Reve{a,i}ling the risks:
a phenomenology of information security

Wolter Pieters

University of Twente

Originally submitted version. Accepted for publication in Techné.

Abstract:

In information security research, perceived security usually has a negative meaning, when it is used in contrast to actual security. From a phenomenological perspective, however, perceived security is all we have. In this paper, we develop a phenomenological account of information security, where we distinguish between revealed and reveiled security instead. Linking these notions with the concepts of confidence and trust, we are able to give a phenomenological explanation of the electronic voting controversy in the Netherlands.

Keywords: electronic voting, information security, phenomenology, risk, trust

Acknowledgements:

The research described here was partly performed while the author was employed at the Radboud University Nijmegen and supported by a Pionier grant from NWO, the Netherlands Organisation for Scientific Research. This text is based on parts of the author's PhD thesis (Pieters, 2008). The author wishes to thank (in alphabetical order) Luca Consoli and Sanne van der Ven for useful comments on drafts of this paper.

Introduction

Information security is an increasingly important area of research. More and more sensitive data is entered into information systems, such as votes, health records and travel behaviour of electronic public transport cards as well as cars. In many countries, controversies exist on the security of such systems. Whereas manufacturers claim that their systems are secure, hackers seem to find all kinds of vulnerabilities, and scientists and politicians either support the manufacturers or the hackers. The question we ask here is how such dynamics can be analysed from a philosophical perspective.

There is some agreement in the analysis of information security about the need for covering both technical and social aspects of security (Evans and Paul, 2004; Nikander and Karvonen, 2001; Oostveen and Van den Besselaar, 2004; Riedl, 2004; Xenakis and Macintosh, 2005). The social aspects are often labelled "trust". It is then said that trust is based on "perceived security", rather than "actual security". The reasoning can be summarised as follows. "Actual security" can be assessed by technical experts, and "perceived security" is a more or less distorted version of this in the mind of a member of the non-technical community. From this point of view, trust is based on "perceived security", as opposed to "actual security". It can easily be determined to be either justified or unjustified depending on the agreement between the perceived and actual security of the system.[1]

Such a view appears to be intuitive, and provides for business a clear division of responsibilities between the technical department and the marketing department: the technical department is responsible for actual security, the marketing department for perceived security. However, it is not satisfactory in scientific analysis of security controversies. The distinction between actual and perceived risk has been subject to criticism in the literature, because there is no method to separate actual risks from perceived risks (Jasanoff, 1998; Hansson, 2004; 2005). This is in line with other results in philosophy of science, which argue that facts are constructions rather than states of the world independent of experience. Risk, instead, should be seen as constructed. Since security can be thought of as absence of certain types of risk, the same holds for security. The precise meaning of "construction" can vary according to the philosophical perspective taken.

This article provides an alternative vocabulary for discussing information security controversies from the point of view that risks are emergent from the relation between humans and the environment, which is a phenomenological perspective. We will make use of terminology from Luhmann's system theory as well.[2] The controversy on electronic voting, especially in the Netherlands, will serve as running example.

First of all, the controversy on electronic voting is introduced, as well as its problematic explanation in terms of actual security and perceived security. We will then argue that an alternative explanation should take into account that risks are always *selected*. Then, we will introduce the philosophical concept of "entbergen" due to Heidegger. Using this concept, we will argue that selection involves “revealing” risks, but that this means at the same time a “reveiling” of other risks. Drawing further upon the work of Heidegger, we will try to distil the specific way in which these risks are dealt with from a cultural perspective, and what this means for information security and electronic voting in particular. This will lead us to conclusions on the use of the phenomenological terminology in the context of risk.

Electronic voting

In the Netherlands, electronic voting (e-voting) machines have been introduced in the election process since the early nineties, without much discussion about their security. It was not regarded a serious problem that the design was secret, and only the independent voting system licenser TNO knew the details. Most of the concern was about whether all citizens would be able to operate the machines. After their introduction and the implementation of requirements in the law, the system became a background phenomenon in which people had confidence. Only in 2006, controversy emerged about the security of the machines, after the same thing happening in many other countries earlier. By that time, paper voting had become the exception.

