La Volonté Machinale

Understanding the Electronic Voting Controversy

Wolter Pieters

ISBN: 978-90-9022554-8
IPA Dissertation Series 2008-01

Typeset with LaTeX2e
Cover illustration by the author
Cover design by Ponsen & Looijen BV
Printed by Ponsen & Looijen BV

The work in this thesis has been carried out under the auspices of the research school IPA (Institute for Programming research and Algorithmics). The author was employed at the Radboud University Nijmegen and supported by the Dutch Organisations for Scientific Research (NWO) within the PIONIER project "Program Security and Correctness".

La Volonté Machinale:
Understanding the Electronic Voting Controversy

een wetenschappelijke proeve op het gebied van de
Natuurwetenschappen, Wiskunde en Informatica

PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Radboud Universiteit Nijmegen
op gezag van de Rector Magnificus prof. mr. S.C.J.J. Kortmann,
volgens besluit van het College van Decanen
in het openbaar te verdedigen op maandag 21 januari 2008
om 10:30 uur precies

door

Wolter Pieters
geboren op 4 februari 1978
te Pijnacker

Promotor:
Prof. dr. B.P.F. Jacobs

Copromotores:
Dr. ir. E. Poll
Dr. M.J. Becker

Manuscriptcommissie:
Prof. dr. F.W. Vaandrager
Prof. S. Rogerson, De Montfort University, Leicester, UK
Prof. dr. P.Y.A. Ryan, University of Newcastle upon Tyne, UK
Dr. ir. L.A.M. Schoenmakers, Eindhoven University of Technology
Prof. dr. H.A.E. Zwart

For security

How to Write

In the interest of safety, read instructions
completely before operating heavy machinery
safely. Do not run motor at excessive speeds:
your poem should be a set of instructions,
to deaden motor skills in the interest of safety

avoid the use of fashionable words and phrases;
avoid the repetition the repetition of the avoidance
repeatedly of the use of the use of repeated words
and phrases such as CNN-speak, sometimes, often,
and repeatedly called "bureaucratese," and seen

repeatedly in words such as "factoid."
As a matter of fact, certain facts of matter matter
(what's the matter?, the matter of matter is not to be taken
lightly); beware the perils of the machine:
always keep hands and feet clear of rotating parts.

Appendix A: Troubleshooting. If pencil breaks,
flow of thoughts, or clear vision of glory fades
wanly, consult fig. 17-a, diagram of Ezra Pound
in old age. Note the white beard, the crazed, deranged stare:
clearly, in the interest of safety it is safer not to write at all.

Matthew DeVille[1]

[1] `http://grove.ufl.edu/~esociety/tea_2/01.html`

Preface

"Could you make a website on electronic voting in the Netherlands?" This innocent request during the first year of my PhD research at the Catholic University of Nijmegen (now Radboud University Nijmegen) was probably the butterfly creating the storm that led to this book. At that time, I was trying to understand the LOOP program verification tool, and my master's degree in philosophy of technology did not seem so relevant. After making some small changes to this tool, I moved on to work together with another PhD student, Martijn Warnier, on a new approach to verifying confidentiality in Java programs. I had no idea that the societal aspects of information security would become a major theme in my thesis.

A couple of more pushes in this direction were needed. One was the subtle hint of finding my own topic, instead of collaborating with Martijn. Another was the involvement of the Security of Systems group in Internet voting experiments in the Netherlands. Lastly, my promotor Bart Jacobs introduced me to Marcel Becker, a researcher from the Centre for Ethics, whom he knew from the school yard of their children. The first result from this contact was a joint essay on ethical aspects of Internet voting. E-voting had become my topic, and social aspects seemed to be essential in the discussion on such new technologies. But it did not stop there.

From a philosophical perspective, I was baffled by the ease with which social aspects of security were reduced to "perceived security" in research papers on this topic. The suggestion that there is a fundamental difference between "actual security" and "perceived security" triggered the breakthrough paper of this thesis, which was published in the LNCS proceedings of the iTrust 2006 conference. After that, the social aspects played a vital and maybe even dominant role in my PhD project. In the meantime, I contributed to several computing science papers on topics such as anonymity.

I was strongly encouraged by my promotor, as well as by my daily supervisor Erik Poll, to continue my own line of research, even though it was not part of the mainstream work of the department. This appreciation of diversity seems to be a major factor in the success of the security group. I was given the opportunity to visit several conferences, and to spend six weeks in the United Kingdom for research on the e-voting debate in that country. These experiences greatly improved my understanding of the problems at hand.

All of this would not have been possible without the funding of NWO through

the PIONIER project on program security and correctness, and the guidance of my promotor Bart Jacobs, co-promotor Marcel Becker, and daily supervisor Erik Poll. Various people have contributed to papers of which results were included in this thesis: Marcel Becker, Luca Consoli, Robert van Haren, Engelbert Hubbers, Flavio Garcia, Ichiro Hasuo, Bart Jacobs, Hugo Jonker, Peter van Rossum and Martijn Warnier. I would like to thank the reading committee and the anonymous referees of the various papers for their careful consideration of the manuscripts.

I also wish to express gratitude to the respondents of my interview research in the United Kingdom: Alan Winchcombe, Ben Fairweather, Jason Kitcat, John Borras, Louise Ferguson, Paul Docker, Peter Facey and Peter Ryan. They provided essential information, and no-one complained that the interview lasted longer than expected. Robert van Haren did a great job in conducting the interviews in the Netherlands. Kees Aarts, Esther Beneder, Rop Gonggrijp, Maarten Haverkamp, Peter Knoppers, Piet Maclaine Pont, René Mazel, Berry Schoenmakers: thank you for your cooperation in the interviews.

The people of the anti-e-voting pressure group "Wij vertrouwen stemcomputers niet" provided a reliable resource of documentation on the political and societal process around the introduction of e-voting in the Netherlands. Even though I do not fully agree with their views, this database has been very valuable for researchers, and will be in the future.

This book would not have been the same without the support and advice of many people: Gerard Alberts, Erik Barendsen, Riyan van den Born, Iwan Bos, Simon Bouwman, Alf Bång, Ling Cheung, Luca Consoli, Charles Ess, Ben Fairweather, Steve Fuller, Rachel Gibson, Anders Hansen, René Heikens, Hugo Jonker, Joe Kiniry, Piet Maclaine Pont, Tarvi Martens, Wieneke Mulder, Bruno & Nanny Pieters, Simon Rogerson, Peter Ryan, Tim Storer, Wouter Teepe, and last in the alphabet but first in my life, Sanne van der Ven.

Wolter Pieters
Oosterhout/Nijmegen/Zeist
November 2007

Contents

Part I

Introduction

Chapter 1

Introduction

"One of the first things I learned in flying was that airplanes don't just fall out of the sky."

– Bruce Tognazzini, in The Butterfly Ballot: Anatomy of a Disaster[2]

Man did not really land on the moon. The WTC was not destroyed by terrorists. And electronic voting machines were introduced to make democracy a slave to capital.

Conspiracy theories are readily expected after each major achievement or disaster. But they also appear after the introduction of controversial new technologies. They seem to express above all a lack of trust in things that people have no control over, whether this is knowledge, technology, or both. In the old days, small groups of people were relatively self-sufficient in their needs. In the modern world – as we call it – information supply, energy supply, food supply, money supply have all been taken out of the hands of individual people and become part of major technological and social institutions. Functional differentiation has flourished, and each particular field of knowledge has its own experts. What exactly determines whether we trust the experts or not? And who are the experts? Can democracy be an exception to the tendency of dependence on specialised and localised knowledge?

1.1 La volonté machinale

This thesis is about electronic voting. I limit myself to voting in political elections, i.e. elections in which suffrage is not restricted to members of particular organisations.

[2] `http://www.asktog.com/columns/042ButterflyBallot.html`

Traditionally, voting in such elections, e.g. for president or parliamentary representatives, has been done by paper ballots. Even longer ago, oral voting by stating the name of the preferred candidate was practised.

In the second half of the twentieth century, the era in which the computer was transformed from a very special, very hard-to-use and expensive mainframe into a cheap and easy solution to all kinds of problems, the option of electronic voting came into focus. The first type of e-voting concerns the replacement of ballot boxes at polling stations with electronic devices for registering votes. This replacement had been almost completed in the Netherlands, and has affected a substantial percentage of polling stations in the United States. The technology is referred to as "electronic voting machines", "voting computers" or "polling place electronic voting". A second, and more radical, variant enables voters to cast their votes from anywhere using electronic devices, for example a computer connected to the Internet. This so-called "remote electronic voting" is usually not seen as a replacement, but rather as an additional option.[3] Estonia is the only country having this option in place for the general public.

When I started working on my electronic voting project, I doubted whether it would ever become such a major issue as genetically modified food, the greenhouse effect (now called climate change) or another new contagious disease. Especially here in the Netherlands, the introduction of electronic voting machines at polling stations had – at that time – not been very controversial. However, the list of countries that have the e-voting issue within the focus of the media is expanding, and particularly the way a recent campaign against e-voting in the Netherlands was set up makes clear that it is relatively easy to sensitise public opinion — or at least policicians' opinions – to this issue.

Are critical reactions to e-voting merely conspiracy theories? This thesis aims at offering conceptual tools for understanding the electronic voting controversies. How can we understand the discussion that e-voting has raised in so many different countries? Why do people claim that there is something fundamentally wrong with entrusting such a sensitive process as choosing our representatives to a machine? And how does this relate to scientific research into electronic equivalents of or substitutes for paper ballot properties?

Readers familiar with the work of the political philosopher Jean-Jeacques Rousseau (1712-1778) will have recognised the title of this book. Others may have wondered why a text on e-voting would have a French name. As I see it, the term explains more about the e-voting controversy than whole sentences in different languages.

Rousseau proposed the term "volonté générale", usually translated with "general will" to indicate what people would do if they were aiming for the common good. He

[3] In this thesis, I will use the terms "Internet voting", "online voting" and "remote electronic voting" synonymously, in the sense of what is sometimes called remote Internet voting (i.e. from any computer connected to the Internet, or other personal device). I do not discuss other forms of Internet voting that use access restrictions such as "kiosk voting" (Alvarez and Hall, 2004, p. 4).

contrasted the term with the "volonté de tous", the will of all, which was the sum of the individual, and selfish, preferences.

Elections are about determining the will of the people. Whether this should be characterised as the general will or the will of all is a matter that I do not wish to discuss here. However, electronic voting introduces a new way of expressing this will, i.e. through a machine. "La volonté machinale" has been born.

The title of this book can be translated as "the mechanical will" or "machine will". It can be taken to mean the following things:

- the will of the people calculated by a machine (as in the instrumental view of technology): technology is merely a means to do the same thing differently;
- the intention of the machine to substitute its own will for that of the people (as in a pessimistic view on verifiability of computers): technology is fundamentally incompatible with democracy;
- the people's desire for having machines (as in the argument that people want new ways to vote): people do their banking online, so they want to vote online;
- the machines having a will to be introduced (as in technological determinism): the technology will come, if we want it or not.

We will see all of these aspects of the "volonté machinale" in this book.

1.2 Flying & voting

If someone casts a vote, she wishes to be certain that this vote is counted at the end of the day. This holds both for paper voting and for e-voting. As for many other technologies, people are dependent on voting systems for the adequate performing of certain tasks. And as for other technologies, people may experience that they fail.

Let us consider an example with a longer history. If someone boards an airplane, why would she trust to be transported safely to her destination? Primarily because there is a lot of experience with airplanes by now, and there are many safety and security procedures around flying, as anybody who has ever been on a plane knows. This does not mean that nothing ever happens, but there is considerable consensus about measures that can certainly reduce the risk.

The first airplanes *did* break down easily. The inventors had enough problems making their constructions fly, and it took two world wars to make planes that were not only good enough for military purposes, but also safe for transporting citizens. Incidents and accidents throughout the history of aviation have set the agenda for many improvements in safety and security measures. Of course, it was a new means of transportation, and it did not make sense to say "The airplane is safe, because it works exactly like a ship; it's just faster."

Similarly, electronic voting is not just a new implementation of paper voting. It is different. There are different requirements, different procedures, and so forth. And,

as in aviation, there may be people who wish to disrupt the system. But people are impatient. Let's all exchange the water for the skies.

Avi Rubin, a well-known American e-voting critic, writes about his opponent Brit Williams:

> "Williams emphasized that people should not reject technology just because it is complex. After all, he said, people fly on airplanes all the time, so there was no reason to fear electronic voting machines." (Rubin, 2006, p. 55)

The analogy with flying helps as far as we wish to express that new technologies need new requirements. It does *not* help if we wish to express that these requirements will come in the same package as the technology. This did not happen in flying either. It also does not help if we wish to express that the new technology is completely secure *by itself*. Even with appropriate measures, the security of many devices is still dependent on people:

> "Aviation systems are designed to be reliable, but not necessarily secure. If a pilot wants to crash a plane, the system might trigger some kind of alarm, but it will not be able to stop him." (Rubin, 2006, p. 184)

An important distinction can be made between *safety* and *security*. In case of safety, possible problems are understood in terms of properties of the airplane itself. In case of security, possible problems are understood in terms of these properties *in combination with those of people who would like to make the airplane crash*. Security, as opposed to safety, involves human opponents.

As well as in the case of airplanes, the e-voting issue is typically a discussion on *risks*. Other "risky discussions" in society take place or have taken place around for example genetically modified food, climate change and nuclear energy, and, taking into account the previous example, new means of transport.

It seems to make sense to separate discussions on risky technologies from discussions on risky theories, since the first have to do with manipulating, and the second only with understanding. Darwin's evolution theory was (and is) not primarily subject of controversy because of its risky implications for breeding animals. Instead, it was under attack because its theoretical implications were irreconcilable with existing world views. For a similar reason, whether or not we have been on the moon does not really matter that much for our safety. It is a matter of *belief*.

Controversies that involve technology, instead, are usually based on uncertainty about possible *future safety or security threats*. This is not to say that theories or claims cannot lead to future problems, but these are usually not discussed when the theory or claim is first presented. There, the primary concern is the *truth* of the theory; in cases of risk, it is our safety.

There is a link, however, between the two types of controversy. The consequences of a risky technology for our safety depend on *facts* about the risks that it entails.

These facts are claims or theories. So, while the primary concern is safety and security, the discussion inevitably includes a theoretical dimension.

It is this theoretical dimension of discussions on risk and security that this thesis will focus on. Related concepts that often appear in the debate are trust, safety and security. I will not primarily discuss practical consequences of or reactions to e-voting for their own sake. Rather, I focus on how benefits and risks of the new technology are being determined and agreed upon, and use specific cases as examples. Thus, I do not discuss whether or not e-voting systems can be hacked, but rather how it is being determined that they can be hacked or not, and how this helps us to make sense of the debates in different countries. Practical consequences are only discussed in their role as facts or claims in the theoretical discussion.

1.3 Problem statement

The main research question of this thesis can be formulated as follows: How can we explain the controversies on e-voting in terms of the conceptual or theoretical dimension of risk, trust and security?

There are four subquestions:

1. Which are the similarities and differences between conceptualisations of e-voting in controversies in different countries?

2. Which reasons on the conceptual level make e-voting become a controversial topic for the public?

3. What is the role of (computing) scientists in such discussions?

4. How can we pro-actively use this conceptual level to improve the discussion on e-voting and similar topics?

Once we understand the concepts that are used in the controversies (question 1), we may be able to find conceptual-level explanations of the controversial character of e-voting (question 2). Understanding the role of scientists in creating conceptual frameworks (question 3) may offer starting points for pro-active improvement of these concepts (question 4).

If we wish to understand the controversies, we cannot do without this conceptual level, as I hope will become clear in these 181 pages.

1.4 Method

This text is not a description of empirical research. This is not to say that it is purely theoretical, but apart from the interview research discussed in chapter 3, the method starts from conceptualisation, not from *systematic* observation. Neither is it constrained to a single discipline. If disciplinary at all, it is a combination of

philosophy of technology and computing science[4]. Philosophy, because it contributes to the concepts we can use in discussing information security. Computing science, because at least part of the research contributes to making certain desirable properties of electronic voting systems precise and measurable. In some sense, the whole project is about conceptual analysis, which is philosophical on a high level and mathematical on a low one.

Some people call such approaches "information science". I did indeed teach courses to information science students on information security and research methods. But information science can also mean information architecture design or even communication studies. What I do is discussing the relation between information technology and society, from a conceptual and sometimes empirical perspective.

Annemarie Oostveen (2007) describes her related research on societal aspects of e-voting as "social informatics". From her description, it becomes clear that this more or less means constructive technology assessment (Schot and Rip, 1997) of information technology, i.e. including considerations of the implications of the technology in the design process. A multi-method empirical approach is used to study the e-voting developments, from which it is concluded that it is essential to have a paper copy of each vote. The present research, however, is more focused on theory than on empirical study of small-scale experiments. Also, I am much more hesitant to draw strong normative conclusions from empirical data.

A better categorisation of this work would include it in the field of science and technology studies (STS). This interdisciplinary type of research investigates scientific and technological developments from different perspectives, such as philosophy, sociology, political science and communication studies. In e-voting, both technological and scientific developments play an important role. Since this study is also interdisciplinary, the categorisation as an STS endeavour is justified. Philosophy and computing science are the dominant disciplinary perspectives here. As a computing scientist, I use the STS "detour" for considerations on how to improve technology and its embedding in society.

This project does not aim to give clear answers to questions posed *within* the e-voting debate. Rather, it provides a vocabulary that can be used in scientific and public discussion on desirable scenario's on the future of democracy. That is to say, even the ethical part of the book is descriptive rather than prescriptive, although there certainly is a normative element: the assumption that conceptual clarification is a high priority matter in general; if not for itself, then for the sake of our future. For if we do not have the proper concepts to discuss things, then democracy and technology will (indeed) exclude each other. The value of conceptual clarification will be justified for and from the case of e-voting. Still, conceptual clarification is also part of the scientific enterprise, and in that sense it does not need justification in a scientific book, except maybe for those who believe all science is quantitative.

[4]Computing science is also called "computer science". I judge the former term to be more appropriate, since the device is the means rather than the goal. Whether "computer security" should also be replaced by "computing security" is less obvious, and I will use the former and more common notion in this thesis.

What can the reader expect, then? First of all, she will find a philosophical analysis of the electronic voting controversy within the wider context of information security, and within the even wider context of risk assessment. This analysis draws primarily on 20th (and 21st) century philosophy. The focus is on philosophical theories that help us solve political problems by realising that the world is not the same for all of us but also avoiding the conclusion that there is no world at all. Particularly helpful in this context are phenomenology, pragmatism, systems theory and actor-network theory.

Moreover, the reader may come to realise that certain notions in the electronic voting debate are vague, and may need more and possibly mathematical (or legal!) precision. The question then becomes if we can still reach agreement, if the formulation of the problem gets so formal that many people will not be able to understand it, or its implications. Therefore, we will need to discuss the notion of trust.

Three warnings need to be explicated here. The first warning states that even though certain notions of scientific objectivity are criticised in this thesis, this is *not* to be read as criticism of the scientific discipline of information security. Rather, I try to provide an alternative vocabulary for speaking *about* the achievements of the discipline.

The second warning states that even though this thesis is presented as a single book, the origin of the chapters often lies in separate articles, and the order in which the chapters are presented here, even though convenient for the line of argument, is certainly not the only option. The reader may discover many family resemblances[5] between the chapters. If the reader feels like this is repeating the argument in different words, she may appreciate that precisely these similarities may help others in understanding the main points.

The third warning is about interdisciplinarity. The writing of this book required conceptual research in computing science and philosophy, as well as qualitative empirical work. I think that it is indispensable for an interdisciplinary study of science and technology developments to reach a level of understanding of the field one is studying that allows one to contribute to the field itself. In such a study of science and technology, it takes at least one year to be able to understand the scientific and technical issues at stake. Inevitably, this means that the time left to spend on the sociological and philosophical issues is limited. The book is therefore not meant to be an in-depth study of the application of philosophical theories to information technology. Instead, new directions are explored in the interaction between theoretical frameworks and empirical material on scientific, technological and societal aspects electronic voting. The book is aimed at a more general audience of scientists and policy makers, and some of the background material in both computing science and philosophy necessarily has to remain implicit, or included in footnotes. References are provided for further reading though, and, most importantly, opportunities for future research are identified.

[5] A notion introduced by Ludwig Wittgenstein. It expresses the idea that several phenomena are put in the same category, even when no common feature can be mentioned, e.g. in the concept of "game".

	controversies	public	science	future
overview	2,3		7	
limitations		4	8.1	
alternatives		5,6	8,9	10

Table 1.1: Dimensions and chapters

1.5 Reader's guide

Apart from introduction and conclusions, the present book can be seen as having four main parts. In the first part, which consists of chapters 2–3, evidence of the existence of the controversies is presented, and similarities and differences between countries are identified. The second part, consisting of chapters 4–6, focuses on the issue of public perception in such controversies, usually called perceived security. Chapter 6 leads us to a conclusion on how science can help in such a controversy. The third part, then, concentrates on this role of science (usually discussed in terms of actual security), and consists of chapters 7–9. The last chapter returns to the society perspective, and aims at giving directions for the future of the debate.

