement, the beginning can be noticed of a transformation of the descriptive range into a normative range. Especially noteworthy is the role of the term "maximum". Although used in a descriptive sense before (the maximum range that was measured), this concept clearly has a normative connotation, and this may have invited the transformation into a norm (the maximum range that is acceptable). There is now agreement on the acceptability of radiation within a range of 5 metres, whatever that may mean exactly for the measuring equipment of the intelligence agency, and this political agreement is convenient for future government action: if one sticks to the 5 metre norm, the acceptability does not need to be renegotiated. This norm had major consequences for the outcome of the discussion, as we will see next.

3.3 The association of impossibility

After all the problems had revealed themselves, it was up to the Election Process Advisory Commission to propose a new way of voting that would (at least partly) solve them. Concerning the tempest problem, the report of the Election Process Advisory Commission considers the following:

> "It might be wondered how great the need is to protect voting equipment against compromising TEMPEST radiation. There are both matters of principle and pragmatic aspects here. The rules and regulations require the secrecy of the ballot to be protected. The question, however, is: how great is the risk of the compromising radiation emitted by

> the voting equipment being misused? Sophisticated TEMPEST expertise is currently well protected, but a motivated, technically knowledgeable amateur can go a long way. Ignoring the phenomenon is not an option, especially now that the subject is commanding wide attention. It is not desirable, for example, for the political leanings of Dutch celebrities to be published on the web. Theoretically it is even conceivable that real-time election results could be obtained on election day and published on the Internet. This, however, would involve eavesdropping on the ballots in at least enough polling stations for the results to be representative of the totality, and it is highly doubtful whether anyone would be willing to go to that much expense and trouble." [4, p. 34]

The Commission did not seem to be convinced that the problem really needed (technical) solving in general, but given the attention that the topic received, it could not be ignored: the risk of misuse had increased by the widespread coverage of the issue. The Commission recommended reactive measures, and was doubtful about the feasibility of preventive ones:

> "The Commission recommends that reactive measures be taken, by making such practice a criminal offence and reaching clearly defined agreements with the Public Prosecution Service on investigation and prosecution. If the additional cost of protection against compromising radiation is not prohibitive, the current NATO SDIP-27 Level B standard should also be applied." [4, p. 35]

The NATO norm, however, is confidential, which conflicts with the demand for transparency in the election process. This created a new problem hindering simple technical measures. Still, the Electoral Council (Kiesraad) strongly advised against solving the tempest issue by legal measures only:

> "From the point of view of the Electoral Council, safeguarding the secrecy of the ballot should be a self-evident topic in this accreditation procedure. This guarantee is incorporated in various international treaties and in the Dutch Constitution. This means that potential problems with radiation found in the ballot printer (the TEMPEST issue) cannot only be dealt with repressively by making eavesdropping an offence. For this problem a preventive solution should be sought, protecting the secrecy of the ballot to the greatest possible extent. It appears to the Electoral Council that minimally, a norm should be enforced according to which radiation is not allowed to reach further than a few metres from the device." [14, translation by the author]

This led the government and the new expert group to give an assignment to the German company GBS to draw up a public norm for radiation in electronic voting machines. This resulted in the document mentioned earlier [15]. In the report by GBS, the 5 metre norm finally materialises in a physically meaningful form: 5 metres means 5 metres with an antenna aperture of 1 square metre

[15, p. 6]. The physical relation between antenna aperture and possibility of capture seems to be more or less randomly chosen: one could also have said 0.5 square metre, as long as it could be justified that anyone with a larger antenna inside a polling station would draw attention. However, if one gets closer to the voting machine, the signal may be captured by a smaller antenna. It is thus assumed that smaller antenna sizes closer to the machine are also infeasible for the eavesdropper.

The document also provides procedures for testing and re-testing. Two types of measurement are defined: an accreditation measurement (for a type of machine) and a compliance measurement (for each machine). The accreditation measurement would take 4 hours, the compliance measurement 25 minutes. It is calculated that with normal working hours in a single lab, the compliance testing of the 10,000 machines necessary to cover all of the Netherlands would take 50 weeks. The compliance measurement needs to be repeated every two years. It is noted that transport and wear and tear can change the tempest properties of the machines.

For the test, it would be required to run test software on the machines, maximising the possible radiation during the test. The rationale behind this may be that emulating real voting during the tests would lead to strong fluctuations in radiation depending on the state of the device. This would not lead to repeatable results. Thus, the specific software used for voting would *not* be included in the test. First of all, this means that special software techniques would not improve the measured tempest behaviour. Secondly, this means that the device should allow software different from the normal voting programme to be run, introducing a security risk.