The Dutch debate was due to a group of people launching a campaign against the use of the machines. The anti-e-voting pressure group was set up after the founders experienced e-voting for the first time themselves, in Amsterdam. These people argued that “unverifiable” voting systems should be abandoned, which they thought applied to all e-voting systems. They managed to get hold of a couple of voting machines, and took them apart, demonstrating security problems both with the correctness of the results and the secrecy of the vote (Gonggrijp et al., 2006). The demonstration included replacing the counting program with a fraudulent one, and eavesdropping on the voter’s choice by means of radio signals. This initiated major attention of the media and the government. Eventually, the pressure group succeeded in making electronic voting machines disappear from the Dutch scene.

The e-voting controversy has been analysed in terms of actual and perceived security. It is then usually taken to mean that in paper voting, actual security can easily be observed, whereas it cannot in electronic voting. Hans Geser (2004) finds that in traditional systems, “all the documents and devices which could potentially be subject to manipulation (voter registries, voting papers, ballot urns, handwritten signatures, etc.) exist in physical form, which makes them amenable to objective visibility and unimpeded examination." (p. 91) Xenakis and Macintosh (2005) argue that “[s]ince procedural security is evident and understandable to voters, it has a comparative advantage when it comes to developing and supporting the social acceptance for the new e-processes". In case of procedural security (measures requiring human intervention, as opposed to technical security), the actual security of the system can apparently be perceived by the voters, such that trust can easily be established and justified, because perceived and actual security coincide.[3] In case of electronic voting, it takes experts to show to the unknowing public the actual (in)security of the electronic systems, thereby invalidating the public’s trust in the systems, which was based on perceived security rather than actual security.

From this perspective, it is easy to explain why the Dutch anti-e-voting campaign was successful: they were right. The only thing they did was replacing perceived security with actual security, thereby demonstrating that paper voting is actually more secure than electronic voting. This explanation is not satisfactory from a philosophical point of view, though, because it assumes the actual security of both paper voting and electronic voting as a priori, rather than accounting for their construction. For why is paper “evident and understandable”? This is itself something that requires explanation. If anything, this is a matter of degree rather than a fundamental difference: paper is understandable because people have been educated in processing paper, and this education may be easier than education on the workings of computers (if scientists have figured this out at all). The introduction of what we now think of as “normal” paper voting raised major issues in the United Kingdom (Asquith, 1888; Park, 1931).

The problem with such an analysis, therefore, is that it does not account for why certain claims are acknowledged the status of facts (actual security) and others are not. Woolgar and Pawluch (1985) have termed the drawing of arbitrary boundaries between facts and claims “ontological gerrymandering”, analogous to the drawing of arbitrary boundaries between electoral districts to the advantage of the ruling party. According to these authors, there can be no such thing as objective underlying conditions if one wants to explain controversies, precisely because controversies question which claims deserve the status of fact.

Moreover, arguing that paper votes can be more easily perceived invalidates the argument that perceived security is something bad that should be banned from voting processes, and replaced with actual security. If there is a truth about voting, this actual security will certainly be known through perception, but perception is used as at the same time as a deceiving opposite of actuality. We want to perceive because then we can know, but if we know then we should not perceive. Is, consequently, perceived security something that should be replaced by actual security, or is perceived security precisely what we need?

Providing a deeper explanation of why the anti-e-voting campaign in the Netherlands was successful is therefore necessary, and will be the final goal of the phenomenological argument presented here.

Risk assessment as selection

In order to analyse information security from a philosophical point of view, we first need an understanding of what it is that information security experts study, and how this relates to the concept of risk. Information security is the field of research that deals with modelling the security properties and security risks of information systems. Security, as opposed to safety, describes measures to protect the system against *deliberate* attacks, not unintentional failures. Unintentional breakdown of computer systems is therefore not part of information security, but hacking is.

Typically, goals of security measures include confidentiality, integrity and availability of information. In order to study the protection of these properties by an information system, security experts need an *attacker model* that describes the capabilities of an enemy trying to disrupt the confidentiality, integrity or availability of information. The capabilities of the attacker correspond to potential risks that could affect the security of the system if it were not designed properly.

It has been shown many times that the attacker models of security experts can be incomplete. For example, a security protocol for electronic authentication was proven correct with respect to generally accepted security models, but an attack was found many years later (Lowe, 1996). The inherent limitation of security verification is widely recognised by computer scientists. One can never know what an attacker will be up to in the future, and one can never know whether confidentiality, integrity and availability cover all possible risks. Therefore, studying the security risks of information systems inherently involves more uncertainty than scientific knowledge in general. Instead of describing risk analysis in terms of measuring actual security, one should focus precisely on this uncertainty to understand security controversies. This can be achieved by addressing the problem of risk selection.