Three main themes help us to unravel the leading question of this book on concepts and facts, and its subquestions, in the e-voting debates:

1. What is perceived to be going on in the e-voting controversies? (ch. 2, 3 for society as a whole, ch. 7 for science)

2. What are the limitations of common (positivist) explanations? (ch. 4 for society, section 8.1 for science)

3. Can we use alternative theories to explain the situation better? (ch. 4–6 for society as a whole, ch. 8–9 for science, ch. 10 integrated perspective)

In table 1.1, an overview is presented of the subquestions of the research against the themes mentioned above. For each combination, the chapter discussing it is indicated, if available. In table 1.2, the main theoretical approaches used in the chapters are mentioned. Where possible, connections between the different approaches will be identified in the text, but I consider them valuable in their own right as well, in the sense of approaching the same problem from different angles, without necessarily pretending to have an overall systematic theory.

The book is organised as follows. In chapter 2, an overview is sketched of the electronic voting debate, particularly in the US, the UK, the Netherlands and Estonia. This will provide the reader with an idea of what are judged to be the most important issues. In chapter 3, empirical research based on interviews with experts in the UK and the Netherlands is presented. This will improve the understanding of what constitutes an e-voting debate, and how this is framed by the cultural setting. In chapter 4, I will explain the paradigm in which such a controversy is usually explained once it is realised that technical sophistication is not a sufficient condition for acceptance and

chapter	theory
3	strategic niche management
4	Woolgar/Pawluch, Latour, Luhmann
5	Smits (monster theory)
6	Luhmann
8	Smits (monster theory)
9	Heidegger
10	Dewey, postphenomenology

Table 1.2: Overview of theories

success of a new technology. I will also provide three arguments for my reluctance to adopt this paradigm, and I will provide the basic ingredients for an alternative to be developed in later chapters.

Chapter 5 turns towards a cultural explanation of the e-voting controversy. This provides a counterbalance to the explanation in terms of failure or misunderstanding of the technology. In chapter 6, the focus is on what happens to the debate once the cultural problems have been exposed. This has consequences for our trust relations with respect to the technology, and entails new requirements for electronic voting systems.

Chapter 7 concentrates on the scientific challenges in computing science that are raised by the new requirements. In chapter 8, I investigate how scientists try to solve these issues. Chapter 9 is devoted to introducing new terminology that may serve as a replacement for the vocabulary of the problematised paradigm.

In chapter 10, I show that the process of determining the new requirements is naturally influenced by the technology already developed or under development. In this way, the technology requires reconstruction of the concepts with which we judge the technology. The term *reconstructive technology assessment* will be coined as a summary of what is described in this book with regard to the e-voting controversy.

In the conclusions, the argument is summarised, and I will discuss benefits and risks not of e-voting, but of my approach to investigate the controversy.

Part II

The controversies

Chapter 2

The e-Voting Controversies

"Vote: The only commodity that is peddleable without a license."

– Mark Twain (American humorist, writer and lecturer, 1835-1910)

As a start of the argument set out in this thesis, an overview is given of the e-voting controversies in different countries. This will provide the basis for lifting the discussion to the conceptual level. The description of the controversies is not the main contribution of this book, but it is helpful as a starting point for understanding the analysis in the following chapters. This chapter is not derived from a full empirical study, but rather from a literature-based historical overview of the situation in different countries.

The focus in this thesis is on the controversies in the Netherlands and the UK, for which both literature study and interview analysis were performed. The comparative study of the discourses in the UK and the Netherlands is my main empirical work, and will be presented in the next chapter. This chapter is limited to a reconstruction of the situation in these countries based on the available scientific literature. The literature study in the present chapter was extended to include the United States and Estonia, two countries which have often appeared in the news regarding e-voting. Much has been written about the controversy in the US, and Estonia has shown a remarkable speed of development in e-voting matters.

Concerning the US, the description is mainly based on four books: *Steal This Vote* by Andrew Gumbel (2005), *Brave New Ballot* by Avi Rubin (2006), *The History and Politics of Voting Technology* by Roy G. Saltman (2006) and *Point, Click and Vote: the Future of Internet Voting* by R. Michael Alvarez and Thad E. Hall (2004). Besides, references are provided to the major publications in the controversy. As for the book by Gumbel, this is first and foremost a journalistic review of the matters.

Scientifically, we should not take the contents at face value. This also holds for the autobiographic story by computing scientist Rubin on his experiences as an e-voting critic, identifying many of the social connections in the e-voting network. Although trained as a scientist, Rubin is not primarily a sociologist, which requires us to take caution in interpreting the work.

I consider the books by Saltman and Alvarez and Hall the most trustworthy scientific sources on the issue, because they succeed in approaching the issue from many different, but coherent, angles. Also, their approaches do not rush to conclusions, but rather provide valuable unbiased material that can be consulted by decision makers (and voters). Still, Saltman's historical approach is very brief on some contemporary – especially technical – matters. Alvarez and Hall focus only on Internet voting, and not primarily as historians. The other two books do contain some essential information for filling these gaps. Therefore, if we are conscious of possible prejudices and biases, we can reconstruct – in the meaning of re-construct, not as in putting it back into the state it was in before – to an acceptable extent the problems in the United States.

As for the other countries, the Estonian situation is explained based on reports (Drechsler, 2003; Drechsler and Madise, 2004; Breuer and Trechsel, 2006; Madise, Vinkel, and Maaten, 2006; OSCE Office for Democratic Institutions and Human Rights, 2007b) and an informal conversation with project leader Tarvi Martens, and should be considered no more than an introductory sketch. For the UK and the Netherlands, a comparative case study was done based on formal interviews with experts involved in the debate, but in this chapter I limit myself to a reconstruction of the situation. This reconstruction is based on available documentation, and serves as an introduction to the interview results in the next chapter.

Electronic voting machines or voting computers have also been used in for example Brazil (Rezende, 2004), India, Venezuela and Belgium. Switzerland has used online voting in referenda (République et Canton de Genève, 2003; Geser, 2004). These countries will not be discussed in this thesis.

2.1 Help America vote

America is often seen as the prototype of a western democracy. For all the limitations of a two-party system, for all the conflicts between federal and state level, there must be something that makes American democracy what it is and makes the world look at it. The world is also watching how American citizens do their democratic duty, which is more and more by means of electronic voting. The US have a complicated election system, with many races – federal, state, local and referendum – being run simultaneously in a single election. This has led to continuous incentives to modernise the process.

From viva voce to the ballot

The discussion on voting methods is as old as the country. After the American independence, the clause of "consent of the governed" in the Declaration of Independence became important in framing the debate on the conduct of elections. If a government is to be really sure to have the "consent of the governed", how should this be expressed in the way in which elections are run?

> "The question in 1776 was whether each individual granted the right to vote would be able to cast those votes without intimidation. Separation from Britain would assist that cause, in that it would foster some elimination of oral voting, but it would not fully assure secret voting for more than a century." (Saltman, 2006, p. 41)

By that time, many states used oral (or "viva voce") voting. This did not allow voting in secret, because one had to say out loud the names of the candidates that one preferred.

> "On the day or days of election, each voter would make his way to the table where the judges of election and their clerks sat. A voter would be asked to verify his financial and residence status, and then requested to declare his choices. Votes would then be written down by the clerks, and any candidate present might publicly thank a voter who voted for him." (Saltman, 2006, p. 43), see also Nutting (1948)

Still, the transition to paper voting was not self-evident. Many people opposed paper voting for different reasons. There was the issue of illiteracy, allowing cheating in "helping" the voters who could not read or write. It has been argued that in some places, ballot voting was introduced precisely to disenfranchise the illiterate. Then there was the issue of ballot stuffing. With ballot boxes, it became possible to fill those with illegitimate ballots, since there was no longer a need to associate the name of a voter with a ballot. Some elections had more votes than voters.

Even after oral voting was gradually eliminated, the ballots being used did not guarantee secrecy. Some districts used handwritten ballots, in others pre-printed tickets were distributed by the parties in newspapers. Often, an observer could determine from the colour of the paper which party ticket was placed in the ballot box.

The officially produced ballot containing all candidates and available only on election day, now in use in many countries, is called the *Australian ballot*. It was first introduced in the Australian state of Victoria in 1856 (Saltman, 2006, p. 96). The concept first appeared in the US in an article from 1871. It took until 1885 before the first proposal appeared in a state legislature, but this Michigan bill was rejected. In 1888, the Australian ballot became finally mandatory somewhere in the nation, albeit only in the city elections in Louisville, Kentucky. However, developments went very fast from that point onward. By 1896, only seven states had not passed legislation mandating the "real" secret ballot.

The poll tax for federal elections was abolished in 1964. The issue of having to pay for voting becomes relevant again with new technologies. If Internet voting were the only means of casting a vote, voters could only vote from home if they would pay for an Internet connection and equipment.

Levers and punch cards

Around 1900, many US patents were filed involving the design of mechanical voting machines using push-keys or levers. Their use was accepted in many states, either by legislation or by court ruling. It was argued that the previous requirement of having a paper ballot was mainly meant as a safeguard for the secrecy of the vote, and therefore not an impediment to mechanisation: a so-called teleological interpretation of the law,[6] which we will see in Estonia a century later. The concept of verifiability had apparently not been invented yet.

In 1928, 1/6 of the voters were using lever voting machines, according to an advertisement by one of the manufacturers (Saltman, 2006, p. 121). The main advantages of the machines seemed to be faster announcement of results and the elimination of error-prone hand counting. Disadvantages of machine voting included congestion at the polls (only one voter could vote at a time), necessity of a backup paper ballot system in case of machine failure, and limitations of the machine in particular voting systems. One of the other effects of the introduction of voting machine was the elimination of the Electors from the presidential ballot. Due to space restrictions, it was impossible to list on the machines all the names of those who would participate in electing the president on behalf of the State.

Punch card machines and optical-scan systems were introduced in the 1960s. Both had the opportunity for manual recount, as opposed to the lever systems. People did not agree about whether this was an advantage. The advent of direct recording electronic machines (DREs), similar to lever machines in the sense that there are no visible ballots, started around 1975, but mainly developed from the late 1980s. By 2000, 13 percent of the voters used DRE equipment.

Still, there was not much discussion going on about the effects of the new technologies, the last federal intervention stemming from the previous century:

> "*Vote casting technology would fall off the national agenda* for a full century. The adoption of a voting machine not using ballots would be permitted by the Congress in 1899 [...] but, after that, there would be no federal legislation concerning vote-casting technology until 2002.
>
> Additionally, the adoption of PPCs [a type of punch card, WP], mark-sense ballots, or direct recording electronic machines for voting in public elections would not be listed as significant events in respected volumes of histories of the United States, *even when specific sections of the books were devoted to science and technology.* It would be as if a new type of voting technology was a mere administrative detail no more important than, say,

[6] i.e. an interpretation in terms of the goal a certain article was meant to achieve

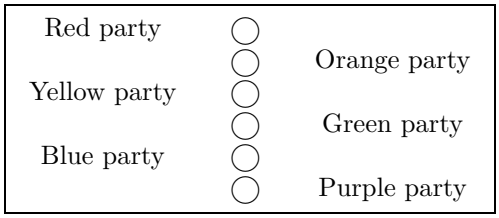

Figure 2.1: A butterfly ballot design.

> the purchase of new calculators for office workers at the local city hall. The mind-set of both policymakers and the media would change after the close of polls on November 7, 2000." (Saltman, 2006, p. 103)

Florida 2000

The major battleground of the 2000 presidential election was the state of Florida. The count was extremely close there, and particular arrangements, political and technical, proved decisive for the outcome. Apart from partisan officials more concerned with helping their party than with ensuring a fair outcome, there were legal matters as well. Florida law states that "no vote shall be declared invalid or void if there is a clear indication of the intent of the voter as determined by the canvassing board" (Saltman, 2006, pp. 6, 19). But what is "the intent of the voter"?

Each county was free to determine its own voting technology and ballot design. Types of equipment being used included punch cards, optically scanned ballots (mark-sense), lever machines and hand-counted paper ballots.

With one of the type of punch cards being used, PPC for Prescored Punch Cards, voters had to push out a piece of paper that had been partly cut out from the card, but was still attached at each of the corners. Many voters, due to either lazy behaviour or particular difficulties of the voting devices, failed to remove the "chad" completely from the card, which left room for discussion on the "intent of the voter". If a chad is still attached at one corner, is this a vote? And two corners? And three? And if it is only "pregnant", i.e. indented? (Saltman, 2006, p. 8)

In Palm Beach County, another problem worsened the intricacies of the punch card devices. To make it possible to use a large font, candidates on the presidential ballot were arranged on the ballot in a "butterfly" layout (see figure 2.1). With the line of punchable chads in the middle of the device, the booklet accompanying the voter in her journey through all the races would show some of the candidates on the left page, and others on the right. If all the candidates would have appeared on the left, the font would have needed to be smaller, causing usability problems for sight-impaired voters.

The effect of this alignment may have been that voters who would have liked to vote for the *second* candidate on the *left* side, could have chosen the *first* candidate on the *right* side. This is because they would look for the first hole below the first

candidate on the left to vote for the second candidate. In this particular case, they might have voted for Pat Buchanan instead of Al Gore. There is statistical evidence that this may have influenced the outcome of the nationwide election (Saltman, 2006, pp. 16, 35–36). Also, voters may have thought that they were required to cast a vote for *both* pages, leading to overvotes[7].

Thus, both accuracy and usability problems of punch card voting machines showed up in the 2000 election. With such possibilities for challenging the outcome, any country would have some trouble. But in the US, all election officials are partisan. This means that *if* the officials cannot separate their partisanship from their role as election supervisors, they will inevitably support the claims that are beneficial to their own party. In such a situation, no one will trust each other.

The problems led to court cases challenging the results, demanding manual recounts, and accusing officials of partisan decisions. The effect of the apparent problems with the technology, combined with the issue of partisan officials and even judges, made it last until December 12, more than a month after the election of November 7, before the US Supreme Court put an end to the challenges.

The Florida disaster exposed the problems, but it was (and is) certainly not the only state having problems with voting technology. Besides these accuracy and usability problems, voter registration is a major factor in the US as well, involving again partisan supervisors. I do not discuss voter registration in this book.

For all the reluctance in the US to have problems solved at federal level, in this case there was bound to be intervention. But what was learnt from the experiences?

DRE: our saviour?

In 2002, Congress passed the Help America Vote Act (HAVA). The new legal arrangements provided for independent advisory and certification agencies, and funding for new voting equipment. Many states and counties were eager to use HAVA funding to have their punch card and lever machines replaced with something more "modern". Modern practically meant computer-based.

Again, America was looking for technical solutions to the voting problems. They had done so since 1900, but both lever machines and punch cards had been accused of causing their own problems. Would the computerisation of the DRE machines be the final technological fix?

Use of DRE equipment rose to 31 percent in 2004. Meanwhile, criticism of the lack of verifiability in DRE systems had become more pronounced. The critics concentrated on the touch-screen systems, not so much on the older full-face DREs, which used buttons instead of a computer-like screen. This may have had its origins in the same machine-computer dichotomy that would have a major influence on the debate in the Netherlands, as we will see.

The particular event bringing election verifiability to public attention was the leakage of the source code of one of the systems of the manufacturer Diebold. It was

[7]Overvotes are votes for more than one candidate in a race, where only one vote is allowed.

found in July 2003 by Bev Harris, who was not particularly familiar with source code, on Diebold's own servers. Researchers of Johns Hopkins University, most notably Avi Rubin, analysed the code and found various security problems and naïve use of security measures meant to protect against malicious use (Kohno, Stubblefield, Rubin, and Wallach, 2004). By handing their report to the media before discussing it with the state officials (Rubin, 2006), they triggered a chain of events that would seriously challenge the trust in e-voting in the US, and even the world.

Rebecca Mercuri, another well-known computing scientist, had not been very happy with their report. She posted "a harsh criticism of the report to her website." (Rubin, 2006, p. 25) The critique mainly focused on the lack of understanding of election procedures. According to Rubin, she warned them not to go public or at least add a link to her criticism.

Mercuri had been known as the inventor of the "voter verified paper audit trail" (VVPAT), also labelled the "Mercuri Method" (Mercuri, 2002). In this procedure, the voting machine produces a piece of paper representing the voter's choices, which can be verified by the voter, but not taken away. The paper copies of the ballot can then be used for recount purposes. With respect to this background, Rubin realised he was "working in what arguably was her turf." (Rubin, 2006, p. 25)

Voting machine manufacturers responded to the report by saying that the researchers had focused too much on technical security, ignoring other security measures, especially in the procedures invoked in using the machines (Oostveen, 2007, p. 134). Apart from the issue of technical security versus organisational security, and the accusation against Rubin of only focusing on the technical matters, a couple of other counterarguments appeared:

- the fact of Rubin being on the board of advisers of VoteHere, a company developing voting software (not complete systems), being seen as a conflict of interest;

- election officials being proud of their modern systems, and not accepting the fundamental criticism, arguing that the systems have never caused any problems;

- mixed responses by Diebold, saying that the source code that was found had never been used in elections, that it was an old version that had been improved since, that the problems mentioned in the report were not real problems, or that all the problems mentioned in the report had been taken care of after the release;

- organisations of disabled people fearing that the benefits they gained would disappear if doubt were cast on the security of the new and accessible systems (Rubin, 2006, pp. 242-248).[8]

[8] One of the critics of the report was Brit Williams, whom we already met in the introduction of this book when we discussed flying and voting (page 6).

Still, it seems like the US authorities are beginning to agree on the facts. These are often interpreted as indicating that a paper trail is necessary. A majority of the states have now passed legislation making a paper trail mandatory.[9] The arguments are being transferred to Europe (Oostveen, 2007), without much discussion of different cultural circumstances. Still, critics argue that there is no meaningful way to determine which trail (computer or paper) should have priority in case of a dispute. Which of the two is most likely to contain mistakes or manipulation? Also, it has been suggested based on psychological arguments that voters are not likely to check the paper receipts (Selker and Goler, 2004). If that is true, what benefit do we gain by printing the things? Manufacturers also point to breakdown problems becoming much more likely if mechanical parts like printers are introduced in the machines. Availability is a serious security issue in elections too. But so far, the paper trail machines seem to work acceptably.

The breakdown of the Internet alternative

A different approach to electronic voting (and a cause of much confusion in terminology) is voting through the Internet. I will use the term e-voting for *any* kind of electronic voting equipment or software, and reserve the concept of Internet voting (or i-voting) for voting from an electronic device connected to a data network. Apart from computers, voting equipment may also include computerised devices such as mobile phones or digital television.

There are various different ways in which the Internet can be used in voting. Firstly, *remote* Internet voting allows voting from any computer connected to the world-wide network. A more controlled variant is to have "kiosks": supervised locations with (dedicated) computers connected to the Internet, but more widely spread than the current polling stations (e.g. in supermarkets). One could also allow voters to cast their ballot through the Internet from any polling station of their choice. Finally, one could allow voting only from the voter's precinct polling station, but still use the Internet to submit the vote (Alvarez and Hall, 2004, p. 4).

In this book, I focus on remote Internet voting. Because the voter can fill in her ballot from any location, this is similar to voting by mail (VBM), which is called postal voting in the UK. The idea of voting through the Internet is popular, because it seems to be very modern in the age of Internet shopping and banking. Why bother with voting machines if more and more people own a very flexible voting device, i.e. a personal computer?

The main experiment in the US with remote Internet voting was the SERVE project (Secure Electronic Registration and Voting Experiment). The system developed was meant to allow military personnel oversees to cast their ballots in the 2004 presidential election. However, four people invited to participate in the Security Peer Review Group, among whom again Avi Rubin, released a report in which they not only

[9] See Election Reform Information Project (2006) and `http://www.verifiedvoting.org`, consulted February 21, 2007.

claimed that the security of the SERVE system was broken beyond repair, but also that *any* Internet voting system would suffer from unacceptable security problems (Jefferson, Rubin, Simons, and Wagner, 2004). This report effectively put an end to the project (or at least the authorities made it appear that way). R. Michael Alvarez and Thad E. Hall had written in their book that the SERVE experiment would yield very valuable data on the effects of online voting (Alvarez and Hall, 2004, p. 146). Since the project was shut down, they would never get their results.

The SERVE experiment was not the only project with remote voting in the United States. In general, there are two ways to make it easier for people to vote: extending the place where they can vote, or extending the time when they can vote. This leads to absentee voting and early voting, respectively. *Absentee voting* can be done through voting by proxy, which was in use already in 1635 in Massachusetts (Alvarez and Hall, 2004, p. 106). In Europe, the Netherlands have a exceptionally liberal policy of voting by proxy. *Early voting* can be done by going to a polling station *before* election day to cast a ballot. It was allowed in 13 states in 2000 (Alvarez and Hall, 2004, p. 103).