The report by GBS also provided for requirements on polling stations, including:

- placement of the machine opposite the windows;
- no other technical equipment (mobile phones switched off);
- procedure for checking seals on the machines.

According to a member of the expert group, a prototype ballot printer satisfying the requirements was built as well, weighing over 100 kg, due to the heavy metal case [12].

Now it was the turn of the government and the Expert Group to respond to the contents of the report. As in most information security problems, a balance was sought between technical, organisational and legal measures. The Electoral Council had indicated clearly that organisational and legal measures only were not acceptable. The technical norms, though, would lead to high costs and heavyweight devices, and most importantly, a host of additional organisational measures, including test logistics and polling station design. These organisational burdens were not considered acceptable.

In response to the report, the Expert Group states the following:

> “In fact, the issue of compromising emanations demands a process such as exists in military circles, where all factors can be controlled.

> According to the Expert Group, this is not realistic for the election process, and not desirable either." [19, p. 2, translation by the author]

The fact that this report was even written already reinforced the perception that the issue should be resolved technically, which was also advised by the Electoral Council. Thus, a coalition had emerged supporting the idea that technical measures were necessary. At the same time, the report showed clearly that even if technically acceptable devices could be built, the testing procedure would be impractical. This initiated a second coalition, namely one that judged the tempest problem to be insolvable. As we have seen, this coalition came out as a winning one in the discussion.

Relaxing the technical tempest requirements was not an option either. Knowing that the activist group was closely following the developments – and would be prepared to demonstrate any possible attack – and that parliament would see no reason to abandon the firmly established 5 metre norm, the government could not afford to take any risks, and decided not to introduce the ballot printer. One might be tempted to analyse this as a capitulation to a public perception issue that had got out of hand. The tempest issue, however, was not only a matter of perceived security; because it had been revealed so clearly, the likelihood of people actually attempting to find out the vote of someone, especially celebrities, had increased considerably.

> "In case it would still be decided to introduce the ballot printer, discussion on this topic will remain, possibly undermining trust in the new voting method. The government considers this not desirable, and therefore decides not to introduce the ballot printer." [19, p. 2, translation by the author]

Thus, from the perspective of ANT, the prominence of the tempest issue in the Dutch debate can be explained in terms of shifting associations between humans, devices, distinctions, norms etc. Interestingly, the tempest issue has not been discussed much in other countries, and neither in the Dutch debate on Internet voting. In the major Belgian e-voting study, it is mentioned as a requirement, but without explanation or a realistic estimation of costs: "The embedded computer system is made resistant to tampering and is shielded to prevent advanced attacks, e.g., tempest and electromagnetic radiation." [3, p. 98]. This technical guideline is seen as an implementation of the requirement of "System integrity & Voter anonymity: the remote observation of an electronic voting machine may compromise the privacy of the voter. Shielding the embedded computer system so that such information cannot easily be derived from side channels (e.g., electromagnetic radiation and power consumption) improves the trustworthiness in the eVoting system." [3, pp. 98–99] Note that any practical considerations regarding residual risk and measurement are omitted.

As Internet voting is performed on electronic equipment as well, it is potentially affected by the same threats. Still, the Dutch debate on Internet voting did not include tempest. We will come back to this curiosity in the next section.

The lesson to be learnt here is that perceived security is not an innocent naiveté of the public towards security issues. Rather, the entire battleground of attackers and defenders in a society can be changed by relatively minor details happening in the domain of perceived security and the forming of associations between different types of people and things. In such a case, the political options for the government may be extremely limited.

4 Risk analysis

Considering this – from a scientific point of view – rather disappointing conclusion, what can science do to contribute to the discussion on voting and tempest? Probably the best option is to widen the blinkers of the risk assessment a bit, enabling governments to make well-founded decisions in case the tempest discussion spreads to other countries. The question to ask, then, is of what type of risk in voting tempest is an instance, and how it compares to other instances of the same class.

There are similar threats to the secrecy of the ballot in voting systems. For example, what is the risk of attacks on the secrecy of the ballot by comparison of fingerprints with those on paper votes? In general, we can speak of *electoral traces* as a general term to denote physical, digital or social evidence of choices made by voters in elections. Physical evidence can be present in the form of fingerprints, recognisable handwriting, physical remainders in receipt printers, et cetera, Digital evidence can consist of compromising radiations, images in computer or printer memory, or cookies in case of Internet voting. Social evidence may be related to voter behaviour, exit polls.