Risk, according to Niklas Luhmann ([1993] 2005, 21-22), is uncertainty in relation to future loss, attributable to a decision. Luhmann contrasts the concept with danger, which is not attributable to a decision. If a river floods once every ten years and this is accepted as a fact, it constitutes danger. If it floods after it was considered to build dikes, it constitutes risk. Which possible losses are included in a decision depends on the perspective of the decision maker. Luhmann thus frames the question on knowing the risks as a question of *selection*:

> “[Social science research] brings to the foreground the question of who or what decides whether (and within which material and temporal contexts) a risk is to be taken into account or not. The already familiar discussions on risk calculation, risk perception, risk assessment and risk acceptance are now joined by the issue of selecting the risks to be considered or ignored.” (p. 4)[4]

Rather than being a problem of representation, therefore, security assessment can be considered a problem of selection: selection of what needs to be protected and selection of how this can be threatened. Instead of representing security assessment as a way to measure actual security, we will ask the question how risks are *selected*. However, in order to avoid the pitfalls of the actual/perceived distinction, we should not think of this selection as a matter of picking something that is already there. Neither is it a purely social construction independent from the environment, for we may perceive losses even if we did not select the particular event as a risk. We therefore choose a phenomenological approach, which promises to give an account from the interrelation of humans and their environment. How can we describe this selection process from a phenomenological point of view?

Heidegger’s concept of “entbergen”

To provide a vocabulary to explain risk selection, a particular concept due to the German philosopher Martin Heidegger can be very useful. This section is necessarily only a sketch of the features of Heidegger’s thought that are relevant for the aim of this article: using a specific Heideggerian concept in a phenomenological approach to risk controversies. The use of Heideggerian terminology is thus pragmatic rather than orthodox.

As all phenomenologists, Martin Heidegger (1889 – 1976) took a specific position between realism and idealism: it is from the inevitable relation between the subject and the object (“Verklammerung”) that things appear to the human mind; there is no primacy for either the subject or the object. This means that there *is* an active part in perception, but the content is not determined by the subject completely. Rather, the subject must bring the beings into being by revealing them in a specific way. It is in this specific context that Heidegger introduces the concept of “entbergen” (Heidegger, 1982; Tijmes, 1992; Verbeek, 2005).

“Entbergen” means bringing something from concealment into unconcealment (“aus der Verborgenheit in die Unverborgenheit bringen”). It is a concept of truth (Greek: aletheia) that has something active in it. In English, it is usually translated as revealing. One of the most famous (and notorious) ways in which Heidegger uses the concept is in the analysis of technology. Heidegger sees the essence of technology as a specific way of revealing the world, namely as a set of resources (something that was ordered: “bestellt”, “herausgefordert”, a “Bestand”). This view on technology is now widely disputed and claimed to be too essentialist (Verbeek, 2005). Still, the fact that technology (and also specific technologies) makes us see the world in a particular way is generally recognised. The problem with Heidegger’s interpretation is that it seems to allow for one way of “entbergen” at a time. A more modest claim is that a cultural framework, including available technologies, invites revealing the world in a certain way. Such a weaker claim can be defended from both pragmatist and system theoretic points of view, which is beyond the scope of this paper.

At the same time that something is brought from concealment into unconcealment, something is also being “reveiled”. This intentional misspelling indicates that in the process of revealing, the process itself and the original concealment are being concealed. This connotation is also present in the original German term “entbergen”: “verbergen” means to hide. The human mind clings onto the things that have been revealed rather than the fact that these things came from concealment, and that other things are even more concealed after the act of revealing others.

Heidegger’s ideas have later been taken up by philosophers of technology (Ihde, 1990; Verbeek, 2005). Although these “postphenomenologists” have a far less radical view on the changing potential of technology, they acknowledge - more than Heidegger did - the mediating character of concrete technologies, from telescope to hotel key, in our experience and actions. The idea that aspects of reality can be amplified or reduced by technological means is a central theme within this movement. It is from this postphenomenological tradition that we polish up the concept of “entbergen” for use in the information age.

Reve{a/i}ling the risks

When discussing risk selection, we have to deal precisely with the intricacies of avoiding both the interpretation as selecting something that is already there and the interpretation as selecting something independently from the environment. We therefore argue that the process of selecting the risks can be understood as a process of “entbergen”. Risks are not purely socially constructed phenomena, but they do not represent an objective nature either. They are revealed from concealment, and the particular mode of “entbergen” determines which risks become visible (and how) and which do not.