Usually, early voting and absentee voting are combined. Traditionally, this meant voting by mail. This procedure has its roots back in the Civil War, when the troops could send their ballot to a person back home who could cast it for them. Mail voting procedures changed over time, but the option remained restricted to military personnel – with a few exceptions. Oversees military VBM ballots became common in the Spanish-American War and World War I.

In 1916, the first law allowing mail voting for nonmilitary oversees citizens was adopted in Virginia (Alvarez and Hall, 2004, p. 106). After World War II, absentee balloting flourished, but there were still restrictions on the circumstances under which people could request an absentee ballot. By 2000, 22 states no longer requested any reason or motivation (p. 103), which is called "no-fault" or "liberalized" in the US and "on demand" in the UK. In California, the percentage of absentee ballots increased from 4.4 percent in 1978 to 26 percent in 2002 after the introduction of liberalised absentee voting (p. 109). Many states also offer the opportunity to register for permanent absentee voting (p. 103).

In a gradual implementation process, the state of Oregon made a transition to universal VBM (the British would say all-postal) elections, starting with pilot laws in 1981. Since December 1995, the state has stopped the traditional voting methods. In 1998, the citizens made this permanent in a referendum (Saltman, 2006, p. 209). According to Alvarez and Hall, "[t]he critical facet of the Oregon experience is that the process of moving to VBM was gradual" (Alvarez and Hall, 2004, p. 122).

The success of this project provides useful experience with citizens voting in a private environment, with other people possibly present. In a survey conducted after the election, 1.4 percent of the voters felt "under pressure", 0.5 percent changed their vote because of the pressure (Southwell and Burchett (1997), quoted in Alvarez and Hall (2004), pp. 114–115 and Saltman (2006), pp. 209–210). However, these figures represent 3 and 1 individuals out of 220, respectively, and cannot be considered reliable numbers. Still, the percentages suggest that the problem of coercion is small.

Thus far, the only experiments with Internet voting in official elections in the US have taken place in the March 2000 Arizona Democratic primary (35,768 remote electronic votes), and in the 2000 general election (84 remote electronic votes) (Alvarez and Hall, 2004, pp. 129, 139). Increased turnout has not been proved to be an effect of Internet voting; even though turnout was boosted in the Arizona primary, this may have been due to extensive publicity campaigns and the novelty effect rather than substantial influence of the medium used (Gibson, 2001).

Oversees voters in US elections could benefit from remote electronic voting, which is at least claimed to be more *reliable* than the postal system, in the sense that there can be a confirmation that the vote has been received. Another advantage is the prevention of time pressure during voting in states with very long ballots, i.e. many races run in the same election. Whether the Internet-based system can be made *secure* enough and *politically acceptable* is an open question. Do we need more experiments to study security and social effects? According to Michael Alvarez and Thad Hall, we do. After the devastating SERVE report (Jefferson et al., 2004), not much has been happening, though. In 2007, a new initiative was proposed for overseas citizens (Department of Defense, 2007), aimed at the elections of 2008 and 2010.

The prospects for Internet voting in the US have been worsened by the popularity of the paper trail requirement for DRE voting equipment. In remote electronic voting, a paper trail is not possible, because "[t]he voter is not at the point of vote summarization to examine a receipt" (Saltman, 2006, p. 211). States requiring a paper trail may therefore not be able to experiment with Internet voting, depending on the legal text and its interpretation. Because of this history, researchers in the US interested in studying the effects of remote electronic voting should probably be looking towards Europe.

According to Alvarez and Hall, the experiments in Europe differ from those in the US in three aspects.

> "First, there is less of a local flavor to elections overseas, where national governments play a greater role in managing elections and promoting new technologies than in the United States. Second, the electoral process in most other nations is much simpler. [...] Third, the European trials have been much smaller in scope than the U.S. trials, giving them the advantage of being easier to control and potentially easier to evaluate." (Alvarez and Hall, 2004, pp. 142–143)

American concerns

Due to the complicated nature of elections in the US, modernising the voting process has often been in focus during the history of the country. After the problems in the 2000 election, polling place e-voting by means of DREs was seen as a good solution. The main concerns in the US have been the correctness and integrity of the voting devices, and the (lacking) opportunity to verify the results. Internet voting has been strongly criticised for lack of security and secrecy.

2.2 Let Estonia be modern

The former Soviet republic of Estonia regained its independence on August 20, 1991. Afterwards, the country experienced a swift westernisation and modernisation, the former leading to EU membership in 2004, and the latter among other things to 65% of the population holding a digital ID card with facilities for electronic identification of persons and digital signatures (Madise et al., 2006, pp. 4, 8).[10]

In October 2005, Estonia was the world's first country to allow all citizens to vote via Internet in an election. The roll-out in the local elections was considered a success, and the national election in 2007 was again "e-enabled". Two reports were issued on the 2005 election (Breuer and Trechsel, 2006; Madise et al., 2006). On June 27, 2006, I had an informal conversation with Tarvi Martens, project leader of the e-elections. Both reports and conversation served as background material for this section.

History of e-voting

In Estonia, the voting system for both local and national elections is based on proportional representation. E-voting was heavily debated before it was introduced (Drechsler, 2003; Madise et al., 2006). The main goal of the project seems to have been the modernisation of the country, which was already taking place in many different fields. People disagree about whether increasing turnout was an aim. The Local Government Councils Election Act was adopted by parliament on March 27, 2002, stating that from 2005 onwards, people had the right to vote electronically and remotely (Madise et al., 2006, p. 15). Traditional means remained available as well.

Wolfgang Drechsler extracted the following concerns from the parliamentary debate (Drechsler, 2003, p. 5):

1. Equality of citizens in political life – "unfair" towards non-connected citizens / digital gap;
2. Detriment to democracy (going to the polling station would be a valuable action by itself);
3. Unconstitutionality of e-voting (secrecy, generality, and uniformity);
4. Privacy and secrecy of voting not guaranteed;
5. Security of electronic voting systems not sure;
6. Proneness to fraud;
7. Negative or absent experiences in other countries;
8. The weakness of technical preparations;
9. The problem of hackers.

[10] Digital signatures are discussed in more detail in section 7.1.

On May 12, 2005, amendments were passed specifying the voting procedure in more detail, based on the technical solution that had been developed (Madise et al., 2006, pp. 17–18).

As far as can be discovered from the documents, the main theme in the Estonian discussion was coercion-resistance versus equality. People might be coerced or tempted to sell their votes in an unsupervised environment. In order to limit the secrecy and freedom problems of remote voting, it was thought appropriate to allow remote voters to change their votes as many times as they wished, including overriding the remote vote in a polling station on election day. In this way, a coercer would need to have control over her victim all the time to be certain of compliance. This regulation was specified in the 2005 amendment.

> "The right to change one's e-vote creates a so-called virtual voting booth: [a voter who has e-voted] under undesirable influence, can choose a moment when he or she is free to vote without outside influence. In order to guarantee freedom of voting, it is advisable to have the right to change one's vote on election day.
>
> With the same amendment, the Penal Code was also changed to exclude changing electronically given votes from punishable offences."
> (Madise et al., 2006, p. 19)

This partial solution to the problem of the secrecy and freedom of the vote can only work under a teleological interpretation of the requirement of secret voting in the constitution, i.e. that this requirement should be interpreted in terms of the problem it was meant to solve. Different means to guard against coercion would therefore also be appropriate. Also, the assumption was made that it was not primarily a task of the State to protect an individual against herself, so that collective voting and vote buying would not be a problem that needed solving (Drechsler, 2003, pp. 4–5).

However, some people, among whom president Arnold Rüütel, had a different problem with the new arrangements. They felt that those gave unfair benefits to the remote voters. It would allow e-voters to change their mind in the period between advance voting and election day, but not those who voted in advance by other means. The president refused to sign the law. The parliament then made another amendment, removing the opportunity to change one's vote on election day itself. The president again refused cooperation, and appealed to the Supreme Court to have the act declared unconstitutional. The Court, however, ruled differently.

> "The principle of uniformity can not be interpreted as a requirement that all voters must in fact vote in a similar manner. Uniformity means, first and foremost, the requirement that all voters have equal possibilities to influence the voting result." (Decision of the Supreme Court of Estonia, quoted in Madise et al. (2006), p. 25)

It must be noted that there is not much jurisprudence about the interpretation of the young Estonian constitution. In any case, the act was deemed to be constitutional,

and the president was forced to sign. Uniformity of means of voting may no longer be a requirement of elections.

The e-voting system

Estonia had a particular infrastructure in place to make the e-voting roll-out possible.

> "Preconditions for the implementation of e-voting were:
>
> 1. the existence of [a] legal basis;
> 2. widespread use of ID card that guaranteed all necessary means for e-voting – electronic identification of persons and digital signature;
> 3. the existence of electronic polling lists." (Madise et al., 2006, p. 20)

Also, early voting was already faily common in the country. Since Internet voting typically involves extended voting periods, this was another advantage. Note that both in the roll-out of ID cards and the existence of a central electronic polling register, Estonia is ahead of the other countries discussed in this chapter. The legal framework is different as well: only Estonia gives citizens the *right* to vote electronically.

The e-voting system is based on public key cryptography, which will be explained in chapter 7. The basic idea is to translate the procedure of postal voting to electronic equivalents. This means an "inner envelope" containing the vote, and an "outer envelope" containing the inner envelope plus a signed statement about who cast this particular vote. Indeed, as in the postal system, the secrecy of the vote depends on procedural measures to ensure that the one who opens the outer envelope does not also open the inner envelope. This suggests that the system is technically not very advanced. However, the analogy with postal voting makes it easy to demonstrate that it is *at least as secure* as postal voting, and makes the system easy to explain to the citizens.[11]

There is a procedure to verify that one's vote has been counted. However, not much attention has been paid to this feature in the evaluation, as opposed to for example the verification procedure in the Dutch RIES system, which will be discussed later.

Evaluation of the election

In general, e-voting in the local elections was evaluated positively, and its use was extended to the national elections in 2007.

> "No failures were found in the technical system of e-voting. No cases of buying e-votes have become public and no legal proceedings were initiated. The legitimacy of election results has not been contested by referring to e-voting." (Madise et al., 2006, p. 42)

[11] A remaining problem is how to "shuffle" the electronic votes, so that individual choices cannot be inferred from the order in which they were cast.

To critics, this will not prove that the system indeed worked correctly. A particular accusation was found in the media.

> "In the media the fact that elderly people e-voted by themselves has been put under dispute. However there is no evidence to prove this statement. It should be mentioned that according to law it is allowed to assist voters if he or she is unable to complete the ballot himself or herself." (Madise et al., 2006, p. 42)

Breuer and Trechsel conclude in their Council of Europe evaluation report that younger voters, voters with good computer skills and voters that trust the e-voting system are more likely to cast e-votes. Language is a factor as well: the Russian-speaking population hardly e-voted, Estonian being the official language of the e-voting system. The option of e-voting did not significantly increase the participation among "structural abstentionists". Only few people in Estonia are concerned about the loss of rituals in e-voting. Breuer and Trechsel conclude that e-voting is neutral with respect to gender, income, education and type of settlement, and does not have a political bias either (Breuer and Trechsel, 2006).

The flexibility of a young democracy and a small community may be a factor in the success of the system: it makes cooperation easier, for example with respect to communication about the project and the adaptation of the legal framework. Besides, there is a pragmatic attitude towards questions of security: the system does not need to be perfectly secure, as long as it is secure enough, and also understandable for the voters.

A concern is the accessibility of the system. Only few Estonians have the equipment to connect their digital ID card to their computer. Using passwords instead of ID cards is not considered secure enough. In the local elections, 9317 voters used e-voting, which amounts to 1.85 % of the people casting a vote (Breuer and Trechsel, 2006). In the national elections in 2007, these numbers rose to 30,275 or 5.4 % (OSCE Office for Democratic Institutions and Human Rights, 2007b). Allegedly, many people used the electronic capabilities of their ID card for the first time in order to cast an e-vote.

Estonian concerns

Estonia is the world's first country to allow Internet voting for all citizens. The main issues around which the discussion in Estonia has developed are the secrecy and freedom of the vote, in combination with the demand that people have equal access to voting procedures (uniformity). Polling place e-voting has never been used.

2.3 Get Britain to the polls

The British political system is a particular one in Europe. There is the predominantly appointed – not elected – upper house, the House of Lords. After the Labour party

reforms since 1997, there exist a parliament of Scotland and assemblies in Northern Ireland, Wales and London – but not England. Most elections use first past the post in single-member constituencies, but the use of other systems, such as proportional representation and single transferable vote, has increased under the reforms.

Pressure for more reforms is high. Campaigns exist for an elected upper house[12] and an English parliament[13]. In autumn 2006, some initiatives were combined in *Unlock Democracy*[14]. Within this – some would say – archaic but currently dynamic system, the technology of voting is under revision as well.

History of the ballot and the tracing requirement

The transition from viva voce voting to the ballot in the UK is well-documented (Asquith, 1888; Gross, 1898; Park, 1931). It took forty years, from 1832 to 1872, for the discussion to stabilise in the passing of a bill. Many felt that the secrecy of the ballot was "inconsistent with the manly spirit and the free avowal of opinion which distinguished the people of England." (Park, 1931, p. 56). It was often thought that the ballot was "un-English" and had never been used in the country, even though evidence was available for the contrary (Gross, 1898).

Against the main advantage, freeing the voters from coercion and other forms of influence, other counterarguments were raised.

> "*If there is ballot there can be no scrutiny*, the controlling power of Parliament is lost, and the members are entirely in the hands of returning officers [officials responsible for elections, WP]. A representative will not be able to tell who are his instructors (i.e. the persons who elect him). People who do not wish to be suspected of voting on the wrong side will stay away. Ballot and universal suffrage are apt to be coupled, and universal suffrage will mean that the poor will gain everything and ruin everything." (Park, 1931, p. 61, emphasis added)

> "The principal objections which have been advanced against the ballot as applied to our elections are, that the act of voting is a public duty and should involve a public responsibility; that it would lead to hypocrisy and deception; that it would do little to restrain the practice of treating; that it would encourage bribery by making it more difficult to detect; that it would be wholly inoperative in the case of spiritual intimidation such as that which is allowed to exist so extensively in Ireland; that it would afford facilities for personation." (from the report of the select committee on the election, *Times*, March 17, 1870, quoted in Asquith (1888), p. 662)[15]

[12] `http://www.electthelords.org.uk`
[13] `http://www.englishdemocrats.org.uk`
[14] `http://www.unlockdemocracy.org.uk`
[15] More recent research also indicates the possibility that vote buying can "survive the secret ballot" (Brusco, Nazareno, and Stokes, 2004).

Also, experiences from America were brought in to criticise the need for the ballot.

One of the most important objections to the ballot, in light of current controversies on electronic voting, is the supposed lack of verifiability when using ballots. Votes cannot be traced back to the voter, so one cannot know by looking at a ballot if it is legitimate. This led the select committee on the election to recommend that "the secrecy of the ballot should be inviolable, except in the case of any voter who is found guilty of bribery, or whose vote, in due course of law, has been judged invalid."[16] Such an arrangement would maintain the possibility of scrutiny in case of irregularities in an election: an investigation could take place not only into the accuracy of the counting, but also the legitimacy of the individual votes. Against the scrutiny argument, it was countered that "[p]arliament would be better off without the unprofitable duty of scrutiny" (Park, 1931, p. 61).

Some people were "averse to secret voting" (p. 64), whereas others were "pleading for a trial of ballot at one election, and promising, in case it was not liked, to say no more upon the subject" (p. 65). In a first attempt to get the new method of voting legalised, Mr. Daniel O'Connell "justified this tentative experiment by the need of experience and the natural dread of a sweeping measure" (Asquith, 1888, p. 658).

It took many accusations of coercion and bribery in elections, and the adoption of laws on extending the suffrage, to create finally a majority in Parliament in favour of the ballot. Even then, the House of Lords rejected the bill at first. "But it was strange to see the House pass a second reading and in committee make secret voting optional." (Park, 1931, p. 82) To the *Spectator*, "it was neither fair nor politic for them to pass an amendment which meant publicity for all but those who needed no secrecy." The notion of optional secret voting reappears with full force in the discussion of remote electronic voting: is it enough to give the citizen the *opportunity* to vote in secret, like in Estonia?

In the end (1872), the Lords passed the bill with two amendments: added scrutiny, and a limit on the measure of 8 years. The act was made permanent afterwards, but the British still have to cope with the issue of scrutiny in their election system, as we will see in the next chapter.

In the discussion on the introduction of the ballot, a fear was pronounced that turnout would fall with secret voting. The elections would be too orderly (and therefore not exciting enough), and there would be no possibility to publish intermediate results to convince people to come and vote (pp. 84–85). After more than a century, the fulfillment of this prediction – although not necessarily connected to the ballot – led to another change in voting procedures.

The Electoral Commission and the e-voting pilots

In the UK, the Electoral Commission was established in 2000, among other things to give advice on modernising the voting process. Since the introduction of the ballot, voting procedures had remained largely unaltered, and people were dissatisfied

[16] From the report of the select committee on the election, *Times*, March 17, 1870, quoted in Asquith (1888), p. 663.

with the archaic system. From that year onwards, an experimental approach to modernising the process, including e-voting, has led to various pilots in local elections. The focus of the experiments was the evaluation of ways of casting vote that would make the experience more convenient for the voter. The focus, therefore, was on remote electronic voting.

Pilots with e-voting were conducted in 2000, 2002, 2003, 2006 and 2007. Local authorities can apply to the central government with a proposal for a pilot, usually in combination with a technology supplier. Next to polling place and remote e-voting, pilots have also been run with all-postal voting. Also, from 2000 onward people do not have to specify a reason to request a postal ballot (postal voting on demand).

A major drive for implementing changes in voting was the dramatic decline in turnout after the 1997 election (Storer and Duncan, 2005). It is hoped that by offering more options to voters, more people will be likely to cast a vote. "The vision of e-voting is not one of a sudden switch over to a new technology. Rather, the vision is one of a phased move to multi-channel elections in which voters are offered a range of means by which to cast their vote and choose the mechanism that most suits them." (Pratchett, 2002, p. 4) It is unclear whether there has been a significant increase in turnout in the pilots. It is generally agreed upon that all-postal elections can experience increased turnout, but the effect of electronic channels is more controversial. Voter apathy may be a more important problem than lack of time or inconvenience, but then why *does* turnout increase in all-postal elections?

Apart from turnout, modernisation was mentioned as a second reason for considering electronic forms of voting. This includes both modernisation from the point of view of administration and from the point of view of the citizen. The "lifeworld" argument states that voting should be compatible with the everyday life of citizens, because they may otherwise lose their interest. An opposite argument says that voting should remain special, otherwise it will lose its particular appeal and turnout may even decrease further.

The hope was that e-voting could be used in a (nationwide) general election around 2010.

The Birmingham incident

After the 2004 local elections on June 10th, six councillors of the Labour party were found guilty of fraud with postal ballots in two wards in Birmingham. According to judge Richard Mawrey, the postal system used was "wide open to fraud".[17] This case of fraud, the judge stated, would "disgrace a banana republic". The persons involved allegedly managed to get their hands on thousands of blank postal ballots and had them completed to their wishes. It was ordered that the elections in the two wards be rerun.

This incident, even though local in scale, sensitised the media to problems with the pilot schemes, and had a major influence on the framing of discussions on the pilots afterwards. The problems with the postal system were the most important

[17] `http://news.bbc.co.uk/1/hi/england/west_midlands/4406575.stm`

reason for the limited pilots in 2006. E-voting was not deemed to be appropriate, because the problems with postal voting had to be solved first.

Because the pilots in the UK are about increasing turnout, convenience for the voter is very important. In case this leads to reduced security, as in liberalised postal voting with reduced authentication requirements, decisions will have to be made on where to draw the line. This will be an important theme in future pilots.

Criticism of the pilots

Not all experts have been happy with the way in which the government pursued modernisation of the voting process. The so-called "Technical Options Report", by Ben Fairweather and Simon Rogerson of the Centre for Computing and Social Responsibility of De Montfort University, identified major problems in the technical realisation of remote e-voting, similar to the report by Jefferson et al. (2004) in the US. Apart from that document, there have been no systematic efforts to try to slow down or halt the process through a media offensive, but people such as Jason Kitcat, Louise Ferguson and Ian Brown follow the developments critically. In 2007, major problems with the new pilots were reported (Open Rights Group, 2007; Electoral Commission, 2007).

British concerns

The main reason for the British to start e-voting pilots is the drive to increase easy availability of voting methods to the citizens. This has led to concerns in terms of authenticity of remote votes. Verifiability and secrecy are also mentioned.