Definition 1. *An* electoral trace *is a piece of information (partly) revealing the connection between voter and vote.*

Electoral traces can appear in various ways:

1. The vote is marked such that it can be traced back to the voter;
2. The voter is marked such that she can be traced back to the vote;
3. A different medium is used to emit or store the relation between voter and vote.

Examples of the first category are fingerprints on paper ballots or electronic storage of votes in sequential order. An example of the second category is a receipt that carries a proof of the voter's choice. Tempest constitutes an example of the third category. Other examples of electoral traces include the following: markings on ballots, fingerprints on keys/touchscreen, camera recordings, proxy voting. In the British system, a registration is kept of the relation between voters and ballot numbers, which also constitutes a vote trace. An interesting overview of additional privacy risks is found in [13]. Apart from the traditional risk attributes of probability and effect, electoral traces can be characterised along a number of dimensions:

Added value Benefits of the system causing the electoral traces. The British system allows for easier corrections in case of fraud. The US elections are much more complicated than the Dutch, so there will be a higher added value of voting electronically. In Internet voting, some traces may be allowed to increase verifiability;

Context Likelihood of the electoral trace being exploited given the social context. In the Dutch context, the tempest issue had become riskier due to media coverage;

Domain Digital, physical, social;

Effort Effort required to reconstruct vote-voter relation from trace (e.g. breaking weak crypto, matching paper ballot numbers with their registration in the British system);

Information content Amount of information that the trace reveals about the vote. The tempest attack due to the special character only revealed whether the voter voted for a specific party or not;

Intentionality Unintentional electoral traces are related to the secrecy of the ballot, intentional electoral traces are related to the freedom of the vote. Intentional traces may include video recordings of casting the vote or markings to make a ballot recognisable;

Overtness Overt (designed communication) vs. covert (not designed channel) [13];

Persistence Transitory (e.g. tempest) vs. long-lasting (e.g. fingerprints).

In each case where the risk of electoral traces is considered, a comparison should be made of the various traces that are possible and their properties along the mentioned dimensions, leading to a balanced view on their relative importance. In this way, the alliance of entities focusing on a particular type of trace can be placed in a wider context, such that appropriate measures can be taken not only for the risk that has the public's attention, but for similar risks as well.

We can now understand why tempest has not been considered important for Internet voting. Other electoral traces are already present in this voting method, e.g. the verification option in the RIES Internet voting system (digital, intentional, long-lasting) and shoulder surfing (social, unintentional/intentional, transitory), making the tempest issue relatively low-risk. If one allows people to check for which candidate their vote has been counted, this may constitute a high-risk electoral trace. Still, prominence of the tempest issue in the discussion on voting machines was harmful for the Internet voting efforts in a different way. The tempest issue put the requirement of the secret ballot high on the agenda, and because of the inherent secrecy problems in remote voting, this may have worsened the perspectives for success of the Internet voting effort of the water boards.

Still, the tempest discussion and the associated awareness of the secret ballot has not led to major discussion on the future of proxy voting in the Netherlands, which also has problems with the secrecy of the ballot in terms of social electoral traces. The risks of this feature of the Dutch electoral system have apparently been well-hidden, and there was no association of actors that was strong enough to put this back on the agenda.

Comparing different electoral traces thus leads to a more balanced view on voting system issues related to the secrecy of the ballot. Only if different dimensions of electoral traces are identified for each possible electoral trace in a voting system can electoral traces be subject to a more rational analysis and comparison, and can the Dutch tempest discussion be placed in a context fruitful to other countries. Other case studies of electoral traces may provide additional dimensions for the framework presented here.

5 Combatting vote traces

Given the framework provided in the previous section, how can we counter the threats of electoral traces in elections? Based on the estimated importance of the risks, several countermeasures can be proposed. We will first give some suggestions with respect to the tempest issue, based on the discussion in the Netherlands, and then broaden the view to other electoral traces.

The tempest issue arises from the *simultaneity* of the casting of the vote and the electronic processing thereof. Only in that case is it possible to derive the relation between voter and vote from the signal. Therefore, the following types of e-voting are affected by the tempest issue: DRE, precinct-count optical scan (where the voter enters the ballot into the counter), and Internet voting. Central-count optical scan, where e-counting starts after the close of the polls, is not affected, because there is no simultaneity of the casting and electronic processing of the vote.

For all the affected types, the tempest risk needs to be compared to other threats of electoral traces. An assessment should be performed in which it is made clear how much higher the risk of a breach of the secrecy of the ballot will be in case the particular e-voting system is used. Several technical measures can help to reduce this risk: the type of screen, the type of printer, shielding of the machine and cables, software measures (e.g. randomised display), and jamming stations (if legally allowed).