This is not to say that there is only one way of “entbergen” possible given the technological constitution of our society, as Heidegger himself seemed to imply. It is precisely the history of things that have already been revealed, which is culture-specific (and even subculture-specific), that influences the characteristics of the process of “entbergen”. That which has already been revealed mediates the process of revealing other beings. It may both invite and inhibit the revealing of certain risks (cf. Verbeek, 2005).

Moreover, revealing certain risks hides the process of revealing, and thereby the risks that were not revealed. These risks can be said to be *reveiled* in the process of “entbergen”. Thus, when we have done a risk assessment, not only have we revealed certain risks, but the risks that we did not reveal may have been even more reveiled in concealment than they already were. On the other hand, revealing certain risks may also invite revealing other, similar, risks.

For example, if climate change has been revealed as a major risk of energy consumption, fossil fuels become less attractive, and biofuels may get into focus. At this point, because the climate change risk has been revealed, other risks may be reveiled and receive less attention. In such a context, it is no wonder that risks of biofuels, such as competition for soil with food supply, are overlooked at first.

In security, as opposed to safety, the process of revealing is not only mediated by security experts, but also by the intruders or attackers. The assessment of which features of a system are risks is a continuous process of “negotiation” between the attackers and the defenders. When an attacker reveals a risk, the reply by the defenders (a defence against the attack) makes the risk even more visible. It may also work the other way round: a risk that is revealed by a security expert may be even more revealed if it is exploited by an attacker.

For example, when we have revealed so-called buffer overflows as a major cause of security vulnerabilities in computer programs, other vulnerabilities may become more concealed. This is due to both attackers and security experts focusing on what has already been revealed (the buffer overflow vulnerability), trying to exploit and remedy this problem, respectively. On the other hand, risks that are similar to or instances of buffer overflows are more likely to be revealed once the buffer overflow has become common knowledge.

This yields a meaningful distinction between “perceived risk” and “non-perceived risk”, or “revealed risk” and “reveiled risk”, replacing the distinction between “actual risk” and “perceived risk”. Perceived risk is risk that has been revealed, and now takes on a positive meaning, as opposed to the negative meaning it has in relation to actual risk.

As argued above, different cultures may reveal risks in different ways. We can understand this from the perspective of the distinctions that are used in the culture to describe the world. Such distinctions or cultural categories are our means of dividing the world into different types of objects (Smits, 2002; 2006). Animals may be categorised as mammals, reptiles, birds, fish, et cetera. Information systems may be categorised as hardware and software, programs and data. Cultural categories may also exist for subcultures within a society, for example industry, academia and activists. The level of analysis will depend on the distinctions that we are interested in.

From the perspectives of different sets of cultural categories, a new technology may be categorised differently, and also the risks will be revealed differently. For example, the risks of genetic modification will be revealed differently from the perspective of human health than from the perspective of ecology. Sometimes this does not cause major problems when a new technology is introduced, but it may also lead to controversy. If we cannot agree on the relevant categories, we may have to adapt our categories to find a common way of revealing the risks.

Once agreement on the risks and countermeasures has been established, the risks of technology may be reveiled once more. Some risks that were revealed in the early controversy on a new technology have been taken care of, others have been forgotten, and may re-appear later. This process of reveiling brings things back from unconcealment into concealment, by “undoing” the process of revealing. Later, risks may be revealed again, for example in case of an incident or an active campaign against the technology, but they need not be the same anymore.

We argued that the existing distinction between “actual security" and “perceived security", on the latter of which trust is supposed to be based, is problematic. We can now rehabilitate the term perceived security. Security measures, implemented to protect against revealed risks, are reveiled together with the risks once agreement has been reached, and they become invisible. Also, when certain risks were never explicitly thought of but accidentally addressed by the design of the technology, there may be invisible security measures. We thus have “revealed security” and “reveiled security”, complementary to “revealed risk” and “reveiled risk”. Here, we have a more meaningful distinction than between “perceived security” and “actual security”. Risks and security measures that have been “forgotten” (both in the sense of never thought of and in the sense of thought of but not remembered) can re-appear in the future, and thus the concept of “reveiled security” can contribute to the analysis of controversies.