2.4 Give Amsterdam back its ballot boxes

The Netherlands are a constitutional monarchy, and have a system of proportional representation for local and national elections. Universal suffrage is in place since 1917 (male) and 1919 (female).[18]

There is no registration procedure. Eligible people receive a polling card by mail a couple of weeks before the elections. This polling card is handed in at the polling station. One can be asked to present identification, but the general feeling is that this hardly ever happens. When voting was limited to the local polling station, one could also vote with a passport instead of a polling card. Now that experiments are being run with voting in any polling station within the municipality, this is not possible anymore, because there is no central voter register. This has led to some complaints in recent elections by people who lost or forgot their polling cards.

Particularly noteworthy is the liberal policy for voting by proxy. Since 1928, the option of "stemmen bij volmacht" (voting by proxy) exists: one can authorise other

[18] I have not been able to find information on the introduction of the ballot in the Netherlands. It has been suggested though that part of the inspiration for the transition to the ballot in the US came from Holland (Nutting, 1948, pp. 183–184).

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. It is not necessary to register a proxy vote; one simply signs the polling card and hands it to the designated proxy.

Since 1983, Dutch citizens living abroad, or having job duties abroad during the elections, are allowed to vote by postal ballot. The postal ballot needs to be accompanied by a signed statement and sent to the election office in The Hague or a special office in the country of residence. A (manual) procedure is invoked before counting the votes to guarantee the secret ballot, even in presence of a signature in the same envelope. Postal voting is not allowed within the country.[19]

Certification of electronic voting

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 during elections. It is said that little attention was given at the time to security and verification possibilities. The main issues were related to the usability of the machines, especially for elderly people. How the votes were counted and how the result was calculated did not seem to be of much public interest.

Since 1997, regulation on voting machines exists, including an extensive list of requirements that voting machines have to meet ("Regeling voorwaarden en goedkeuring stemmachines"). Demands on the verifiability of the counting, however, largely remain unspecified. Moreover, criteria for software that calculates the results from the totals of the individual machines have not been assessed at all. In 1999, local authorities were even reported to have used self-written software for this purpose (Expertise Centrum, consultants voor overheidsinformatisering, 1999).

Voting machines in the Netherlands have to be approved by an evaluation institute. Although multiple institutes could be designated in principle, only TNO has been involved in this procedure thus far. Only TNO (the department doing the evaluation now being called BrightSight) gets the source code of the software running on the machines, and the evaluation reports are not public either.

The full requirements specification, consisting of 14 sections, can be found as an appendix to the regulation. I quote and translate the items from section 8: Reliability and security of the voting machine.

1. The vote stored in the vote memory of the voting machine is the vote cast and confirmed by the voter;

2. A cast vote cannot be lost due to breakdown of the energy supply, failure of one

[19] Source: www.parlement.com, an excellent site on Dutch politics (in Dutch only, alas)

component, the specified environmental conditions, normal use or mistakes in the operation of the voting machine;

3. The read-in lists of candidates are maintained completely in case of breakdown of the energy supply, the specified environmental conditions, normal use or mistakes in the operation of the voting machine;

4. The functions of the voting machine are maintained completely in case of breakdown of the energy supply, the specified environmental conditions, normal use or mistakes in the operation of the voting machine;

5. 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;

6. 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;

7. The way of vote storage does not enable possibilities to derive the choice of individual voters;

8. 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;

9. The voting machine may have functions which are not described in the Election Law, the Election Decree, or this appendix, as long as they do not impair the required functionality of the voting machine and are related to the voting procedure.

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

The most widely used voting machines are produced by the company Nedap. These are so-called full-face DREs, with a button for each candidate. The verification possibility that these machines offer is the comparison of the votes per candidate to the votes per party, and to the total number of votes cast. This check, however, is based on votes that have already been processed by the machine. There is no paper trail. More recently, touch-screen based systems marketed by the former state press Sdu have also been used, notably in Amsterdam.

The niches of expats and water boards

In the Netherlands, several experiments have been performed with voting via the Internet. During the European elections 2004, Dutch citizens living abroad were allowed to vote online. Moreover, elections for two water boards have combined

postal ballots with Internet voting in fall 2004, with a total of 120,000 actual online voters.

Expats vote online

The first of the two experiments in the Netherlands was initiated by the Ministry of the Interior and Kingdom Relations. The experiment 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,[20] and a law regulating the experiment was passed through parliament.

The main setup of the system is as follows (Expertise Centrum, consultants voor overheidsinformatisering, 2000). Voters register by ordinary mail, and choose their own access code as password. In return they receive 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.

The system was designed by Logica CMG. However, the government demanded the transfer of the intellectual property rights of the source code with the system. This made it possible to publish the source code after the elections. The source code zip file, published on the website www.ososs.nl, contained all Java code written specifically for the online voting system. Code that was part of general Logica CMG technology was not open source. This meant that it was only possible to inspect the (partial) source, not to compile and run it. A fully open-source version of the system has been developed later by Joe Kiniry and colleagues from Trinity College Dublin (Kiniry, Morkan, Fairmichael, Cochran, Chalin, Oostdijk, and Hubbers, 2006).

A follow-up trial was conducted in the national elections in 2006. However, the system used was different.

Rijnland Internet Election System

A somewhat more sophisticated system, called RIES, was developed with far less money by the water board of Rijnland[21] together with two companies cooperating under the name TTPI[22]. 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 has been conducted in the regions Rijnland and Dommel in 2004, with 1 million eligible voters. 120,000 people voted online, but turnout did not increase.

[20] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2004), see also `http://www.minbzk.nl/persoonsgegeven_en/kiezen_op_afstand`, consulted October 11, 2005.

[21] `http://www.rijnland.net` and `http://www.rijnlandkiest.nl`, consulted October 11, 2005.

[22] `http://www.ttpi.nl`, consulted October 11, 2005.

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. The Radboud University Nijmegen did such a recount for all elections in which the system was used, and confirmed the official results (Hubbers, Jacobs, and Pieters, 2005).

Because the water boards are not bound by the Dutch election law, they are relatively free in their means of voting. In 2008, all water boards intend to use the RIES system in their combined elections. RIES was also used in the second KOA remote voting experiment during the national elections in 2006, instead of the Logica CMG system from 2004.

"We don't trust voting computers"

There have been some minor incidents and accusations during the history of electronic voting in the Netherlands before 2006. In 1998, it was found that the machines led to a competitive advantage for the numbers 31 of the candidate lists of the parties. Due to space restrictions, these were placed in the top of a second column, next to the candidates heading the lists. Also in 1998, Hans Janmaat of the right-wing extremist Centrum Democraten accused the voting machines of deliberately reducing his number of seats.

Criticism of the obscurity of the election procedure when using voting machines has raised after 2000. Main reasons were the secrecy of the source code and the evaluation reports, and the lack of verifiability. Attempts to retrieve the source code of the machines via the "Wet Openbaarheid van Bestuur" (Freedom of Information Act) failed, because the source code is intellectual property of the producer. But after Ireland judged the Nedap machines they bought unfit for use in the elections,[23] 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, a chain of events completely changed the e-voting battleground in the Netherlands. Main players are the people of the pressure group "Wij vertrouwen stemcomputers niet" ("We don't trust voting computers"), founded around June. They managed to get hold of a couple of Nedap voting machines, 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 (Gonggrijp, Hengeveld, Bogk, Engling, Mehnert, Rieger, Scheffers, and Wels, 2006). 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. Due to the lack of verifiability features, such attacks could go unnoticed: the machine would be able to perform according to its own will. The second main problem shown was the possibility to eavesdrop on

[23] `http://www.cev.ie/htm/report/first_report.htm`, consulted February 21, 2007.

the voting machine via a tempest[24] attack. Tempest involves listening to so-called "compromising emanations", i.e. radio emission from the device, in this particular case the display. Also, they found problems with the security of the storage facilities where the machines are 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, but the public bought it), 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 (see page 34). Nonetheless, the minister suspended the certification for the Sdu machines three weeks before the elections, because the Election Law requires that machines are certified only if the secrecy of the ballot is guaranteed. 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.

There was some discussion about whether eavesdropping on election day was such a realistic scenario that it would justify the suspension. In any case, the pressure group was very happy to have a major event that backed their concerns, even though the focus had shifted from verifiability to secrecy. And the minister was happy to have created an image of a decisive government. One of the other things the pressure group achieved is the change of the term "voting machine" into "voting computer", which may be decisive in public perception issues.[25]

Another concession of the minister was the initiation of a commission of independent experts, who would look into the future of e-voting after the elections: the Election Process Advisory Commission.[26] The commission was to report before October 1, 2007. The elections for the provinces took place in March, and it was not very likely that substantial change could be implemented before that date.

In the beginning of 2007, there was an attempt to re-certify the Sdu machines for

[24] Also written TEMPEST, supposedly being an acronym for Telecommunications Electronics Material Protected from Emanating Spurious Transmission or something similar.

[25] The associations people have with the term "machine" may be quite different from those they have with the term "computer". This would be an interesting topic for empirical validation.

[26] The members of the committee were: mr. F. Korthals Altes (chairman), prof. mr. J.M. Barendrecht, prof. dr. B.P.F. Jacobs, C. Meesters and M.J.C. van der Wel MBA.

the elections for the provinces. However, machines with reduced radio-emission turned out to be unreadable for the colourblind, and Sdu had apparently made mistakes in the machines delivered to the testing agency. In the end, the minister extended the suspension. Sdu demanded a new test in a court case, but the machines failed the test again.

The Ministry of the Interior and Kingdom Relations explained their point of view on the controversy on their website. They stated that apart from the secrecy problem due to the tempest attacks, the security of the machines is acceptable. They argued that in the Dutch proportional system, as opposed to the Anglo-Saxon district-based system, small numbers of votes will not have any major influence on the result. Besides, existing guarantees were thought to be sufficient in order to prevent fraud.[27]

In March 2007, the Organization for Security and Co-operation in Europe (OSCE) reported on the Dutch elections (OSCE Office for Democratic Institutions and Human Rights, 2007a). In April, another report was published, this time addressing the history of the e-voting problem (Hermans and Twist, 2007). Both reports argued for increased verifiability, by means of a paper trail or equivalent procedure. It was not made clear what kind of procedures would count as equivalent.

On September 27, the Election Process Advisory Commission reported on the future of the electoral process in the Netherlands (Adviesommissie Inrichting Verkiezingsproces, 2007). 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.

Dutch concerns

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. Secrecy has become a major issue due to the tempest attack, and is also the main reason for the reluctance to increase the use of Internet voting.

[27] `http://www.minbzk.nl/onderwerpen/grondwet_en/verkiezingen_en/stemmachines`, consulted February 13, 2007.

2.5 Conclusions

Electronic voting is one of the most interesting examples of the use of security-sensitive information technology in society. Democracy is one of the foundations on which western culture is built, and it is no wonder that the introduction of new technology into this domain has raised a considerable amount of discussion. Controversies are strengthened by the media coverage of security leaks and viruses in many different information technology applications, and by the vision of Internet voting as a possible future election platform.

In the US, problems with existing voting technology are a major factor in the transition to electronic systems. This was never the case in the Netherlands. Both in the Netherlands and in Estonia, modernisation seems to have been the most important issue. In the UK, the e-voting pilots are about increasing turnout.

These different histories have induced different concerns in relation to electronic voting. Can we still find a list of requirements of voting systems that applies to all countries? On a very high level of abstraction, there seems to be consensus about the importance of the following aspects:[28]

1. Availability: All eligible users can vote (with the same effort);
2. Authenticity[29]: Only eligible users vote, and they only vote once;
3. Correctness: All votes counted are valid votes, and all valid votes are counted;
4. Verifiability[30]: Results can be scrutinised by involved actors;
5. Secrecy: A voter can (or must) keep her vote secret.

When it comes to deciding whether a particular (type of) system satisfies these properties, people do not agree so strongly. Whether Internet voting can meet the secrecy requirement at all is unclear, and often depends on the way of interpreting existing laws. Many people believe only a paper trail can make e-voting satisfy the verifiability requirement. Companies develop fully electronic systems that they claim to be verifiable. Scientists criticise the companies, but they too develop fully electronic systems that they claim to be verifiable.

Also, the relative importance of the requirements seems to be different in each of the countries. Availability and secrecy are emphasised in Estonia. Correctness and verifiability are on the foreground in the US and the Netherlands, although the tempest attacks and Internet voting experiments have put the secrecy issue on the

[28] Similar lists are found in Pieters and Becker (2005) and Pasquinucci (2007).

[29] In this thesis, authenticity refers to the property that all votes can be attributed to legitimate voters (without disclosing the relation to others). Authentication, which is sometimes mentioned as a security attribute, is reserved here for the *process* by which authenticity can be achieved: having people prove their identity before allowing certain transactions.

[30] Verifiability is closely related to the more general security property of accountability. Both refer to the possibility to trace the flow of information in a system. Verifiability is the dominant term in voting system sciences, and I therefore adopt it in this book.

Dutch agenda as well. In the UK, the focus is on availability and authenticity. What do such differences mean for the future of e-voting?

Thanks to documented evidence from the US and the UK, we can be aware of the discussions on the transition from oral voting to paper voting. We find that this process took a long time to complete, even though the benefits of the paper ballot seem obvious to people in our time. At first, people supported or opposed the paper ballots for reasons that we now consider dubious. Still, some arguments were similar to those used by critics in the e-voting debate. If we compare this transition to the current debate on electronic voting, we should become critical of any attempt to end the debate within a year or even within five years. Instead, the cultural framework takes time to adapt.

Comparing different countries also leads to a critical attitude to claims that security properties of voting systems are fundamental and cannot be subject to discussion. Instead, different countries have different political systems, different voting systems, different attitudes towards trust, and these come with their own security requirements (Kersting, Leenes, and Svensson, 2004). Even if agreement can be reached on the high-level requirements I mentioned, this does not imply that they mean the same thing in different cultures. Besides, there is a lot of path dependence concerning choices made in the past. Liberal proxy voting in the Netherlands, limited secrecy in the UK, liberalised absentee voting in the US, all these provide different cultural starting points for the debates. In that sense, there is probably no single e-voting solution, as there has never been a single type of ballot.

The results of this overview study suggest that e-voting controversies are dependent on history and culture. Different backgrounds will lead to different expectations, institutionalisations and learning processes. In the next chapter, I will investigate these differences in more detail for the UK and the Netherlands.

Chapter 3

The Cultural Construction of Controversy

"Always vote for principle, though you may vote alone, and you may cherish the sweetest reflection that your vote is never lost."

– John Quincy Adams (6th US President, 1825-29)

In this chapter[31], we zoom in on the e-voting discourses in two countries. To investigate possible reasons for differences in discussions on e-voting, a qualitative comparative case study on the e-voting discourses in the UK and the Netherlands was performed, based on the theory of strategic niche management (Weber, Hoogma, Lane, and Schot, 1999; Hoogma, Kemp, Schot, and Truffer, 2002). In each of the countries, eight e-voting experts were interviewed on their expectations, risk estimations, cooperation and learning experiences. The results suggest that differences in the discourses on e-voting, as identified in the previous chapter, can indeed be attributed to these variables to some extent, from a qualitative point of view.

The theory of strategic niche management identifies variables that guide the dynamics of the development of new technologies, which can explain differences in discussions on e-voting. In relation to the previous chapter, which was descriptive, this chapter has an explanatory function, and tries to relate the differences between countries to the variables of the strategic niche management theory.

[31] A different version of this chapter, which was joint work with Robert van Haren, will be published in the *Journal of Information, Communication and Ethics in Society*. An extended version has been published as Pieters and van Haren (2007).

3.1 Method

In both the UK and the Netherlands, 8 e-voting experts from different backgrounds were selected for interviews. In each of the countries, we spoke to 2 government executives, 2 critics, 2 academics, 1 political expert and 1 technical designer. In the UK, these included:

- John Borras, OASIS technical requirements committee;
- Paul Docker, Department of Constitutional Affairs;
- Peter Facey, director of New Politics Network;
- Ben Fairweather, Centre for Computing and Social Responsibility; De Montfort University;
- Louise Ferguson, usability expert and critic;
- Jason Kitcat, technical expert and critic;
- Peter Ryan, Centre for Software Reliability, University of Newcastle upon Tyne;
- Alan Winchcombe, Association of Electoral Administrators.

In the Netherlands, the following participants were selected:

- Kees Aarts, professor of Political Science, University of Twente;
- Esther Beneder, Ministry of the Interior and Kingdom Relations;
- Rop Gonggrijp, technical expert and critic;
- Maarten Haverkamp, Christian Democrat MP;
- Peter Knoppers, technical expert and critic, Delft University of Technology;
- Piet Maclaine Pont, designer of the RIES Internet voting system;
- René Mazel, substitute director Constitutional Affairs and Law, Ministry of the Interior and Kingdom Relations;
- Berry Schoenmakers, cryptography and e-voting expert, Eindhoven University of Technology.

The questionnaire[32] (see appendix A) contained open questions based on the theoretical framework of strategic niche management (Hoogma et al., 2002). This theory is particularly useful for investigating the introductory phase of new technologies, which are usually deployed in a relatively small and protected environment, called a niche.

[32]The questionnaire was designed after the founding of the activist group in the Netherlands, but before the report on their analysis of the Nedap machines (Gonggrijp et al., 2006).

This has been the case for Internet voting in both countries. Main variables in this framework are expectations, cooperation and learning experiences. For purposes of clarity, the variable expectations was split into (positive) expectations and (negative) risk estimations. The interviews were performed either by phone or on-site in the period of October - December 2006. Each interview lasted between half an hour and one hour.

A qualitative analysis of the interview data was performed using the Weft QDA tool.[33] The main variables were refined based on the data, and connections between them were identified. The results are presented below, in sections for each main variable. English translations of Dutch quotes are the responsibility of the present author.

3.2 Expectations

UK

Based on the interviews, it can be concluded that the most common expectation of the e-voting pilots in the UK was that they would increase turnout. The country experienced falling turnout levels, and there was a strong political motivation to stop or reverse this trend. It was thought that modernising the voting process could help in achieving this goal. This clear goal was not appreciated by all of our participants, and critics do not believe that e-voting will boost turnout. Peter Facey: "People tried to find a technical solution to the question 'Why don't people participate in elections?' In the end, it was a political question, not a technical one."

Because of the expectation of increased turnout, the experiments in the UK have focused on making it easier for the citizens to vote. Electronic voting machines at polling stations are not expected to increase turnout, and are therefore not likely to be introduced in the UK. However, the critics of e-voting think precisely of e-voting at polling stations as the only possibly acceptable form, because remote e-voting is done outside a controlled environment, and there can be problems with Internet security. The government, though, is not planning to abandon remote electronic voting.

Other, less pronounced expectations of the e-voting pilots in the UK include easier and cheaper election administration, improved accuracy and making voting fit in people's lives. People who do not believe in increased turnout for remote electronic voting usually offer what can be called the "lifeworld argument". John Borras argued that e-voting is "a necessary development to keep voting up-to-date with people's daily lives." In the UK, four of our respondents mentioned this issue, although it applies to far less text than the turnout matter. Easier administration and improved accuracy have been the drive behind the introduction of e-voting in other countries. In the UK discourse, they tend to be seen as side issues. If they were major topics, electronic voting machines at polling stations might have been a more attractive option.

[33] Weft QDA // A free qualitative analysis software application. Available online: http://www.pressure.to/qda, consulted May 14, 2007.

The quest for turnout has been translated into experimentation with multiple channels, e.g. Internet, digital TV, SMS. The idea is that the more choice the voter has in selecting a channel that is convenient to her, the more likely she is to cast a ballot. According to Alan Winchcombe, research indicates that voters want such a choice. The use of multiple channels leads to different views on security. Multiple channels may both increase and reduce the risks. Ben Fairweather: "On the one hand it may reduce risk, because there is no single point of failure. On the other hand, it may increase risk, because there are multiple ways to attack the system." Another issue that was raised is the balancing of security between the channels. This is a variant of the well-known equal access argument, stating that changing the voting procedures should not benefit certain groups in society more than others. John Borras: "The security should be balanced among the different channels. If some channels are more secure than others, this leads to inequality, which is undesirable."

Netherlands

Most of our Dutch respondents agree that voting machines in polling stations have advantages in terms of efficiency of the process and accuracy and prevention of errors by the voter. René Mazel: "In the paper voting system, there were about 5% votes that had to be checked afterwards because they had arrows and notes on them. 0.5% to 1% remained as invalid. With the voting computer, the number of invalid votes has been reduced to almost zero. On the other hand, the computerised process is much more central. If the programmer makes a mistake, this counts across the board."

Whether the benefits justify introducing electronic voting is a major question. As opposed to the UK, there was no clear problem in the Netherlands that had to be solved. Even if turnout may have been slightly lower in some elections, this was not seen as a major issue. According to Rop Gonggrijp, "there is no need to automate the voting process." Both the turnout and lifeworld arguments hardly seem to play any role in the Dutch discussions.