Technical measures need to be applied in combination with some form of certification. Certification requires a) a norm and b) testing procedures. To guarantee tempest behaviour, each individual machine should be tested, but governments may want to relax this requirement because of organisational burdens. In that case, the type of machine is tested and the government accepts the risk of individual machines not conforming to the norm. A decision should be made on whether a secret norm is acceptable, both for the public and for the manufacturers. As we have seen, the question should also be asked whether a norm should only address hardware requirements or also software. This may have major consequences for the testing procedure.

Next to or instead of technical measures, organisational and legal measures may be applied to reduce the risk of breaches of the secrecy of the ballot through tempest:

- physical requirements for polling stations (e.g. size of the room, placement of the voting machine);

- organisational requirements for polling stations (measures to prevent people from capturing signals both inside and outside the polling station);
- (criminal) law.

It is not possible to combat electoral traces only by addressing the tempest problem. As we have seen in the section on risk analysis, similar risks may appear, and in their presence expensive tempest measures may not achieve their goal. Risks associated with other electoral traces need to be compared to the tempest risk, and an integrated approach to managing these risks should be applied, based on this comparison. Especially in the situation where people carry all kinds of devices capable of recording the environment, high-risk traces may appear. Additional technical measures to combat vote traces may include:

- use e-voting in order to prevent markings on ballots, both unintentional (fingerprints) and intentional (text, symbol, fold);
- use a pen for the touchscreen instead of fingers;
- use printers that do not keep traces of what was printed and when (memory usage, physical traces in print technology, "yellow dots");
- use "privacy folders" to protect machine-readable ballots carried by voters from eavesdropping [13].

Again, certification may be necessary for more complex technical issues, such as the printer requirements. Organisational measures may include:

- disallow electronic equipment in voting booth to prevent intentional traces like video recordings;
- limit proxy and remote voting to prevent social traces;
- in Internet voting, only allow voters to verify *that* their vote has been counted, not how, such that voters will not have proof of their vote (receipt-freeness [2]);
- separate ballots for different races, to prevent using unique combinations to prove one's vote [13].

These measures may reduce the risk of several vote traces, but they may not be able to completely eliminate them. It remains to be seen whether a combination of such measures is sufficient to restore trust in the secrecy of the ballot in the age of electronics. As we have seen in the Dutch situation, the problems may not even be regarded solvable in practice. This may hold both for problems induced by the automation of the voting process and for problems induced by the increasing number of recording devices carried by voters.

6 Conclusions

In this paper, we analysed the Dutch tempest issue in the e-voting controversy. We gave an actor-network account of the emergence of both the tempest problem and the associated 5 metre norm. To place the discussion within a broader framework and allow for risk analysis, we introduced the notion of electoral traces, of which the tempest issue is an instance. We used our risk analysis guidelines to explain why the tempest issue did not come up in the discussion on Internet voting in the Netherlands. Based on the Dutch situation and the analysis thereof, some recommendations were given on which topics to consider in similar discussions elsewhere.

As far as we are aware, this paper is the first to give a systematic account of the Dutch tempest discussion. It remains to be seen whether the discussion on electoral traces and tempest emerges in other countries, but if it does, the framework devised here may be helpful in guiding the scientific and political analysis. Otherwise, it is just a scientific contribution, both on the social dynamics of risks of information technology and on risk assessment of electronic voting systems.