Risk assessment as ordering

According to Heidegger, modern society does not reveal things in a way that corresponds to the old Greek “technè”, which he sees as a form of “entbergen”. “Technè” was creating things in a craftsman’s way, things that do not appear by themselves. Instead, the modern technological society *orders* (“bestellt”) the world: it *forces* things to appear. The world is constituted as a set of resources. “Entbergen” has become a *forcing into unconcealment*.

Although this analysis can be rejected for being too abstract, massive and nostalgic (Verbeek, 2005), it offers some profitable insights in the use of risks in modern society. When applied to risk, the analysis states that modern society *forces the risks into unconcealment*. This seems to be quite an appropriate expression for what happens in risk assessment. We do not wait until something goes wrong; we want to know *beforehand* what can go wrong, how likely that is and how severe the consequences are.

“Ordering” means both asking for something and structuring the contents of it. In this way, “ordering” risks means both requiring the technology to show its risks and structuring these risks at the same time. Thus, “ordering” the risks is both ordering in the sense of asking for, and in the sense of structuring. The first meaning is expressed in the goals of risk assessment, namely forcing the risks into unconcealment; the second meaning is expressed in the way the result is presented: as a list of risks associated with probabilities and costs.

Thus, following Heidegger just far enough in his sceptical view on modern society, we see that modern society tends to reveal risks by “ordering” them. We find that risk assessment can be described as “ordering” the risks into unconcealment, by revealing them with “force”. This ordering is both a demand and a quest for structure. The ordering may hide the process of revealing and the original concealment, which leaves the scientist no other choice than to claim that she has found a “real” threat, which, in case of information security, is called actual security. Or, in more pragmatic terms, the scientist (or activist!) does not have the tools to describe her discovery in a different way. This may explain why the distinction between actual and perceived security is prevalent in analyses of information security controversies.

Confidence and trust

Thus far, we have achieved two main results. Firstly, based on the use of the concept of “entbergen”, we have rehabilitated the notion of perceived security. Perceived security should not be understood as opposed to actual security, but as opposed to non-perceived or reveiled security. Secondly, we have analysed how it can be explained that this approach is often overlooked, and why both activists and scientists demonstrate their findings in terms of actual security (and designate the previous, uninformed state as “perceived security”). We will now proceed to redefine a concept that was seen as derived from perceived security: the concept of trust.

Trust is a form of self-assurance. It entails reliance upon something else, and the belief that this other will not fail in meeting certain expectations. Technology is acceptable if we trust it to have limited unwanted effects. However, the grounds on which self-assurance is based can be quite different. In earlier work, I used Niklas Luhmann’s distinction between confidence and trust (Luhmann, 1988) to disentangle the discussion on the relations between security and trust (Pieters, 2006).

Confidence, following Luhmann, is taken to mean self-assurance of the safety or security of a system without knowing the risks or considering alternatives. Trust means self-assurance by assessment of risks and alternatives. A technology can be said to be *reliable* if it is suitable for acquiring confidence. It can be said to be *trustworthy* if it is suitable for acquiring trust. A technology that operates successfully may acquire confidence, but it may become problematic when subjected to comparative analysis, and therefore fail to acquire trust. In information security, a proprietary security mechanism - such as in the Mifare classic chipcard - may acquire confidence, but since it cannot be publicly analysed, it may not be trustworthy.

We can now be more precise about the relation between confidence and trust. “Ordering” the risks denotes a transition from confidence to trust. Trust in this setting means self-assurance based on knowledge (i.e. unconcealment) of risks and alternatives; confidence means self-assurance without such knowledge. By forcing the risks into unconcealment, one can exchange confidence (or a lack thereof) for (dis)trust. However, this also means that the concealment, the process of revealing *and thereby the original confidence* are hidden.[5] Rather than a replacement of perceived security with actual security, what often happens in a controversy is a replacement of confidence with trust or distrust: more risks are being revealed, and decisions between alternatives are taken accordingly.

Electronic voting revisited

Provided with the conceptual tools developed in the previous sections, we now turn our attention to a phenomenological analysis of the electronic voting controversy in the Netherlands.