Internet voting in the Netherlands is mostly seen as an addition to postal voting for citizens living abroad. Compared to postal voting, it is regarded as more transparent and more convenient. People can see if their vote has been counted, and people can participate on election day itself instead of in advance. Due to the focus on the comparison with postal voting, and the problems associated with voting in an unsupervised environment, implementation for a wider audience is only considered hesitantly. Esther Beneder: "Internet voting [...] is mostly like postal voting. Internet voting should therefore comply with the same rules as postal voting. It should be at least as reliable and accessible. Internet voting should therefore not be compared with other forms of voting."

Piet Maclaine Pont mentioned an additional problem: "According to the politicians, the disadvantage of Internet voting is that people who are disinterested in politics will be more likely to vote." A similar remark is made by Maarten Haverkamp: "Internet voting will indeed lead to higher turnout, because of convenience. However, the quality of the vote will not be better."

Comparison

The main drive behind the pilots in the UK is increasing turnout. This expectation has been translated into a vision of multi-channel voting, to make the experience as convenient as possible for the voter. This explains a lack of interest in voting machines. Other expectations, like improving accuracy and administration and the lifeworld argument are also mentioned, but seemingly to a lesser degree than in other countries.

In the Netherlands, there was no clear problem guiding the implementation of electronic voting. Key expectations of e-voting in the Netherlands are clearly separated between voting machines and online voting. For voting machines, the main expectations are increased accuracy and efficiency. For online voting, increased convenience for expats is the main drive. The idea that these benefits are important enough to justify e-voting is questioned by the opponents. E-voting is not primarily seen as means to increase turnout. Two of our respondents even question the desirability of increased turnout. Interestingly, no-one in the UK mentioned this objection against the possibility of higher turnout. Criticism was more oriented towards the lack of proof of increased turnout; not towards the desirability of increased turnout itself.

3.3 Risks

UK

Generally, the insight has spread that electronic voting is a risky technology. Many of the participants indicate that they have become more aware of the risks during their involvement. Opinions differ about which risks are the most important. We will cover the aspects of verifiability, authenticity and secrecy in more detail, since these seem to be the most important ones in the discussion.

The discussion on verifiability in the UK is judged to be different from that in other countries, notably the US and the Netherlands: Louise Ferguson: "In polling place e-voting, the most important technical problem to be solved is the provision of confidence that an individual's vote is cast in the right way, without the vote being revealed. The one way this has been arrived at so far is a voter verified approach. This concept has led to discussion in other countries, but not in the UK: no-one in authority has mentioned it or expressed a view on it." Ferguson refers to a so-called "paper trail", in which each individual vote is kept on paper next to the machine counting (Mercuri, 2002). It is fairly easy to explain why the paper trail solution is not that popular in the UK: because the UK wishes to increase turnout, the focus is on remote voting (which is clear to all participants), and in remote voting, a paper trail is impossible (see page 24).

The discussion on verifiability is closely linked to the discussion on the relation between system security and voter confidence. Many of our participants judge perception of security to be important, as opposed to reality. Peter Facey: "Perception in elections is equally important as reality. In the UK, the perception is that polling

station voting is secure, safe and reliable. The reality is you could walk into my polling station, say that you're me, be given a ballot paper, and vote. [...] The problem with new ways of voting is that even if it's more secure, perception may be different and there may be a lack of confidence."

Because of these issues, security requirements of electronic voting systems may be stricter than those of traditional voting methods. Peter Facey: "A higher threshold of risk is often applied to e-voting or remote voting than to traditional methods: the security of e-voting should be 'beyond doubt', whereas this is not the case for the polling station paper system."

An important consideration in remote voting is its unsupervised nature. In the UK, concerns around this theme have been oriented more towards personation than to coercion or family voting: voter identification is seen as a major issue. Both from the UK's history of weak authentication mechanisms, and from the incidents with postal ballots (such as in Birmingham), it seems reasonable that personation is a great concern in the UK.

However, our respondents do address the coercion issue. The proponents of e-voting quote figures from research indicating that the problems with voting under pressure are small. The critics are much more sceptical, and find remote voting unacceptable, especially in relation to human rights treaties. Jason Kitcat: "The legal problem is that remote e-voting and postal voting break the various human rights treaties (UN, Europe, UK). They do not meet the secret ballot requirement. The government is aware of this – it is now being investigated by the Council of Europe – but they do not seem to care about treaty obligations. Moreover, the British system is already problematic with respect to this requirement, because of the vote tracing possibility. This has been in place since the introduction of the paper ballot in 1872."

Here, we find another peculiarly British phenomenon. Indeed, the secrecy of the ballot in the UK can be broken by court order, due to the scrutiny requirements added by the House of Lords in 1872 (see page 30). There is a sequence number that can be used to trace the relation between voter and vote, although the physical separation of registration and votes does not make this an easy task. Peter Facey and Ben Fairweather are concerned that keeping the vote tracing requirement in e-voting makes it too easy to trace, and thus invites breaking the secrecy.

While the vote tracing requirement leads to these complications in e-voting, it also influences the discussion on secrecy in remote voting. If remote e-voting does not conform to the treaties, neither does the current British system, and no one is aware of legal challenges to that practice. The vote tracing option may be one of the reasons why the British are less concerned about the requirement of the secret ballot. Paul Docker: "The Council of Europe and the Venice Commission have looked at remote voting and e-voting and feel there is no legal issue with that."

Netherlands

In the Netherlands, the activists have finally managed to persuade the government to abandon the existing voting machines. Why did this not happen earlier? Berry Schoenmakers states that "risk is a calculated property of on the one hand the vulnerabilities and on the other hand the probability of exploitation. [...] The vulnerabilities in voting computers are big, but chances of exploitation in the Netherlands are minimal. That's why we can cope with the risks at this point."

The argument here is that the *context* is important for the security of the voting systems. In the Netherlands, recent experiences with fraud in elections are nearly absent. There was a small case of a candidate being a poll worker as well, and having an improbable number of votes in exactly that polling station.[34] Apart from that, people do indeed seem to have confidence in the limited likelihood of vulnerabilities being exploited. This may be a feature of the Dutch multi-party system: no single party will get a majority, and if they do, people will be *very* suspicious.

Beneder, Schoenmakers, Knoppers, Gonggrijp, Aarts and Maclaine Pont mention the issue of lack of transparency in voting computers. Opponents of the present e-voting systems mainly focus on open source[35] and the paper trail solution. Kees Aarts: "The ideal voting computer will need to be open source, and certainly also have a paper trail for recount purposes."

Generally, the discussion on the verifiability of voting computers seems to be almost completely separated from the discussion on the verifiability in the RIES Internet voting system. This may be due to the fact that the voting machine infrastructure has been in place for a long time, whereas Internet voting is relatively new. Also, different people are involved. Piet Maclaine Pont thinks that the anti-e-voting campaign may be beneficial for the Internet voting efforts. Piet Maclaine Pont: "The verifiability as demanded by Gonggrijp can be made a reality by RIES."

The recent discovery of the possibility of tempest attacks on the Dutch voting machines made the secret ballot appear on the agenda with full force. Contrary to the expectations of the pressure group, the main issue in the media was not the verifiability, but the secrecy of the votes. The issue of secrecy is also prevalent in the discussion of Internet voting, in the form of concerns about family voting. Esther Beneder: "Ensuring a secret ballot is a great concern. It is not possible to verify that people are not being coerced." The coercion issue is dominant over personation, and agreed upon by almost all respondents. It leads to reservations with regard to expanding the use of Internet voting. This may be explained from the very limited experience with postal voting. Human rights treaties were not mentioned in this context.

[34] Security.nl. Fraude met stemcomputer in Zeeland. July 6, 2006. Available online: `http://www.security.nl/article/13917/1`, consulted February 19, 2007.

[35] Meaning that the program code is available for public inspection.

Comparison

In the UK, the most pronounced risks of e-voting are personation and the lack of verifiability. Verifiability is mainly discussed in terms of voter confidence. The paper trail solution is not in focus, because of the lack of interest in voting machines. The focus on personation can be explained from the history of weak authentication in elections, in combination with recent incidents. The acceptability of remote voting under human rights treaties is questioned. There is a concern that the vote tracing requirement cannot be maintained in e-voting.

In the Netherlands, verifiability is considered an issue as well. Open source and paper trail are mentioned more often than in the UK, which can be explained from the widespread use of voting machines. Secrecy is dominant over authenticity, and is associated with tempest attacks on voting computers on the one hand, and family voting and coercion in remote systems on the other.

3.4 Cooperation

UK

Because of the district-based voting system in the UK, there can be a close cooperation between the local authorities, the local candidates and the local electorate. The local authorities have the initiative to apply to the central government for a pilot, together with a supplier. At the central level, advice is given by the Electoral Commission. There are some limitations to what the local authorities can do, as determined by the central government. They select the companies that the local authorities can contract. Some of our respondents are critical about this approach, mainly because there is no set of standards that the systems have to meet.

The issue of certification turns out to be a real bottleneck in the UK pilots. On the one hand, the central government states that the pilots are run precisely in order to make clear what kind of requirements should be included in the certification process. On the other hand, critics argue that doing experiments without proper certification of the systems being used is asking for trouble. The differences in opinion in the UK can partly be explained from attitudes towards and trust in the suppliers. If one believes the suppliers are competent enough to deliver reasonably well-designed systems, the need for a certification procedure is less strong than if one believes the technical expertise of the suppliers is insufficient.

The local authorities realise that they are dependent on the vendors. Alan Winchcombe: “I’m not a technical person; [...] to a certain extent you are totally reliant on the suppliers’ technical people being able to deliver and prove to you that what you’re asking them to do they are capable of doing.” With the government, the opinion is that enough technical expertise has been acquired to ensure the quality of the pilots and the ability to set up a certification procedure in the future. Paul Docker: “The pilots should reveal what it is that needs to be accredited and how that process might work. A system security consultant is helping with this. Also the people within

government working on system security are involved. Nothing will be introduced on a mainstream basis without having an accreditation system in place."

Academics hired by the government have contributed to the e-voting developments on a theoretical level (Pratchett, 2002). One report was particularly critical (Fairweather and Rogerson, 2002). Peter Facey: "There has been some impact on the pilots by some reports of academics in the UK, making it more difficult to go ahead." The evaluation of the pilots was done by the Electoral Commission rather than academics.

On a local level, there seems to be good cooperation with the media. Alan Winchcombe: "The local media help us very good with free publicity. Our feedback shows us that the local media is a significant source of information on what we're doing in this local area." However, most of our participants are critical about the coverage in the national media. It is said that, because the pilots are run on a local level, national media are only interested in major events, which usually means problems.

The media may contribute to a wider debate in society. This has not happened in the UK until 2006. People seem to be expecting something like that, in light of national and international developments. There is more communication among activists within the country, and campaigns have been started in other countries such as the Netherlands. Even though there is no systematic campaign, activists do seem to have some influence. Paul Docker: "Some people expect e-voting to create havoc, and all sorts of expectations need to be addressed. [...] They do not come from uninformed positions."

Netherlands

In the Netherlands, the local authorities are free to decide which voting equipment to use in polling stations, as long as it has been certified by the Ministry of the Interior and Kingdom Relations. Internet voting experiments have strong central steering. The Beverwijk local authorities were not allowed to pilot with Internet voting in the 2006 local elections, officially because the law could not be adapted in time.[36]

Opinions about the technical expertise in the Dutch process are very different, even among critics. Rop Gonggrijp: "There is no technical expertise with the suppliers at the moment. They have not done any research for years." Peter Knoppers: "The suppliers have enough knowledge about voting computers and their limitations. However, the problems with voting computers have been underestimated for a long time. Issues like transparency have never been thought about, so that this knowledge has not been turned into technology."

Certification for voting machines has been in place since 1997, but this meant that the list of requirements turned out to be incomplete or underspecified many years later. The current suspension of the certification of the Sdu voting machines is not due to a failure to meet the requirements; rather, the requirements were judged to

[36] Webwereld. Pechtold: Beverwijk mag niet online stemmen. October 13, 2005. Available online: `http://www.webwereld.nl/articles/37796/pechtold--beverwijk-mag-niet-online-stemmen.html`, consulted May 25, 2007.

be incomplete with respect to the law (see page 37). Piet Maclaine Pont: "Nedap and Sdu have always complied with the requirements posed by the Ministry." Maarten Haverkamp: "The roles have been reversed: now the suppliers have to prove that their systems are secure."

Next to the expertise of the suppliers, expertise is also required with the government and the politicians. Some of our respondents think that such expertise is increasing; others are less convinced. A generally acknowledged view is phrased by Rop Gonggrijp: "The government has slowly lost control over the elections, giving control to the vendors. The expectation is that the government will make the elections its own task again and that the vendors will only have an executive role." The recent involvement of the intelligence agency is seen as an indication for a more pro-active role of the government, no longer taking the existing requirements and the suppliers' expertise for granted.

This also means that the government is closely following the Internet voting developments, and these will have to conform to the law in detail. However, the law is still largely based on paper voting. Piet Maclaine Pont: "The Election Law regulates the voting process even on a practical level, particularly concerning polling stations and transport of ballots or data carriers. Obviously, the process will be completely different in case of Internet voting."[37]

Anti-e-voting activists spread the view that most people agree on the paper trail solution. Berry Schoenmakers thinks there are better solutions: "Politicians have introduced many organisational security measures for voting computers, instead of cryptographic measures." However, cryptographic systems should be more advanced than the present ones. "Initiatives like RIES are insufficient."

The Electoral Commission (Kiesraad) has a role in acquiring academic expertise for the voting process. Esther Beneder: "On a higher level, the Electoral Commission have visited various conferences. They look at the topic of Internet voting from a more abstract and long-term perspective." This is in stark contrast with the role of the British Electoral Commission, which is responsible for the evaluation of all local pilots. Kees Aarts suggests that the current modesty of the experiments in the Netherlands may be due to influence from science. "Developments in science are being followed carefully. If not, we would see even more of exceptional and diverse experiments."

Apparently, the media have been sensitised to the e-voting issue by the campaign. As in the UK, most of our respondents are critical about the media's ability to cover the whole process. Respondents in the Netherlands agree that the anti-e-voting campaign is a good thing, if only for the fact that it made people sensitive to possibilities to improve the system. Again, Internet voting is seen as a completely different matter. Esther Beneder: "Voting computers cannot be compared with Internet voting."

[37] The need for adaptation of the law was acknowledged by the OSCE report on the parliamentary elections (OSCE Office for Democratic Institutions and Human Rights, 2007a).

Comparison

In the UK, the initiative for the pilots is local, and there is currently no framework for certification. In the Netherlands, local authorities can use voting equipment that has been certified, but they cannot experiment with different methods of voting. The only available "niche" for experimentation are expats. The UK has the advantage that in a district-based system, elections are local by definition.

Judgements about technical expertise with the suppliers and the government are very different among actors in both countries. The Electoral Commission of the UK has been more involved than its counterpart in the Netherlands. The UK Electoral Commission is responsible for evaluating the pilots, whereas the Dutch "Kiesraad" only studies the processes on a more abstract level. In the UK, academics have been systematically involved in the process, mainly on a theoretical level. In the Netherlands, academics have mostly followed the developments from the sideline, although some were invited to participate in testing and evaluation.

These particular divisions of responsibilities between academics and the Electoral Commission may have had influence on the actors' positions in the debate. What are the consequences of the UK approach of having the Electoral Commission do the practical research, and consulting the academic community for more fundamental questions? It can be suggested that such an approach tends to polarise opinions in the academic world, whereas the Electoral Commission is encouraged to adopt a more pragmatic point of view. In the Netherlands, it may be the other way around.

In both countries, coverage by the media is appreciated, but they are said to be missing the bigger picture. The contribution by the anti-e-voting pressure group in the Netherlands is acknowledged by the various actors. Similarly, the UK government realises that the criticism is well-informed and has to be taken into account. In both countries, the vendors are said to have too much power over the process.

Changes in voting procedures may be more difficult to implement in the Netherlands due to the political situation. Because of the multi-party system, no single party will ever have the opportunity to implement its ideas about modernising the voting process without having to agree with other parties. The modernisation initiative by the Labour party in the UK would not have been possible in the same way in the Dutch system.

3.5 Learning

UK

According to Paul Docker, the pilots were successful, and provide a basis for going forward. "The DCA [Department of Constitutional Affairs] seeks to identify all the issues and risks, but if some are exposed by actually piloting, this is part of what the pilots are for." Many participants are critical about the ability of the government to

learn from the pilots.[38] Louise Ferguson criticises the pilots for mainly three things:

1. the government has not learnt from the pilots: they just run another pilot like the last pilot;
2. the reports of the pilots were very constrained, and problems were not mentioned in the published reports (only mentioned informally, in private conversations);
3. there is still insufficient time allowed for the roll-out of the new pilots.[39]

The government does not see any problems in doing more of the same, because this allows more learning to take place. Apart from identifying issues, there is also a clear educational goal in running pilots. What is needed to implement e-voting on a larger scale is people who understand what is going on. According to Alan Winchcombe, both political and technical expertise are improving because of the pilots.

Some of our participants think that learning about risks has made the government decide not to pilot in 2004-2005, and to have only limited pilots in 2006. According to the government, the reason is that they were not allowed to pilot in elections where local races were combined with national or European ones. In 2006, the focus was on solving the problems with postal voting, because of the incidents in Birmingham two years earlier.

Both national and international experience changed the expectations of e-voting, in terms of increased expectations and better risk estimations. Alan Winchcombe: "Certainly, when we had not done e-voting for two years because we weren't allowed to we had to do a reverse education program and go back to the voters and explain to them why we couldn't do it. We got a lot of feedback from voters who were very unhappy having been able to e-vote for two years in succession and having to go back to a polling place again." These remarks suggest that experiments are not just neutral means of assessing benefits and risks. Instead, the experiments lead to expectations on the continuation of similar services.

It seems that the main aspect of learning is the consciousness of the importance of the security of the systems. The consciousness of security threats often increases with the knowledge of the intricacies of electronic voting. Peter Ryan: "New tenders stress the importance of security a bit more than previous ones: the government seems to be more aware of security dangers."

Netherlands

In the Netherlands, as we have already seen, it took a pressure group to initiate large-scale learning in the domain of voting machines. With respect to Internet voting, the government will probably learn most from a comparison between the 2004 and 2006

[38] See also Pratchett and Wingfield (2004).

[39] In an evaluation of the 2002 pilots, the Electoral Commission already advised to give more time for the procurement process (Electoral Commission, 2002). Three of our respondents criticise the government for not addressing this issue.

experiments. Quite different systems were used. Of course, this hardly provides as much material as the British Electoral Commission has available.

Kees Aarts argues that the experiments with Internet voting have been inspired by the UK pilots. Meanwhile, the problems in US elections and the Irish criticism of the Nedap machines have challenged the existing Dutch e-voting solution. International developments, among other things, may lead to improvements in the Dutch voting equipment. René Mazel: "There is a gradual improvement of the voting computer. However, we are facing new leap now, partly because of the recommendations of the Council of Europe and the "energy" of Rop Gonggrijp. Because of the recommendations, people started thinking about a new generation of voting machines."

As for Internet voting, it is generally agreed upon that expectations have been reduced with respect to some years ago, and that there was too much technological optimism before. Voting in any polling station seems to be more likely than full-fledged Internet voting.

Comparison

In the UK, the pilots were set up with the explicit goal of learning. Some of our respondents are not satisfied with the learning curve of the government, especially when it comes to the time scale of the pilots. People have all kinds of explanations for why there were no pilots in some years, but the government states they were simply not allowed to pilot.

Since the requirements of voting machines were specified in 1997, the "paradigm" (Kuhn, 1962) in the Netherlands has remained largely unaltered, even though there were some "anomalies", especially the Irish criticism. After the launch of the activist group, a strong demand for new learning has emerged, which can be called a "revolution" in thinking about electronic voting. This revolution has led to a proposal for a completely new voting process. Still, compared to the British situation, the focus on learning appears to be less strong. It is mentioned far less often, if at all. The proposed new technology is seen again as something to be introduced, not something to be experimented with.

As for Internet voting, the experiments in the Netherlands have been more careful than in the UK. Although expectations were higher before, there does not seem to be a discontinuity in this development. There is more consensus in the Netherlands than in the UK about what future e-voting will look like. Most of our respondents do not see Internet voting happen on a large scale: it is not seen as a suitable alternative to the debated voting machines. In the UK, the government had the expectation of having an e-enabled general election around 2010, which would include remote voting.

variable	dimension	UK	Netherlands
background	voting system	district-based	proportional
	government	single party	coalition
	Electoral Commission	2000	1951
	postal voting	on demand	expats only, liberal proxy
expectations	drive	turnout	accuracy, efficiency, ease
	machine / remote	one issue	separate issues
	channels	multiple	single
risks	verifiability concerns	voter confidence	open source, paper trail
	authenticity concerns	personation	coercion
	privacy concerns	vote tracing	radio emission
cooperation	role of EC	practical	theoretical
	steering policy	decentral	central
	requirements	learn from pilots	voting machines only
	role of academics	reports	ad-hoc
	image of vendors	too powerful	too powerful
	image of media	sensationalist	sensationalist
	image of activists	valuable	valuable
learning	focus of process	pilots + learning	phased introduction
	starting point	open investigation	existing paradigm
	speed	gradual, slow	campaign, sudden
	consensus remote e-v	weak	strong
	future remote e-v	general election	no explicit plan

Table 3.1: Summary of results.