References

1. Adviesommissie Inrichting Verkiezingsproces. Stemmen met vertrouwen, September 2007. Available online: `http://www.minbzk.nl/contents/pages/89927/advies.pdf`, consulted November 3, 2007.
2. J.C. Benaloh and D. Tuinstra. Receipt-free secret ballot elections (extended abstract). In *Proc. 26th ACM Symposium on the Theory of Computing (STOC)*, pages 544–553. ACM, 1994.
3. BeVoting. Study of electronic voting systems, part i of the studie geautomatiseerde stemming def. vs 18122006, version 1.1. `http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections/fr/presentation/bevoting-1_gb.pdf`, 15 April 2007.
4. Election Process Advisory Commission. Voting with confidence. `http://www.kiesraad.nl/nl/Overige_Content/Bestanden/pdf_thema/Voting_with_confidence.pdf`, 27 September 2007.
5. Commission on Electronic Voting. First report of the commission on electronic voting on the secrecy, accuracy and testing of the chosen electronic voting system. `http://www.cev.ie/htm/report/first_report.htm`, 2004.
6. Het Expertise Centrum, consultants voor overheidsinformatisering. Definitierapport kiezen op afstand, 15 September 2000.
7. B. Fairweather and S. Rogerson. Technical options report, 2002. Available online: `http://www.communities.gov.uk/documents/localgovernment/pdf/155484.pdf`, consulted March 24, 2009.
8. B. Gedrojc, M. Hueck, H. Hoogstraten, M. Koek, and S. Resink. Rapportage advisering toelaatbaarheid internetstemvoorziening waterschappen. Fox-IT, `http://www.verkeerenwaterstaat.nl/Images/20081302%20Bijlage%201%20Rapport_tcm195-228336.pdf`, 12 August 2008.
9. R. Gonggrijp, W.-J. Hengeveld, A. Bogk, D. Engling, H. Mehnert, F. Rieger, P. Scheffers, and B. Wels. Nedap/Groenendaal ES3B voting computer: a security analysis, October 6 2006. Availabe online: `http://www.wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf`, consulted March 16, 2007.
10. L.M.L.H.A. Hermans and M.J.W. van Twist. Stemmachines: een verweesd dossier. rapport van de commissie besluitvorming stemmachines, April 2007. Available online: `http://www.minbzk.nl/contents/pages/86914/rapportstemmachineseenverweesddossier.pdf`, consulted April 19, 2007.

11. E. Hubbers, B. Jacobs, and W. Pieters. RIES – Internet voting in action. In R. Bilof, editor, *Proc. 29th Annual International Computer Software and Applications Conference, COMPSAC'05*, pages 417–424. IEEE Computer Society, July 2005.
12. B.P.F. Jacobs. Practical issues in electronic voting. Slides of FOSAD summer school presentation, `http://www.cs.ru.nl/B.Jacobs/TALKS/fosad08.pdf`, 30 August 2008.
13. A.M. Keller, D. Mertz, J.L. Hall, and A. Urken. Privacy issues in an electronic voting machine. In K.J. Strandburg and D. Stan Raicu, editors, *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, pages 313–334. Springer, 2006.
14. Kiesraad. Reactie op rapport 'stemmen met vertrouwen' over inrichting verkiezingsproces (commissie-korthals altes). Kiesraad advice 2007-0000406046, `http://www.kiesraad.nl/nl/Overige_Content/Bestanden/Advies-Adviezen/reactie_15_okt_2007.pdf`, 15 October 2007.
15. M. Kuhn, G. Friedrichs, A. Aksoy, E. Koch, and L. Friedrichs. Tempest specificaties en testmethoden voor elektronische stemapparatuur. Appendix BLG15766 of Kamerstuk 2007-2008, 31200 VII, nr. 64, Tweede Kamer, 21 May 2008.
16. B. Latour. *Reassembling the social: an introduction to actor-network theory*. Oxford University Press, Oxford, 2005.
17. Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties. Vaststelling van de begrotingsstaten van het ministerie van binnenlandse zaken en koninkrijksrelaties (vii) voor het jaar 2007; brief minister over stemmachines. Kamerstuk 2006-2007 30800 VII, nr. 13, Tweede Kamer, 3 November 2006.
18. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Project kiezen op afstand. report BPR2004/U79957, November 11 2004. Available online: `http://www.minbzk.nl/onderwerpen/grondwet-en/verkiezingen-en/kiezen-op-afstand/kamerstukken?ActItmIdt=12800`, consulted March 13, 2007.
19. Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties. Vaststelling van de begrotingsstaten van het ministerie van binnenlandse zaken en koninkrijksrelaties (vii) voor het jaar 2008; brief staatssecretaris met oordeel kabinet over uitkomsten nader onderzoek naar haalbaarheid stemprinter en stemmenteller. Kamerstuk 2007-2008 31200 VII, nr. 64, Tweede Kamer, 21 May 2008.
20. Vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties. Vaststelling van de begrotingsstaten van het ministerie van binnenlandse zaken en koninkrijksrelaties (vii) voor het jaar 2007; verslag algemeen overleg van 12 oktober 2006 over beveiliging van stemmachines. Kamerstuk 2006-2007 30800 VII, nr. 18, Tweede Kamer, 28 November 2006.
21. Vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties. Vaststelling van de begrotingsstaten van het ministerie van binnenlandse zaken en koninkrijksrelaties (vii) voor het jaar 2007; verslag algemeen overleg van 31 oktober over stemmachines. Kamerstuk 2006-2007 30800 VII, nr. 19, Tweede Kamer, 28 November 2006.