In the Netherlands, the paper voting system had effectively reveiled the risks of proxy voting (voting by authorising someone else). Ten to twenty percent of the votes cast in an election are typically cast by someone else than the voter. The risk of vote buying or coercion, and the accompanying security measure of the voting booth, had apparently been reveiled. Only after the OSCE revealed this risk again, discussion re-emerged (OSCE Office for Democratic Institutions and Human Rights, 2007a). Once buying and coercion have disappeared as a profound risk in elections, partly due to security measures, they can be “forgotten" in the introduction of a new technology, such as Internet voting, where a voting booth is not possible. In the Netherlands, they seem to have been revealed again, whereas in the UK, they are not so much seen as substantial risks (Pieters and Van Haren, 2007). Apart from this problem, most risks of paper voting remained reveiled for a long time.

Because of its short history, agreement on the risks of e-voting is far less strong. The risks of e-voting, therefore, can only be a reveiled by now if they are able to hide within the existing system. This has happened in the Netherlands. Security measures that were reveiled in the paper system, e.g. in terms of verifiability, continued to be hidden when the transformation towards e-voting took place. The possibility of a recount completely changed in e-voting compared to paper voting, but this security measure remained reveiled, together with the risk it was meant to address – discussion about the count. When risks are revealed anew, which the pressure group encouraged, the notion of verifiability may be associated with major risks in e-voting.

Many security measures in the paper voting system have been reveiled by now (why a voting booth, why recounts, why paper in the first place), together with the risks in elections that made them appear. This explains why the paper voting system appears as less risky than new electronic systems. Paper voting does not appear as less risky because it is actually more secure, but because the risks and security measures have been reveiled. This, however, may also mean that risks are overlooked when e-voting is first implemented. E-voting, until 2006, was able to rely on the reveiled security of the paper voting system. However, the activist group made sure that this was no longer possible. They “ordered” the risks.

Following the line of argument set out in this text, the most important reason for the smooth introduction was that the electronic systems were not seen as *alternatives* to the existing procedures, but rather as automated versions of existing procedures. This made it easy to transfer confidence from paper voting to the new systems, without revealing new risks.

After the introduction, the public became sensitive to computer security issues due to media coverage of Internet security problems such as viruses and worms. This revealed new categories of risks in computer systems, which led to revealing new risks of voting systems as well. Accordingly, opposition to electronic voting ensued in countries such as the United States and Ireland. In the Netherlands, some criticism appeared, but the scene remained relatively silent, possibly due to soothing remarks by the highly trusted Dutch government. After 2006, however, the pressure group created in their arguments a clear distinction between paper voting on the one hand and electronic voting on the other: they were said to be fundamentally different.

If electronic voting is seen as a really different alternative to paper voting, which the pressure group encouraged, people suddenly get the option to *decide* on a voting system. This invites actively revealing the risks of the different systems, and basing the decision on an analysis of these risks. This means that *trust* now becomes the dominant form of assurance, as opposed to confidence. This has as a consequence that voting systems are required to be *trustworthy* rather than reliable only.

By making the distinction between paper voting and e-voting, the pressure group thus created a set of alternatives, requiring a decision, and changing the expectations from reliability to trustworthiness. This, again, led to the traditional paper system becoming *more* attractive, because it is based on human procedures. Human procedures more easily acquire trust than automated procedures, for humans generally have more experience with and knowledge of the former. On the other hand, if the new technologies are not seen as an alternative, but as an improvement of existing procedures, electronic devices are more attractive, because they are more reliable and thus more easily acquire confidence. The risks are then reveiled.

The two main (new) risks that the pressure group revealed in their media offensive were the ease of replacing the chips with counting software, and radiation leaking information about the voter’s choice. Apparently these were not problems that were addressed by the testing criteria of the law: they had been reveiled in the original discussion. This can be explained by a focus both on verification of the *design* by testing authorities rather than verification of *results* by election observers, and on secrecy of the ballot in *storing* the voter’s choice rather than in *casting* the vote. Why this particular revealing took place at the time is an interesting empirical question from the phenomenological perspective sketched here.

After the demonstrations of the pressure group, the only thing in the law to build upon was the demand of the secret ballot, which was apparently violated by the radiation problem. The Minister decertified about 10% of the machines for this reason: not because of failure to meet the criteria laid down in lower legislation, but because of possible problems with the orderly conduct of the elections. Therefore, the selection of this risk now makes it impossible to introduce voting machines in the Netherlands that do not meet radiation requirements, effectively banning electronic voting from the country. In other jurisdictions, the radiation issue has not been revealed as a major risk.