3.6 Conclusions

In this chapter, various similarities and differences were identified between the e-voting discourses in the UK and the Netherlands. The most important ones include the focus on turnout, authenticity versus secrecy, the role of the Electoral Commission, and the focus on learning through experimentation. The framework of strategic niche management has been helpful in categorising both interview questions and interview data. The results are summarised in table 3.1. To finalise the analysis, some considerations are given on the differences that were found with respect to the histories and political cultures of the countries.

First of all, the local nature of district-based elections seems to favour a pilot-based approach, since each district is easily perceived as a potential "niche". In the Netherlands, expats have been chosen as a niche instead, leading to more limited experiments and learning. Secondly, the UK's differences were identified between the e-voting discourses in the UK single-party governments have more opportunities for modernisation than the Dutch coalitions, in which at least two parties have to agree on the direction to be taken. Thirdly, the histories of the Electoral Commission and the Dutch Kiesraad are completely different, which may explain their different roles and attitudes. Fourthly, remote voting by postal ballot has been more accepted in the UK than in the Netherlands, which have focused on proxy voting instead. This makes the leap to Internet voting smaller for the UK. Relations between such cultural

variables are manifold, and many have been addressed in the comparisons in previous sections.

The results of our comparative study on e-voting indicate that conceptualisations of e-voting may differ between countries. It was shown that the differences in discussions on e-voting in the UK and the Netherlands can be partly explained from expectations, cooperation and learning experiences, which again are related to cultural and historic differences. If e-voting is seen as an issue of turnout, then remote e-voting is key, and a paper trail is not interesting. If voting computers and Internet voting are seen as different issues, then methods of verifiability in Internet voting are not discussed in the context of voting computers. If authenticity has been an issue in elections, then it will be even more so in e-voting, and possibly more important than coercion.

Such cultural differences imply that systems developed for use in a particular country may not meet the requirements in another. Requirements are specified in a discourse in which distinctions are made based on culture, rather than a universal frame of reference. Even though requirements are discussed at an international level, these standardisation and normalisation attempts are themselves part of a higher level discourse, in which certain concepts are more prevalent than others. This also holds for concepts with respect to security. Thus, security assessment seems to be dependent on articulation of specific security-related concepts, and these may be different depending on the context.

Intuitively, there is a second reason for security being culture-dependent. The *goals* of attackers trying to manipulate the systems may also differ between cultures, which leads to differences in importance of security measures. In the UK, the aim of election fraud may be to install a single-party government of the desired colour. In the Netherlands, the highest achievable end seems to be making one's own party the largest one, still requiring negotiations for a coalition. Thus, both from the perspective of the defenders and from the perspective of the attackers, there are reasons to understand security as related to culture.

Still, many people believe that there is an objective property "actual security", described in terms of facts, that can be ascribed to voting systems, independently from cultural perspectives. The facts then determine the necessary measures. In the next chapter, we will see how this assumption can be challenged.

Part III

Society

Chapter 4

Against Ontological Gerrymandering

"Creatures whose mainspring is curiosity enjoy the accumulating of facts far more than the pausing at times to reflect on those facts."

– Clarence Day (American humorist, essayist, biographer and writer, 1874-1935)

In the previous chapter, we have seen how we can explain differences between e-voting discourses in different countries by concentrating on expectations, risk estimations, cooperation and learning experiences. A major question is how such social phenomena relate to something often called "reality". It was argued that security should be understood in relation to culture, but what does this imply for analysing discussions on security?

In this chapter[40] I consider the perspective from which issues of social acceptance in information security are commonly being discussed in the scientific literature. This paradigm is part of a positivist or naturalist conception of the world, which distinguishes between things-as-they-are and things-as-we-see-them. For security, this means that a distinction is made between "actual security" and "perceived security", similar to the use of "actual risk" and "perceived risk". Using results from science and technology studies and the discussion on the concept of risk, I argue that such a distinction is meaningless and only confuses the debate. Instead, I propose to adopt the social science principle of relativity, which states that social laws should be the same from all reference frames. Key concept in such an approach is observation, and I refer to the German sociologist Niklas Luhmann to explain this concept.

[40] Part of this chapter has been previously published in Pieters (2006c).

4.1 Who has the facts?

If a debate is about finding the truth, it is very convenient if you can convince others that the truth is on your side. If you can manage this, the debate will be over. If you can establish as a fact that e-voting is insecure, nobody will want to use it. If you can establish as a fact that e-voting is more secure than paper voting, more and more countries will adopt it. The question still remains, however, if you were wrong or right in establishing this fact. For how do we determine if something is a fact?

In the American e-voting controversy, Avi Rubin seems to use a positivist view on science in his response to the various counterarguments against his position. This means that he refers to the facts that are established by science, which are contrasted with the claims being made in the controversy.

> "I was beginning to understand that pretty much anything goes when you're fighting issues out in public. You can distract people from the facts by raising irrelevant issues, or you can frame the discussion in any way that's advantageous to you." (Rubin, 2006, p. 74)

> "[...] their comments illustrated a totally misplaced concern about voter *confidence* rather than about the actual security of the system. The notion that a sense of confidence was more important than whether the confidence was in fact justifiable spoke volumes about the triumph of image and perception over substance." (Rubin, 2006, p. 126)

> "There was Diebold, once again, smilingly telling the world that black was white and white was black." (Rubin, 2006, p. 146)

> "What suddenly became very clear to me [...] was that a court of law [...] was perhaps the single worst venue in which to debate this issue – or for that matter any issue of science, or any issue concerning public interest. These issues should not be subjected to semantic debate and selective fact-finding. They are issues in which all sides should be working toward the same goal – finding objective truth through comprehensive analysis." (Rubin, 2006, p. 158)

This positivist perspective is strongly at odds with the cultural differences I discussed in previous chapters. As I concluded, even the experts' views are framed by the cultural context in which they operate. This also holds for Rubin: "No American should have to trust someone else, someone with obscure expertise regarding the integrity of the system [...]" (Rubin, 2006, p. 268) Indeed, research suggests that American trade and culture is much more based on distrust than for example the Dutch variants (Hofstede, Jonker, Meijer, and Verwaart, 2006). From a cultural perspective, it makes sense that Rubin does not wish to rely on trust. But can we do completely without it?

In the British debate, we find the same problem in a different disguise. It is suggested by various actors that perceived security is important. What do they mean

by perceived security? It is judged to be related to voter confidence, but what about confidence of the experts? Is confidence of experts not based on perception?

A related question is what the role of the anti-e-voting pressure group is in the Dutch debate. Has the campaign been "caused" by the government not paying attention to important risks, or does the pressure group itself contribute to the "risky" or controversial character of the technology (Gerlach, 1987)? Did the government put too much trust in the manufacturers and do we now know the facts, or has a new form of trust been established, namely in the findings of the campaign? Even if an independent commission agrees with the activists' views to a large extent (Hermans and Twist, 2007), this does not mean the commission would have reached the same result without the campaign's activities.

After the Estonian parliamentary election in 2007, the OSCE election assessment report states that "While trust in the system can be positive, that trust should be based on a full understanding of the security and transparency issues related to Internet voting." (OSCE Office for Democratic Institutions and Human Rights, 2007b) This suggests that trust may be perceived as a good feature in elections rather than something that should be eliminated. But it needs to be a special kind of trust.

In all cases, the philosophical question is what the relation is between actual security, perceived security and trust. This is a philosophical question about the role of information security in society. In this chapter, the relation between actual and perceived security will be discussed. In chapter 6, the notion of trust will play a key role.

4.2 Actual and perceived security

Explicit philosophical work on information security is rare.[41] There is some agreement in the analysis of information security, however, 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".[42] It is then said that trust is based on "perceived security", rather than the "actual security" reflected in the technical aspects. Such a view appears to be intuitive, and provides for business a clear division of responsibilities between the technical department and the marketing department. It is also dominant in science, though. In fact, all of the papers that I consulted about social aspects of security reflect this view in their analyses of security-sensitive systems (Evans and Paul, 2004; Nikander and Karvonen, 2001; Oostveen and Van den Besselaar, 2004; Riedl, 2004; Xenakis and Macintosh, 2005).

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

[41] There is some general work on philosophy of information systems that could be applied to information security, e.g. Dobson (2001); Floridi (1999). This could be an interesting starting point for future research.

[42] Trust can also have a more technical meaning, in the sense of reputation management in computer systems (Nielsen and Krukow, 2004). I will only use it as a human feature.

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.[43]

This distinction can also be applied to election systems. 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" [emphasis added].

In the 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.[44] This yields the hypothesis that resistance to electronic voting is explained by the fact that the paper system is evident and understandable to voters and electronic systems are not.

From the distinction between actual security and perceived security, it becomes easy to state – as Rubin does – that his opponents in the controversy do not care about the facts, about actual security. In a political setting such a statement may be advantageous in advancing your own views, but it is not clear if it helps society in the long run. It may easily lead to polarisation of the debate.

4.3 Ontological gerrymandering and its problems

Apart from the consequences for public discussions about security, this – as I will argue – artificial dichotomy has another problematic effect. It excludes the scientific endeavour from its cultural environment by identifying scientific claims with actual reality. This is not in line with empirical results on the work of scientists. Results

[43] 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. This could be a topic for further research.

[44] 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. However, many researchers after Descartes' time have confirmed that there is much more "constructed" about our experience of even common sense issues than people in the Enlightenment age would have admitted. The apparent clear-and-distinctness of certain things is nothing more than our self-initiated reduction of complexity.

of science and technology studies (STS) have shown that the concept of "scientific fact" can not directly and naïvely be linked to *actual* reality, but is rather partly *constructed* in a process of interaction and negotiation: "Modern technology studies have opened up the "black box" of technological development and revealed the intimate intertwinement of technology and society. Both scientific facts and technological artifacts appear to be the outcome of negotiations, in which many diverse actors are involved." (Keulartz, Korthals, Schermer, and Swierstra, 2002, p. 7) This shows that the distinction of actual security and perceived security is based on a too simplistic notion of objectivity – at least for the aim of this thesis.

It is therefore essential for understanding the issues to provide a more integrated perspective. This is one of the starting points of my analysis of the debate. But before I start that endeavour in the following chapters, I will specify more precisely how this claim can be supported by existing literature and the specific features of the e-voting debate.

Ontological gerrymandering

Distinguishing between actual and perceived seems to have been common practice in the explanation of social problems for a couple of decades. Especially in risk assessment, the "psychometric paradigm" (Jasanoff, 1998, p. 91) was dominant. However, from the 1990s onwards, articles appear challenging the distinction between "actual risk" and "perceived risk" (Cross, 1992; Jasanoff, 1998; Shrader-Frechette, 1990). Cross (1992) realises that "the dichotomy between perceived and actual risk is a false one. All relevant risk measures employ some human agency, so all are literally perceived risks." He uses a distinction between "perceived risk" and "scientific method risk" instead. Kristin Shrader-Frechette (1990) comes to the same conclusion, but adds seven additional reasons for not adopting the distinction:

1. risk probabilities often do not reflect risk frequencies;
2. actual risk estimates are always very rough and imprecise;
3. some of the most important aspects of hazards are not amenable to quantification;
4. risk is a theoretical concept, not something capable of precise empirical prediction or confirmation;
5. because risk perceptions often affect risk probabilities, and vice versa, it is frequently impossible to distinguish hazards from perceptions of them;
6. objectivity and subjectivity cannot be used as criteria for distinguishing actual and perceived risk;
7. perceived risk is not merely an erroneous understanding of actual risk.

Still, the distinction actual/perceived seems to be useful in certain contexts. In research not having anything to do with risk, a distinction was adopted between actual and perceived waiting time in an emergency department in a hospital (Thompson, Yarnold, Williams, and Adams, 1996).[45] That seems to make sense. But in that case, there is strong agreement on how to measure "time". The main point here is that the distinction perceived/actual is similar, or even identical, to self-reported/measured. Then it only works if there is strong agreement on how to measure the property. And that implies, indeed, a distinction between scientific method – in the form of an agreed method of measurement – and "gut feeling". Still, both measurement and gut feeling are to be classified as perceptions or observations. If actual security means measured security, it also relies on observation, although a more systematic one than in "perceived waiting time" (see chapter 7).

Before the 1990s, there had already appeared an interesting piece of work on the role of perception in controversies. Woolgar and Pawluch (1985) describe how controversies are explained in the field of social problems research. They argue that, based on a "definitional" or "social constructionist" perspective, research has moved away from the traditional conceptualisation in terms of objective conditions and causes. Instead, social problems are assumed to be "defined" or "constructed". What is investigated is the deviance of the claims made about the problem from the condition or behaviour that is described.

Woolgar and Pawluch ask the simple but devastating question: "But how do authors manage to portray statements about conditions and behaviors as objective while relativizing the definitions and claims made about them?" In an alternative phrasing, how can we distinguish between facts and claims, and why do the authors select certain claims as facts? Woolgar and Pawluch observe in this the drawing of an arbitrary, but convenient, boundary between facts and claims.

The drawing of boundaries convenient for the people in power is far from unknown in research on voting. In the US as well as the UK, where voting is district-based, parties have used the revision of districts for their own benefits: either putting all supporters of the opposing party in one strangely formed district, or separating them in as many different districts as possible. After the American politician Elbridge Gerry (1744–1814) and the salamander-formed district he created, this practice is termed "gerrymandering".

Analogous to the term gerrymandering in voting, Woolgar and Pawluch introduce the term "ontological gerrymandering" for the drawing of cleverly-designed boundaries between facts and claims (see figure 4.1).[46] According to them, the strategy is very common in scientific research on social problems. "In *all* the empirical work we examined, authors assume the existence and (objective) character of underlying conditions around which definitional claims have been made."[47]

[45] Also useful in queues at US polling stations, I would argue.

[46] To be precise, claims should be understood as "mere claims" here. Otherwise, facts and claims would not be disjoint.

[47] Emphasis in original. My claim about "all of the papers that I consulted" earlier in this section was written independently from this text, which makes an arbitrary, but convenient, coincidence.

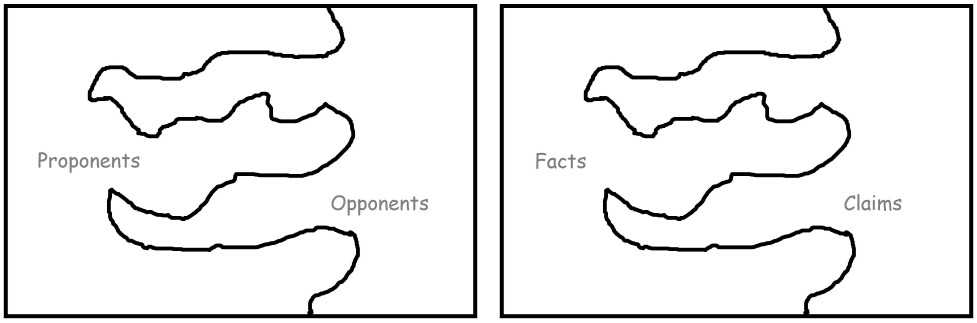

Figure 4.1: Gerrymandering in elections and ontological gerrymandering: proponents versus opponents and facts versus claims.

As we have seen, drawing a boundary between facts and claims happens in the e-voting debate as well. The "facts" found by activists, the "perceived security" that is important in the British debate, and the statements by Avi Rubin in his book on the American controversy all exemplify this statement.

But how do actors (researchers or otherwise) distinguish between actual security and perceived security, i.e. between facts and claims? Which is the objective security condition the deviance from which requires explanation? Often, this problem is not explicitly addressed, and the assumptions can easily be challenged if the method of measurement of the actual condition has not been agreed upon.

Thus, the electronic voting debate is characterised by ontological gerrymandering. Apart from researchers, who would like to explain the social deviance from the real thing, other parties in the controversy can use this strategy as well. Manufacturers can claim that the critique by e-voting opponents is irrational and has nothing to do with the facts. Opponents can argue that the manufacturers are trying to create trust in systems that are actually insecure. The term "ontological gerrymandering" is a good metaphor to describe such a strategy, and obviously the analogy is even more appealing in a book on voting.

The limitations of security models

Some may find, though, that the issue of ontological gerrymandering does not apply to "exact" sciences such as computing science. These are said to be concerned with the natural world, and therefore not subject to social construction. But even if one would agree with this statement in its general form, this does not mean that the same thing holds for information security.

There is, accordingly, a second argument against the use of the distinction between actual and perceived security in information security controversies. In security assessment, there is an inherent fallibility and incompleteness because it is concerned both with the future and with attackers. One never knows what attackers will be up

to in the future, which means that the concept of actual security becomes fluid and open to unexpected changes.

This argument is a specific application of a more general critique of classic theories of technology assessment, where it is pointed out that either the future has too many variables to allow for accurate (or even approximate) predictions of the future, or that models fail to take into account the complexity of the social embedding (Adams, 1995; Bradbury, 1989; Pursell, 1979). We can also – again – refer to the arguments against the distinction between actual and perceived risk, in particular the ones that specifically address the risk concept, rather than any concept (Shrader-Frechette, 1990). Risk is too difficult to capture in a single objective value.

There is an additional complication in (information) security, though. This is related to the distinction between *safety* and *security*. Safety refers to limited effects of the possible unintentional failure of a system. Security refers to limited effects of an attacker deliberately trying to make the system fail in the worst possible way. In scientific research into technological systems, the first property is estimated by verifying the *correctness* of the design. Security is assessed by verifying the *tamper-resistance* of the design. There are connections though; if a computer is easily disturbed by "natural" causes, it may also be easily tampered with.

The possibility of *intentional* behaviour by an attacker to make the system fail increases the problems here. It is not only that we do not know exactly what will happen in the future; we do not know either what *specific people* will attempt to do to compromise the system. Also, what we do to protect the system influences what they will do in order to break into it. There is a so-called *double contingency*, and the vulnerabilities game is an act of "communication" between attackers and defenders (Luhmann, 1995).

In order to talk about such events, we need an *attacker model* that states what potential attackers can do (see also section 7.8). This model is part of the general security model on which verification is based. It is well known in the field of information security that even small security protocols may contain major flaws that go unnoticed for decades, precisely because verification is done using a limited attacker model. For example, the Needham-Schroeder authentication protocol was thought to be correct for 17 years, until it was eventually broken (Lowe, 1996).

Thus, the process of assessing "actual security" is inherently fallible, because assumptions need to be made about the future and about the attackers. Even if a model provides an objective statement about a security property, this statement only holds within the model. In the application of the model, perception may (and will) still play a role.

The complexity of paper voting

My third argument against the distinction between actual security and perceived security is that it does not do a good job in explaining the differences between paper

voting and machine voting. In texts very critical of e-voting, the paper system is usually considered a fixed and transparent way of doing elections. The paper system is "evident and understandable", and its actual security is obvious.

Such a view ignores the long history during which paper voting has become what it is today, and even today, there are many differences between individual countries in counting systems and the way elections are being organised. Most people do not realise why there are pre-printed ballot papers, why some ballot boxes are made of glass, and why you have to go to a polling station at all. Still, all these measures have been considered beneficial to the security of the process.

One might be tempted to say that this indeed proves that the actual security is different from the perceived security. In a sense, we have externalised the security considerations by implementing them in written procedures, and in that respect the original security considerations may no longer be perceived. Also, the paper system is usually considered more secure than can be justified by analysis, which would provide another argument to maintain the distinction between actual and perceived security.

Still, this has nothing to do with the way in which this distinction is used in the e-voting debate. There, it is used to draw a convenient line between facts and claims, which only amplifies the conflict. People point to properties of paper voting as *inherently* more secure, and to the limitations of voting machines as unrepairable, because these properties are due to fixed and undeniable characteristics of the systems, i.e. facts. We have seen that the US have been confronted with many problems in the early days of paper voting as well. By now, these security features have been "blackboxed"[48]. If anything, the not-currently-perceived security of the paper system is based on its history, not on natural properties that were obvious from the beginning.

The paper system is complex enough in itself to reach beyond the understanding of the average citizen, and not to be immediately "evident and understandable". Instead, the security sensitivities of the traditional procedural voting system have been blackboxed in our experience of democracy. Only when something goes wrong in an election, the black box of the "evident and understandable" paper election system is opened, and risks are exposed. Meanwhile, electronic election systems have not been blackboxed yet (except in the Netherlands, where the black box was opened last year), and their vulnerabilities are out there for everyone to discuss. The whole phenomenon of the traditional system being blackboxed, and therefore being "evident and understandable", is already based on trust.