Meanwhile, the original problem the campaign tried to address, the lack of verifiability, had been reveiled by the focus of the Ministry and the media on the radiation risk. The pressure group had a hard time getting this back on the agenda. The campaign people had “ordered” the risks, but what they got was not exactly what they asked for, because they revealed particular risks in a particular way, thereby inviting the revealing by others of similar risks (the government had the intelligence service look into the radiation problem, causing more revealing on this topic), and reveiling their basic argument. Meanwhile, by making paper voting and electronic voting distinguished alternatives, they transformed the original confidence, based on the concealment of risks, into distrust. We now want trust in e-voting systems, not just confidence. This also put an end to the experiment with Internet voting: because of the risks revealed, not only the particular Internet voting in place showed some deficiencies, but probably any Internet voting system would have been deemed too risky.

Conclusions

In this paper, we used Heidegger’s notion of “entbergen” to explain how risks of technological systems are revealed and reveiled in risk controversies. Our point of departure was the assumption that risks are neither purely objective nor purely subjective. Based on the use of phenomenological terminology, we discussed how risk controversies can be understood in terms of the revealing and reveiling of risks and security measures, rather than in terms of actual and perceived security. We linked these concepts to the distinction between confidence and trust and analysed the Dutch e-voting controversy from this perspective.

In general, risks and security measures of paper voting will be reveiled by the time electronic voting is proposed. Which risks will be revealed will determine which security measures are put in place in e-voting. If the voting system functions properly, people will have confidence in it without exactly knowing how it works or considering alternatives. When problems arise and e-voting and paper voting are compared as alternatives based on risk assessment, risks are revealed (again) and trust (or distrust!) takes the place of confidence. Such dynamics of reveiling and revealing can be analysed in similar controversies as well.

One of the main benefits of our analysis is a better understanding of the relation between the revealing of certain risks and the concealing (reveiling) of others. This is hard to account for in a representational view of risk assessment. Moreover, the concept of “entbergen” can be used as a clarification of the distinction between confidence and trust proposed earlier.

Apart from information security, the terminology developed may also apply to other risk-related areas. For example, environmental risks may be revealed differently when the focus is on climate change than when the focus is on acid rain. Again, the media play an important part in the dynamics of revealing and reveiling. Also, if risks are revealed as described in this article, drawing up laws and requirements for technological systems is part of the process of revealing and reveiling risks. This means that the law, in the end, will reflect the process of revealing, which can be an interesting area for further (empirical) research.

Instead of contrasting the concepts of actual and perceived security in risk controversies, we should emphasize the distinction between revealed and reveiled security. This allows for a much richer analysis of the dynamics of the debates. The main disadvantage seems to be the essentialist connotation that Heideggerian terms mostly have. We hope we have made clear that we do not share such a view, but we understand that it must be revealed as a risk of this approach.

References

Alvarez, R.M. and Hall, T.E. 2004. Point, click & vote: the future of Internet voting, Washington, DC: Brookings Institution Press.

Asquith, H.H. 1888. “The Ballot in England,” Political Science Quarterly, 3(4): 654-681.

Gonggrijp, R., Hengeveld, W.-J., Bogk, A., Engling, D., Mehnert, H., Rieger, F., Scheffers, P. and Wels, B. 2006. Nedap/Groenendaal ES3B voting computer: a security analysis. Available online: http://www.wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf, consulted March 16, 2007.

Hansson, S.O. 2004. “Philosophical perspectives on risk,” Techné, 8(1): 10-35.

Hansson, S.O. 2005. “The epistemology of technological risk,” Techné, 9(2): 68-80.

Heidegger, M. 1982. The question concerning technology, and other essays, Harper Perennial.

Ihde, D. 1990. Technology and the lifeworld, Bloomington: Indiana University Press.

Ilharco, F.M. 2002. Information Technology as Ontology: A Phenomenological Investigation into Information Technology and Strategy In-the-World, PhD thesis, London School of Economics and Political Science, Department of Information Systems. Available online: http://www.lse.ac.uk/collections/informationSystems/pdf/theses/Ilharco.pdf, consulted November 9, 2007.

Jasanoff, S. 1998. “The political science of risk perception,” Reliability Engineering and System Safety, 59: 91-99.

Latour, B. 2004. Politics of nature: how to bring the sciences into democracy. Cambridge, MA: Harvard University Press.

Lowe, G. 1996. “Breaking and fixing the Needham-Schroeder public key protocol using FDR,” in: Tools and algorithms for the construction and analysis of systems, number 1055 in Lecture Notes in Computer Science, Berlin: Springer, 147-166.

Luhmann, N. 1988. “Familiarity, confidence, trust: problems and alternatives,” in: Gambetta, D., ed., Trust: Making and breaking of cooperative relations, Oxford: Basil Blackwell.

Luhmann, N. 1995. Social Systems. Stanford, CA: Stanford University Press.

Luhmann, N. [1993] 2005. Risk: a sociological theory. New Brunswick: Transaction Publishers.

Mohen, J. and Glidden, J. 2001. “The case for Internet voting.” Communications of the ACM, 44(1): 72-85.

Oostveen, A.M. and Van den Besselaar, P. 2004. “Security as belief: user's perceptions on the security of electronic voting systems,” in Prosser, A. and Krimmer, R., eds., Electronic Voting in Europe: Technology, Law, Politics and Society, volume P-47 of Lecture Notes in Informatics, Bonn: Gesellschaft für Informatik, 73-82.

OSCE Office for Democratic Institutions and Human Rights 2007. The Netherlands parliamentary elections 22 November 2006: OSCE/ODIHR election assessment mission report. Available online: http://www.osce.org/item/23602.html, consulted March 16, 2007.

Park, J.H. 1931. “England’s controversy over the secret ballot,” Political Science Quarterly, 46(1): 56-81.

Pieters, W. 2006. “Acceptance of voting technology: between confidence and trust,” in: Stölen, K., Winsborough, W.H., Martinelli, F. and Massacci, F., eds., Trust Management: 4th International Conference (iTrust 2006), Proceedings, number 3986 in Lecture Notes in Computer Science. Berlin:Springer, 283-297.

Pieters, W. and Van Haren, R. 2007, “Temptations of turnout and modernisation: e-voting discourses in the UK and the Netherlands,” Journal of Information, Communication and Ethics in Society, 5(4), 276-292.

Pieters, W. (2008) La volonté machinale: understanding the electronic voting controversy. PhD thesis, Radboud University Nijmegen.

Smits, M. 2002. Monsterbezwering: de culturele domesticatie van nieuwe technologie. Amsterdam: Boom.

Smits, M. 2006. “Taming monsters: The cultural domestication of new technology,” Technology in Society, 28(4), 489-504.

Tijmes, P. 1992. “Martin Heidegger: techniek als metafysica,” in Achterhuis, H., ed., De maat van de techniek, Baarn: Ambo, 65-97.

Verbeek, P.P.C.C. 2005. What things do: Philosophical Reflections on Technology, Agency, and Design, Pennsylvania State University Press.

Woolgar, S. and Pawluch, D. 1985. “Ontological gerrymandering: the anatomy of social problems explanations,” Social Problems, 32(3).

Xenakis, A. and Macintosh, A. 2005. “Procedural security and social acceptance in E-voting,” in: Proceedings of the 38th Hawaii International Conference on System Sciences (HICSS’05), IEEE Computer Society.

[1] In this paradigm, “actual" refers to what is scientifically assessable. In this context, it is interesting to remember the distinction between the things in themselves and our observations of them as proposed by Kant. Here, the things in themselves (noumena) are not accessible by science, because science is based on observation. The phenomena, the things as observed by us, are the scientifically relevant aspect. The things in themselves (the “actual" things) are the domain of metaphysics, not science. In a way, the relation of “actual" to science has been reversed when compared to Kant's philosophy.

[2] This is more than just a pragmatic combination of theories. Phenomenology and systems theory have been combined in an analysis of information technology by Fernando Ilharco (2002). In *Social Systems*, Luhmann himself refers to the phenomenological theory and method repeatedly (Luhmann, 1995). Both discuss phenomena “from the inside”.

[3] There is a remarkable resemblance here to Descartes conceiving certain ideas as “clear and distinct". It is supposed, in both cases, that there are certain things that are understandable by just common sense, as opposed to derived or expert knowledge. These things can be directly extracted from experience, such that “perceived" and “actual" coincide.

[4] Interestingly, Latour (2004) uses the same phrase “taking into account” in his solution to the representational versus social constructionist issue.

[5] Confidence, self-assurance without knowing risks or alternatives, corresponds to concealment. Trust corresponds to unconcealment. By revealing the risks by means of ordering, confidence is concealed, and even seems to be unnecessary, or dangerous. Luhmann (1988) warns for a society that relies too much upon trust and neglects the amount of confidence that is necessary for participating in a complex society at all.