Concluding, the claim that in the paper system actual and perceived security coincide, and that it is therefore the better system, cannot be maintained when studying the history of the ballot and the recent controversies on e-voting. If anything, it is the history that makes the paper system secure from the point of view of analysis, and familiarity that makes it secure from the point of view of the citizens.

Based on these three arguments against ontological gerrymandering in the e-voting debate (there is no actual risk, security assessment is fallible and paper voting is not

[48] Cf. the actor-network theory of Bruno Latour, as explained by Verbeek (2005).

fundamentally more transparent), I will describe two alternatives to this distinction. They are based on the works of Bruno Latour and Niklas Luhmann, respectively.

4.4 The Politics of Nature

The claim that there is some kind of actual security, the deviance from which in perception needs to be explained, has strong similarities to a strategy that Bruno Latour has named "the politics of Nature" (Latour, 2004). Latour conceptualises Nature as a term with a political meaning: Nature puts an end to the debate by its association with infallible facts. Thus, Nature is used to "short-circuit political discussion". Nature, in its capitalised version, indicates an appeal to something that is beyond dispute.

But Latour is not the only one investigating this political dimension of nature. Hansen (2006) writes: "It is the polysemy or semantic richness of 'nature', the ability of the word and the concept to accommodate a multitude of contradictory meanings [...], that makes it a powerful and flexible construct in virtually any public debate or controversy. Invoking 'nature' serves to inoculate against criticism or further scrutiny and to invest partisan arguments and interests with moral or universal authority and legitimacy." The qualities of nature are "non-negotiable".

Uses to which Nature is put include accusations of contamination (cf. Douglas (1994 [1966])) and immunisation against further scrutiny or questioning (Hansen, 2006, pp. 827–829). In his media analysis study of biotechnology, Hansen concludes: "Particularly striking is the relative absence of any questioning of the assumed boundaries that separate the natural from the non-natural." We recognise the strategy of ontological gerrymandering here.

Latour makes this political use of the term nature the main theme of his book. He not only describes this issue, but also tries to explain it and to provide an alternative. For Latour, the term Nature is intimately bound to the term Science. The concept of Nature seems to be politically necessary to safeguard the position of Science:

> "However vast the laboratories may be, however attached researchers may be to industrialists, however many technicians they may have to employ, however active the instruments for transforming data, however constructive the theories, none of this matters; you will be told straight out that Science can survive only as long as it distinguishes absolutely and not relatively between things "as they are" and "the representation that human beings make of them."" (pp. 11-12)

Nature, as opposed to politics, does not acknowledge its political dimensions. It is supposed to be free of values and perceptions; it is an ultimate recourse for problems in the political debate, but it is not political in itself. This separation of Nature from society has its roots deep within our culture, and can be traced back at least to Plato's allegory of the cave. In this story, Plato lets people sit in a cave looking at the shadows of figures moving along the wall. They cannot see the figures that are

responsible for the shadows. Then, the Philosopher gets out of the cave, looks at the real world and tries to tell the people in the cave, who of course will not believe him. The Scientist has just consulted Nature.

Latour ties all these considerations to the political movement of political ecology: the "Green" politics. The main emancipation project of political ecology, as Latour sees it, is not bringing Nature into politics, but getting rid of Nature altogether. Other cultures do not have the distinction between nature and society at all; why would we need it?

Since the "matters of fact" approach and the associated politics of Nature makes us blind to different possibilities, either positive or negative, Latour thinks we have to "let go of Nature". No more multiculturalism and mononaturalism, but multinaturalism. To achieve this goal, we have to reconstruct the concepts of fact and value, since facts are associated with Nature and values with politics. Now, facts already have a Janus-face: they are used both as a challenge to the existing order (complication), and as a confirmation of the existing order (unification). In e-voting, we can use "facts" to point out the vulnerabilities of e-voting systems (complication). We can also use "facts" to point out the procedural safeguards that have been in place and that guarantee the overall security of the system (unification). Both are "facts", but in entirely different roles.

The notion of value has a similar duality. It can be used to articulate voices in the discussion ("e-voting can have much value for the disabled"). It can also be used to discuss the compatibility of new developments with the existing order ("e-voting is not compatible with the requirement of verifiability"). In the first sense, it serves to increase the number of parties involved, the number of positions considered. In the second sense, it serves to discuss the place something new can take in the world as we know it.

Latour names the two different roles of facts *perplexity* and *institution*. For values, he uses the terms *consultation* and *hierarchy*. Then, he proceeds to rearrange these four aspects in two new "powers". Perplexity and consultation are joined as the *power to take into account* and hierarchy and institution are joined as the *power to arrange in rank order*.

Thus, new propositions lead to perplexity, values are gathered by means of consultation, these values are judged based on their compatibility with the existing hierarchy, and once things have been settled, new facts are instituted and will no longer be disputed for the time being. An activist group points to tempest attacks on voting machines, the government consults the intelligence agency, the government judges that the tempest problem of the Sdu machines is not compatible with the secret ballot, and the new fact is that voting machines have to make sure that the range of their compromising emanations is limited to within the polling station. According to Latour, this arrangement, when made explicit, avoids the short-circuiting of political discussion by recourse to Nature by means of Science. Instead, politicians, scientists, economists, moralists join forces in *all* of the new tasks: perplexity, consultation, hierarchy and institution.

The main achievement of Latour is that he shows that an arrangement different from the separation between nature and politics is possible. Whether his new division of powers is the best one is not clear, but at least he proves that challenging the separation of Nature and politics, facts and values, is possible in our culture.

What does this mean for our analysis? Clearly, "Nature" and "actual security" are very similar concepts. Both Latour's capitalised "Nature" and "actual security" appeal to something that is beyond dispute. Both can be used to "short-circuit political discussion". Therefore, "actual security" is the "Nature" of the e-voting controversy. The achievement of Latour in light of the aim of this book is that he shows that the concept of Nature, the associated fact-value distinction, and by strong analogy also the notions of actual and perceived security, are based on cultural and historical legacies themselves.

We can therefore conclude that, following Latour, the notion of "actual security" as opposed to "perceived security" is a concept based on cultural presumptions, and not necessarily the only way to discuss social aspects of secure information technology. By employing different basic "categories" (see the next chapter), different separations of powers may become possible.

In Latour's vision, all groups in society will join forces in an effort of observation (perception), rather than relying on a pre-existing division between the real and the perceived. In the next section, a systematic approach to describe this starting point will be presented.

4.5 Luhmann and the principle of relativity

In the previous sections, three arguments were provided against the use of the distinction between actual and perceived security in science. It was also explained how Bruno Latour provides an alternative to such an approach by trying to get rid of Nature, or actual security. In the application to information security, the most important thing to consider is how we can conceptualise the perception of security properties. Can we avoid the notion of "actual" and still speak meaningfully about security?

The social science principle of relativity

In order to avoid using "facts" or "nature" in a political way myself, I adopt the *social science principle of relativity*: social laws should be the same in all reference frames. This is a stronger version of the *principle of symmetry* (Jasanoff, 1998), which states that "the same types of causal arguments should be invoked to explain true beliefs as false ones." As in the world of nature there is nothing like aether to decide what is moving and what is not, there is nothing in the social world – such as "facts" or "nature" that serves as a universal frame of reference.[49] Nothing allows us to decide which way the deviance goes that we have to explain.

[49] Latour (1988) compares aether with "social context", which is also something that is an objective background to a local explanation. I would say "Nature" plays the same role in his later work (Latour, 2004).

To allow the use of such a principle, we have to start from the concept of *observation* from a particular frame of reference. In order to make observation the central theme in the present approach – the starting point of my analysis which is the same in any frame of reference, as opposed to a universal frame of reference called "nature" or "facts" – I turn towards a particular author. Observation is a key term in the philosophy of sociology by Niklas Luhmann.

Systems, distinctions and observations

Luhmann (1927-1998) was a German sociologist engaged in a project he himself called "Soziologische Aufklärung" (sociological enlightenment). He redefined sociological concepts in terms of systems, a system being defined by the establishment of a boundary between the system itself and its environment. In order to function, a system needs to reduce the complexity of its environment within its own operations. This holds both for psychical systems and social systems. Key in this relation is the system's capability to *observe* its environment.

According to Luhmann, observation is distinguishing indication. It requires a difference between two possible situations, of which one is marked in the present experience. Based on observations, observers can make judgements about what is the case, and what possible problems appear or may appear in the future.

In his work, Luhmann uses various existing theories in order to retreat from a distinction between actual and perceived. He acknowledges the failure of the rational/irrational (or actual/perceived) distinction in explaining controversies on risk (Luhmann, 2005 [1993], p. xxxi). What does this mean for discussions on risks and security? Can his perspective provide alternatives to the actual/perceived paradigm?

The sociological question of risk and security

According to Luhmann, the sociological question of risk is one of *taking into account* and *selecting*:

> "Cultural anthropologists, social anthropologists, and political scientists point out – and rightly so – that the evaluation of risk and the willingness to accept risk are not only psychological problems, but above all social problems. [...] This brings to the foreground the question of who or what decides whether (and in which material and temporal contexts) a risk is to be taken into account *or not*. The already familiar discussion 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." (pp. 3-4, emphasis in original)

The similarities with the Latourian terminology are striking. Based on the available distinctions, risks are *taken into account* or not. The question of risk is not only one of measuring, but one of selecting, of taking into account. What is taken into account in an e-voting controversy depends on observations made by the participants. But

what are we taking into account? What do we distinguish with regard to risk and security?

For Luhmann, sociology is only concerned with communication; therefore, risk as a sociological concept must be understood in these terms:

> "It is thus at best an abbreviated (practical but indispensable) way of putting it when we say that modern technology 'is risky'. Only communication about technology and – above all – the deployment or nondeployment of technology is risky." (pp. xxxii–xxxiii)

Commonly, risk is conceived of as a counter-concept to security. This has the advantage that if we argue against risky decisions, we seem to support the popular value of security. Luhmann argues (pp. 19–20) that this distinction is not very useful, since it is very unlikely that we ever encounter a situation where we have to choose between risk and security. Especially with probabilistic risk analysis, the distinction itself fades away, as certain probabilities of loss are associated with *any* alternative.

Luhmann then explains that for first-order observers, including safety experts, the world consists of facts, a world in which conflicts are based on differing interpretations of or claims in relation to the same facts. However, observers can also make judgements about how their observations differ from one another by using distinctions. The second-order observer sees that "what different observers consider to be the same thing generates quite different information for each of them." Second-order observation is the distinguishing indication of distinctions, i.e. making observations on which distinctions observers use to observe. If I discuss properties of an e-voting system, I am doing first-order observation. If I discuss properties of a discussion of e-voting, I am doing second-order observation.

Risk and danger

Based on this notion of second-order observation, Luhmann proposes a distinction between risk and danger instead of the distinction between risk and security.

> "To do justice to both levels of observation, we will give the concept of risk another form with the help of the distinction of risk and danger. The distinction presupposes (thus differing from other distinctions) that uncertainty exists in relation to future loss. There are then two possibilities. The potential loss is either regarded as a consequence of the decision, that is to say, it is attributed to the decision. We then speak of risk - to be more exact of the risk of decision. Or the possible loss is considered to have been caused externally, that is to say, it is attributed to the environment. In this case we speak of danger." (p. 21)

> "The distinction of risk and danger permits a marking of both sides, but not simultaneously. [...] In older societies, it was thus danger that tended to be marked, whereas modern society has until recently preferred

> to mark risk, being concerned with optimizing the exploitation of opportunity." (pp. 24-25)

Luhmann takes the concept of attribution to be the most important advantage of the risk/danger form as opposed to the risk/security form. This makes it possible to observe how other observers make attributions, i.e. second-order observation of risk. The following two quotations give some conditions for a loss to be attributed to a decision, making it an instance of risk as opposed to danger:

> "[...] if a risk is to be attributed to a decision, certain conditions must be satisfied, among which is the requirement that the alternatives [be] clearly distinguishable in respect of the possibility of loss occurring." (p. 23)

> "[...] an attribution can be made to a decision only if a choice between alternatives is conceivable and appears to be reasonable, regardless of whether the decision maker has, in any individual instance, perceived the risk and the alternative, or whether he has overlooked them." (p. 26)

Thus, Luhmann thinks it is essential for regarding something as a risk that there are alternatives to be considered, be they considered in practice or not. But what determines whether someone reasonably should have considered alternatives? These considerations will prove to be very important for the understanding of the e-voting controversy.

Consequences

What needs to be remembered is that we – in analysing communication – are concerned with second-order observation, i.e. the distinguishing of distinctions. In such a perspective, there is no difference between facts and claims. The question is about taking into account. What can be taken into account or not are risks: uncertainties about possibilities of future loss, attributable to decisions. Whether something is attributable, and can thus be considered a risk (as opposed to danger), depends on the distinctions available to consider alternatives.

Luhmann's theory of observation applies from *any* frame of reference in the discussion. A first-order observer uses certain distinctions to consider risky alternatives. A second-order observer observes the distinctions used by others with his own distinctions. In being part of the discussion, the observer may also observe his own distinctions,[50] a sign that Luhmann does not consider self-reference in his theory a problem, rather the opposite.

In analysing the e-voting controversy, research is focused on what was previously called the theoretical dimension of discussions on risk. We can now adopt Luhmann's terminology, and say more precisely that we are analysing the risk controversy from

[50] Not at the same time he is using them, though.

a second-order perspective. From this perspective, we observe the distinctions that other observers use in their judgements on the risks of e-voting, and the way in which they attribute risks to decisions. This perspective treats all claims symmetrically, without referring to a special kind of claims, namely the true ones, or the "facts". Instead, conceptual analysis, or the analysis of distinctions, forms the basis of my approach.

A second contribution of the theory of Luhmann is the distinction between risk and danger. This distinction is based on whether the possible loss can be attributed to a decision. Attribution to a decision requires the availability of distinguishable alternatives. In chapter 6, we will see how important this is for understanding the e-voting controversies.

4.6 Conclusions

The prevailing approach to public acceptance of the security of information technology is based on a distinction between actual security and perceived security. I have three main objections against this approach. First of all, the idea that some people have access to actual reality and others do not is problematic from a philosophical point of view. Moreover, the "actual security" of a system is often verified in terms of a model of security that has its own limitations. Risk assessment has the general complication of being occupied with future events, but *security* assessment also has to deal with future behaviour of adversaries, which complicates assessment even further (see section 7.8). Thirdly, I have shown that this approach does not reach the core of the matter in the case of electronic elections. Although there is a difference in degree of complexity between the paper system and electronic systems, that does not mean that, in the paper case, everyone just knows what is happening and what the risks are.

Criticism of the actual/perceived distinction is not new. The drawing of an arbitrary boundary between facts and claims has been termed "ontological gerrymandering" by Woolgar and Pawluch (1985). It is also a central theme in the book "Politics of Nature" by Bruno Latour (2004), in which he argues that the reason for using such boundaries is political rather than scientific. Their arguments concerning the use of "facts", "actual states of affairs", or "Nature" in research and politics apply to the notion of "actual security" as well. At a sociological analysis level, this makes the distinction between perceived and actual security problematic, since it implies the possibility of distinguishing sharply between the two, as if actual security were not determined by social interactions. Instead of asking why the claims by the lay people do not reflect the facts established by the experts, we should ask how experts conceptualise "safe" and "secure", and which role existing systems play in defining these concepts.

These are the main scientific sources supporting my view that there is no meaningful distinction between "actual security" and "perceived security". Security is always

perceived security.[51] Of course, the perception of the security of a system, and the reasons why the system is believed to be or not to be secure, may differ from person to person based on the methods and tools of analysis that are available, which are different for an expert than for a layman. However, there is no such thing as "actual security" to be considered apart from the tools that were used to determine it. Just as "actual intelligence" is not an objective property measured by an IQ-test, but rather defined in terms of the test, security is defined in terms of the available tools for analysis, and the accompanying attacker models.

This does not mean that there is no value in scientific research into information security properties and methods for proving these properties. I do argue, however, that we should *not* discuss these benefits in terms of actual security versus perceived security, and I will show that there are reasonable alternatives. These issues will get substantial coverage later in this book.

From a philosophical perspective, I conclude that the distinction between actual and perceived security gives a too naïve positivist account of the matter. Instead, observation or perception should be a key to *any* claim in the controversy. I follow Luhmann in his idea that observation is distinguishing indication, and that a symmetric treatment of all claims in a controversy involves the perspective of second-order observation: the distinguishing of distinctions. If we make observation a basic category instead of the actual/perceived distinction, then how can we understand the e-voting controversies? How do new observations perplex the existing order? And how are these new propositions finally instituted in our life? I will develop this approach further in the following chapters.

First of all, I will discuss the origins of the e-voting controversy from the perspective of distinctions. From a traditional actual/perceived perspective, the origins may be found to lie in some people getting the facts wrong. From a second-order perspective, I am interested in which distinctions generate the controversial character of e-voting. A theory that discusses the role of distinctions in the introduction of controversial technologies is provided by Martijntje Smits. I will apply her approach to e-voting in the next chapter.

[51] One might argue that actual security can be assessed in retrospect. If a system was hacked, it was apparently actually insecure. However, the only thing we can conclude from such a case is that something went wrong and a loss actually occurred (or perceivedly occurred; that does not matter here). We cannot say if the probability of this happening was extremely high or extremely low. Estimates of such properties, again, are subject to the arguments I presented against the distinction between actual and perceived.

Chapter 5

A Monstrous Alliance

"The jargon of these sculptors is beyond me. I do not know precisely why I admire a green granite female, apparently pregnant monster with one eye going around a square corner."

– Ezra Pound (American editor, poet, translator and critic, 1885–1972)

If it is not the difference between actual security and perceived security, then what makes electronic voting so controversial? That is the main question that I try to address in this chapter[52]. My perspective stems from the tradition of philosophy of technology, especially the variant initiated by the "empirical turn" (Achterhuis, 2001). A significant contribution to this field, concerning controversies around new technologies, has been provided by Martijntje Smits (2002a,b). This approach offers an explanation of such controversies in cultural terms, as opposed to an explanation in terms of scientific objectivity versus irrational public responses. I investigate what her approach can offer with respect to an explanation of the controversy around e-voting, as an alternative to the actual/perceived distinction.

The chapter is organised as follows. First, I outline Smits's approach. Then, I discuss to what extent the phenomenon of e-voting and the surrounding controversies can be explained from this perspective. Smits discusses four strategies for coping with controversies. In the last part of the chapter, these strategies are discussed in the context of e-voting. The chapter ends with conclusions from and discussion of the results.

[52] A previous version of this chapter has been published as Pieters (2006b).

5.1 Monster theory

Martijntje Smits (2002a,b) introduces the analytical instrument of "monster theory" in order to explain controversies around new technologies from a cultural perspective. "[M]onster-theory stands for an analytical instrument to study and explain risk controversies and [their] moral dilemmas, since it enables us to articulate the cultural dimension of strong intuitions included in opposite views. This analysis should be directed at explicating ambiguities at the cultural level." (Smits, 2002b, p. 275)

Smits illustrates the need for such an approach by explicating the various positions in the debate on the environmental crisis. In this debate, allegedly objective claims about the facts illustrating such a crisis are made by both "ecological modernisers" and "radical ecologists". The former propose solutions to measured pollution within the existing cultural framework; the latter state that the environmental crisis is an inevitable consequence of precisely this cultural framework. Such claims lead to irreconcilable positions and a paralysed decision-making process: if one of the proposed positions is accepted, the other automatically appears as an emotional response. On the other hand, relativism – in acknowledging that all positions have some truth – does not lead to policy recommendations either.

Smits argues that a theory is needed that can do better than both naturalism[53] and relativism in explaining such controversies. She wishes to avoid naturalist explanations, in which one of the parties is said to have the facts and the other to have "merely" emotional responses, but also the claim that there is no problem, because all positions are equally true. Therefore, she poses the following demands on her approach: "[1] It should give a symmetrical explanation, in which fear and fascination for new technology are clarified by the same mechanism; [2] it should avoid a simplistic understanding of emotional reactions (i.e. as if they only resulted from a lack of rationality), and [3] it should avoid a naturalist justification of moral intuitions." (Smits, 2002b, p. 268)

In order to assemble such a theory (and accompanying methodology), Smits takes Mary Douglas' observations on impurity and danger as a starting point (Douglas, 1994 [1966]). According to Douglas, impurity and danger in traditional societies were the products of a cultural classification system, in which all phenomena were supposed to fit. "Dirt is 'matter out of place' in the cultural, symbolic classification system." (Smits, 2002b, p. 269) Thus, classification systems were not only a description of the world as it was, making it understandable to us, but also of the world as it should be. If something did not fit in the categories, it was considered a problem that had to be taken care of. For example, some African tribes considered twins as monsters, because, according to their categories, only animals produced more than one child.

[53] According to Smits, naturalism means that "actions, norms, or political aims are justified by appeal to nature, or scientific statements about nature" (Smits, 2002b, p. 25, translation WP). In a more general sense, I mean by naturalism what is sometimes called *metaphysical naturalism*, i.e. the view that the world, if perceived correctly, is the same for all of us. In terms of the present study, one could say that naturalism entails the claim that distinctions originate from the world itself. Relativism, then, is the view that distinctions originate from human perception.

Therefore, twins had both human and animal traits, which made them "impure" (Smits, 2002b, p. 134).

Smits argues, following Douglas, that modern ideas about impurity and danger are still largely based on the same mechanisms. She generalises Douglas's approach to include controversies around new technologies. In this case, part of the problem may also consist in the impossibility to fit the new phenomenon into existing cultural categories. New technologies may have aspects of different categories, which may lead to both fascination and horror, until the phenomenon and the categories are adapted in such a way that things fit again. For example, we may think of genetically modified food as an (unacceptable?) mixture of nature and culture, in the same sense that the African tribes considered twins as an unacceptable mixture of human and animal.

Classification problems are deeply entrenched in human culture, because we need cultural categories to be able to understand what happens around us. This automatically leads to naturalist claims about states of affairs, since the categories pre-structure our perception and tell us how the world is and should be: they serve as the basic distinctions in first-order observation. When cultural categories are inadequate to fit new phenomena, "monsters" may come into being, combining aspects of different categories into something seemingly horrible. Another example in the field of technology is the introduction of plastics, which Smits uses to illustrate her approach. Here, fascination and horror illustrated the failure to categorise this new phenomenon as well.[54] Smits calls her approach "monster theory", and shows convincingly that this approach satisfies the requirements [1] to [3] (see page 78).

Smits (2002b) argues: "From the monster theory it follows that waste and dangers are inevitable, because they are the unintended by-products of cultural category classifications. On the borders of these classifications, ambiguities appear, that may, among other things, manifest themselves as monsters." (p. 143, translation WP) The latter happens when the ambiguity is experienced as a possible threat to the existing order, and cannot be resolved easily.

According to Smits, and also following the comparable theory of Bruno Latour, which Smits describes in chapter 9 of her thesis, the typical modern monster-producing classification problem is that of nature versus culture. Our tendency to classify things as either belonging to nature or to culture leads to all kinds of problems in debates around for example genetically modified food and environmental problems. Could it also be a source of the controversy around electronic elections? If this is true, then the distinction between nature and culture is not only a *feature* of the e-voting controversies – in the disguise of the distinction between facts and claims/values – but also a *source* of the controversies.

[54] "Public reactions [to plastics], from fascination to abomination, could be explained by the ambiguous position of plastics in the cultural scheme. From the very beginning, plastic was interpreted as unnatural substance, which in advance gave rise to public euphoria, while later on precisely this aspect was the essence of its supposed evil." (Smits, 2002b, p. 270) An extensive discussion (in Dutch) is found on pp. 107–141.

5.2 E-voting as a monster

Traditionally, democracy is associated with transparent procedures for determining who gets what power, and what needs to be done, based on the free expression of opinion of the individual citizens. One shows oneself to others in the public sphere and engages in debate.

There is a strong association between democracy and *freedom*. Hannah Arendt (1958) argues that the political world is a higher part of culture, in which the human freedom comes to expression in the form of *action*. Action refers to a form of human activity that is characterised by freedom both in the sense of having no external (instrumental) goals and in the sense of transcending the laws of cause and effect. She distinguishes this concept from both work (associated with making and creating) and labour (associated with the animal-like maintenance of existence). Thus, the particularly human trait of freedom is supposed to dominate the political arena.

Technology, on the other hand, has been strongly associated with the laws of nature, and the natural sciences in particular. Only recently have the social aspects of technology been subjected to substantial investigation, especially in the field of science and technology studies (STS) Keulartz et al. (2002) but also from the empirical turn in philosophy of technology Achterhuis (2001). The association of the inner workings of technology with nature, as opposed to culture, however, still remains. The robustness of technology, i.e. the obedience of machines to the laws of nature, their deterministic behaviour, makes them particularly suitable for labour. Even if technology has been put to other uses than relieving people from physical labour (e.g. when it is used for designing things, which is the category of work), and even if Arendt herself sees the technologicalisation of society as *reducing* freedom, this is still the basic concept: technology will make things easier for us. The goals are instrumental.

Thus, following this line of reasoning, democracy and technology are two strongly separated categories in our culture. Technology is associated with nature and Arendt's concept of labour (and work), and democracy with culture and action. The distinction between democracy and technology can thus be reduced to a distinction between the categories of culture and nature, which, according to Smits, are at the root of the modern monster-producing category system.

As long as technology is used for activities associated with labour or work, there is no problem. But, when technology is seemingly taking over the domain of action as well, as in electronic voting, there is an issue with the categories of labour, work and action. Technology is supposed to relieve people of labour and help them create things, not to interfere with their freedom in the political domain. Also, technology is supposed to solve a problem, and activists would argue that there is no problem in voting. Based on this perspective, we can derive a working hypothesis: there is indeed a clash of categories in e-voting, namely of those of technology and democracy, or labour and action, or, again, nature and culture. This hypothesis may serve as a starting point for analysing the controversy around e-voting from a cultural perspective.

If we assume that this clash exists, we can use the monster theory to illuminate the controversy around electronic voting. The intensity of the discussion, as apparent from the coverage by the widely read American information technology magazine Communications of the ACM,[55] may be explained by the phenomenon not fitting the two distinct categories of democracy and technology: one associated with transparency and freedom, and the other with black boxes and the laws of nature. E-voting has properties of both categories, and can therefore be considered "impure", or even dangerous.

Often, the discussion concentrates around the issue of transparency, which is thought to be an essential feature of democracy, as opposed to technology. Precisely because the realm of the political, the realm of action, is characterised by freedom, it is judged to be a necessary feature to be able to inform oneself of every aspect of this realm that is deemed useful or necessary for engaging in the political process. This is also seen as providing checks and balances to elections, the core of representative democracy: people are free to observe the election procedures, and this freedom guarantees the correctness of the results. This freedom seems to conflict with the black-box character of technology: it is not possible for an average citizen to open up a machine and see how it works. In the same sense, procedural guarantees of the secrecy of the vote seem to be more appropriate than technical ones, because citizens are better able to inform themselves about how they work. This, however, is a *cultural* explanation rather than the naturalist explanation of the difference citicised in the previous chapter. It depends on the definition of our categories.

Of course, the precise character of the debate varies from country to country, based on the historical configuration of the categories in these countries. For example, the relatively new democracy of Estonia may have had less severe problems in the introduction of electronic voting, because the conceptual separation of technology and democracy does not have a long history there, if it exists at all. Moreover, the technological infrastructure and its associated skills - or lack thereof - may also play a role in the conceptualisation of electronic voting in a country (Warschauer, 2004). These differences can be further explored in future empirical studies.

Some particular features of voting systems may contribute to the outcome of the controversies. In Switzerland, there is a long tradition of postal ballots. Also in the UK and the US, postal voting has been increasingly liberalised. This makes the "public sphere" character of elections, which is again associated with the political world of action, less pronounced than in other countries such as the Netherlands, where citizens have never seen anything else than voting at a polling station. The concept of the secrecy of the ballot is also country-dependent. In the UK, a demand exists that the relation between a voter and a vote can be recovered by court order. This reduces the conflict between the openness in which people can observe that their vote will be kept secret and the lack of transparency of the technology: the link between voter and vote can be recovered anyway.

[55] Cf. Mohen and Glidden (2001); Phillips and Von Spakovsky (2001); Rubin (2002); Jefferson et al. (2004); Mercuri and Camp (2004).

Another distinction that may be further explored is that between voting machines at polling stations and remote electronic voting via the Internet. The former leave the rituals associated with democracy mostly untouched. People still go to polling stations and vote in a voting booth. There is an issue of transparency here, but the circumstances may not be disruptive enough to create a monster out of it. Voting machines may therefore lead to a gradual adaptation of categories. However, the emergence of the network age and the problems people experience with their own computers seem to aggravate the conflict in the case of off-line voting machines, such that countries trying to introduce electronic voting machines today may have to face more severe protests than those that did so in previous decades.[56]

In the remote Internet voting case, many more changes to democracy are foreseen, and this may amplify the clash of categories in the experience of the citizens, too, when citizens have not become acquainted with electronic voting machines first. A gradual adaptation of categories may not be easy here, especially when there is no experience with other remote forms of voting, such as postal ballots.

This analysis suggests that the monster, in the shape of the transparency and verifiability problem, may take different forms in different countries based on existing voting methods, and associated definitions of categories. We have indeed seen such differences in our empirical data on the discussions in the Netherlands and the UK (chapter 3). These subtleties can be further explored when the controversy is explained from the perspective of cultural categories.

5.3 Strategies for coping with the monster

In her thesis, Smits (2002b) discusses four styles of dealing with monsters, which make it possible to live together with them. These are, in my own order, embracing, expelling, adapting and assimilating the monster. These strategies may also be used in the case of electronic voting. In the following subsections, I will discuss each of these styles, first in general, and then in the context of e-voting.

Embracing the monster

Monster-embracers are fascinated by the paradoxes that monsters provide. Like the African Lele people, who worship the pangolin precisely because it does not fit in any of their animal categories (Smits, 2002b, p. 160), they see intrusive technology as something holy, not because of its potential benefits for society, but for its own sake. Such reactions of fascination were for example present during the introduction of plastics (Smits, 2002b, pp. 109–114; 160–161).

In the case of Internet voting, monster embracing is frequently seen among politicians, especially in the initial phase of the discussion in a country. Although reference is often made to expected benefits, such as increased turnout, these expectations are

[56] (Saltman, 2006, pp. 166–167) mentions fear of software fraud starting already in 1969. However, media coverage of computer problems has increased considerably since.

frequently not supported by any systematic research. Instead, the possibility itself is fascinating, and can count on support from politicians who hope that the public is as fascinated as they are. By now, the public reactions, if any, do not seem to support this enthusiasm, although the Dutch seem to appreciate the initiative from a more pragmatic perspective: depending on the context of the question, between 62 and 79 % of the Dutch citizens using Internet would like to vote online (Burger@overheid publiekspanel, 2002, 2004).

In general, the utopian prospect of e-democracy (Anttiroiko, 2003), which deliberately combines the categories of democracy and technology, can be seen as a form of monster-embracing, at least when no need is acknowledged for adjusting the technology and the existing cultural categories to each other. From such a perspective, technology will solve all the problems that democracy is said to experience, by reducing the gap between citizen and government.

The idea that there is no danger involved in moving from face-to-face democracy to electronic interaction can be deceiving, though. In one Dutch political party, an attempt was made to allow Internet voting for members that were not able to attend the party congress. The initiators were very enthusiastic about the possibilities, but they did not realise that there would be severe resistance, from the point of view that the democratic processes within the party are inherently social, and not easily captured in a remote electronic vote.[57] Embracing the monster does not lead to recognition of the challenges that such subtleties provide, both to the technology being developed and to the existing cultural categories.

Expelling the monster

Monster-expellers are basically Luddites, and they attack disrupting technologies based on a dogmatic style, in which existing categories are seen as fixed and pure. This is the strategy that the African tribes used in solving the "twin problem". More recently, similar reactions were seen to the introduction of plastics mentioned before (Smits, 2002b, pp. 114–122). Another illustrative example is the planned sinking of the Brent Spar in 1995. Shell intended to sink the old oil platform, but due to protest and mobilisation of public opinion by Greenpeace, they eventually decided to dismantle it instead, even though the environmental risks of that procedure were later judged to be as bad, or even worse. Smits argues that the mobilisation of public opinion was based on the irreconcilability of the categories of "sea environment" (nature) and "man-made artifacts" (culture) (Smits, 2002b, pp. 150–153). In this sense, expelling a monster is not merely an emotional response, but a reaction to the failure of the attempt to categorise the phenomenon. Seen from a world constructed from these categories, the threat is real.

Many people have responded in a similar sense to electronic and Internet voting. Activist movements in the US and the Netherlands exemplify the case for electronic voting machines, especially in terms of verifiability. For Internet voting, alleged "real"

[57] I was approached to give advice on the plan, and observed the discussion in various meetings.

and insoluble threats include lack of control of the voting environment and the fundamental insecurity of the current Internet infrastructure (Jefferson et al., 2004). Indeed, Internet voting may not fit the category of a democratic election system in the strict sense, because voting is not done in a publicly controlled place.[58] Also, many attacks possible in an Internet environment due to hacking do not fit the existing categories of election fraud (cf. chapter 8). This means that existing countermeasures are not capable of preventing these attacks. Thus, from a dogmatic point of view, it is unacceptable, and has to be destroyed.

Again, these reactions are entirely plausible from a perspective in which an election is something transparent, done on paper in a polling station, with associated (known) procedural security measures, and technology is something suitable for manipulating nature, and inherently black-box. However, many countries in the world already have a tradition of postal ballots, which does not meet the strict requirements of a traditional election system either. Also, creative solutions can be proposed to increase Internet election verifiability, even in the face of hacking activities.[59] And last but not least, there should be a fair comparison of e-voting with paper ballots, in which the risks of both systems are systematically evaluated.

Adapting the monster

Both embracing the monster and expelling the monster suffer from a lack of commitment to improve the state of affairs. People who embrace the technology of electronic elections are not sensitive to the challenges that the new technology brings. People who expel it are not sensitive to the opportunities, and argue instead that e-voting is impossible to implement securely. Both approaches seem to block the progress that could be made by investigating the opportunities and challenges, and testing possible solutions. Even if (remote) e-voting is not deemed suitable for sensitive political elections (yet), testing and improving the concept could be done in other "niches". The two remaining strategies, adapting and assimilating the monster, do provide opportunities for improvement, though in different ways.

Adapting the monster, also referred to by Smits as the ritualist style, means putting the monster back into one of the existing categories, by adapting its features. This can often be done by following the rules that are defined within the existing category system. In this way, biodegradable plastics were an adaptation of the monstrous plastics to an existing category, by giving them a "natural" characteristic.

In electronic voting, there is a remarkable example of monster adaptation. In the controversy around electronic voting machines, Rebecca Mercuri (2002) proposed a "voter verified paper audit trail" (VVPAT) (see page 21). In this way, the monster fits the traditional category of human-verifiable and transparent elections again, while

[58] As we have seen in our UK interview data, there is controversy about voting in an uncontrolled environment in relation to human rights treaties. The 1966 International Covenant on Civil Rights of the UN states that voting should be done by "secret ballot, guaranteeing the free expression of the will of the electors" (quoted in Vollan (2005)). The issue is whether it is the responsibility of the voter or the authorities to provide secrecy.

[59] Cf. the literature review provided in Joaquim, Zúquete, and Ferreira (2003).

maintaining the benefits of electronic voting in terms of counting speed and prevention of mistakes. As we have seen, the concept of a voter-verified audit trail has gained substantive attention in the scientific and political discussion on electronic voting.

In Internet elections, paper trails are not a meaningful adaptation, because there is no way to check that a voter submits the same vote electronically and by paper (see page 24). Instead, other changes have been implemented to make the technology acceptable. These basically amount to limiting the use of Internet voting. This can be either a limitation to certain groups of voters, e.g. expats (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2004), or limitation to certain supervised places (kiosks) (Alvarez and Hall, 2004, p. 4). Again, these adaptations make the voting system fit existing categories, which are often also reflected in the law. To make remote e-voting acceptable for all voters in political elections, however, more advanced strategies are needed.

Various other ritualist solutions to the problem of the "monster" character of electronic voting have been described in the literature. Schoenmakers (2000) argues that we can compensate for the lack of transparency in electronic voting by rigorous mathematical proofs that the election systems do what they are supposed to do. Indeed, very elegant solutions to these proof obligations have been described in the literature.[60] However, it is not obvious that mathematical proofs bear much relevance when taken from the domain of technology to the domain of democracy, precisely because there is a clash between categories here: technical proof (related to technology and laws of nature) is something completely different from public verifiability (related to democracy and culture). It is not easy for the public to accept a system in which these categories are confused. It seems that this problem has been underestimated within the scientific information security community.

Assimilating the monster

The fourth and last strategy that Smits discusses is a pragmatic assimilation of the monster. In this process, both the technology and the cultural categories are being changed. Contrary to the other approaches, the categories are not considered fixed in this style. Smits therefore thinks that this is the best strategy in terms of mutually adjusting technology and society. An example of such an assimilation was the introduction of the concept of "brain dead" following the advent of organ transplantation. This new category allowed organs to be taken from bodies of which the heart was still beating. The line between alive and dead was shifted (Smits, 2002b, p. 159).

The pragmatic strategy of assimilation allows for more flexibility in incorporating technology in society than the other approaches do, by treating the cultural categories as flexible rather than fixed. This is not to say that we automatically have to adapt our cultural system to new technologies, which would suggest a kind of technological determinism, in which the "volonté machinale" degrades into following technological developments blindly. It does mean, however, that the opportunities that the new

[60] Overviews are given in Joaquim et al. (2003); Pieters (2006d).

technology brings can be investigated in a broader cultural sense, hopefully avoiding polarisation of the debate.

I already presented some ideas on adapting the technology of electronic voting to existing categories. How can we adapt the categories to the technology? In order to enable such an adaptation, it is important to realise that elections have always been intimately bound to both culture and technology. The current style of organising elections has been influenced by social and technical developments from the beginning,[61] and electronic voting technology may not be the only monster this history has produced. E-voting, however, is a new phenomenon that will change our elections in a new way. What does this mean for our cultural categories?

The monster character of electronic voting is ultimately based on the categories of democracy and technology, which is again a manifestation of the culture-nature distinction. It is probably naïve to think that introduction of e-voting will fundamentally change these categories. Therefore, developers should be encouraged to take this distinction into account in their designs, e.g. by providing public vote counting instead of mathematical proofs of correctness. Nevertheless, there are some less fundamental categories used in discussing elections that may indeed be subject to change, such as the interpretation of the requirement of secrecy, as we have already seen in the discussion in Estonia. More of these issues will be identified in following chapters, notably chapter 10.

5.4 Conclusions

In this chapter, I aimed at providing a cultural explanation of the controversy around the introduction of electronic voting. The starting point of my analysis was the idea that the perception of risks is related to the cultural categories in which people categorise phenomena, which serve as the basic distinctions from which first-order observers perceive the world. Martijntje Smits (2002b) argues that controversies surrounding the introduction of new technologies can often be explained in terms of a clash between cultural categories. Whereas traditional cultures may for example see twins as an unacceptable mixture between human and animal that has to be destroyed, we may think of genetically modified food as an unacceptable mixture of nature and culture. These "monsters" come into being when cultural categories are inadequate to fit new phenomena.

Based on the monster theory of Smits and the categorisation of human activity by Hannah Arendt (1958), I used as a working hypothesis the claim that e-voting fits the concept of a monster: a technology that leads to controversy by combining aspects of two separate categories. The controversy around electronic voting can then be explained by a clash between the cultural categories of democracy and technology. Based on this hypothesis, explanations can be provided of various positions in the debate on electronic voting.

[61] Cf. Dewey (1991 [1927]) and Saltman (2006).

Whereas some proponents of e-voting are fascinated by the clashing categories and embrace the monster, others do everything to expel the monster by claiming the impossibility of implementing a secure e-voting system. A third approach is to adapt the monster to existing categories. Examples of this strategy in electronic voting are the inclusion of a paper trail in electronic voting machines, and limiting the implementation of Internet voting to citizens staying abroad, who were already allowed to vote via postal ballots. The fourth strategy that Smits mentions, and which she characterises as the most promising one, is a pragmatic assimilation, in which both the technology and the cultural categories are being adapted. I argue that such an approach is advisable to avoid the irreconcilable positions of monster embracing and monster expelling, and the limitations of monster adaptation. Based on further analysis in the following chapters, a systematic way to use such a strategy will be described in chapter 10.

In the context of monster theory, it is exemplary that a relatively new democracy such as Estonia seems to have far fewer problems in converting democracy into something compatible with the information age. This may be explained by a less strong separation of the categories of democracy and technology in this culture. This invites a more flexible attitude, leading to a strategy of assimilation. In other countries, the monstrous character has been exposed by comparison of the new technology of electronic voting with existing arrangements. There, this revelation led to new ways of thinking about electronic voting systems.

There are some subtleties in electronic voting, however, that may lead to refinements to the monster concept in future work. Firstly, there may be good reasons not to implement certain types of e-voting in general elections at all, even if we take a pragmatic point of view. Can this still be called assimilating a monster?

Secondly, the role of the nature-culture distinction as the most important modern monster-producing classification problem may be more subtle than both Latour and Smits acknowledge. Technology seems to be able to appear both on the culture side (as something that is produced by humans, in the Brent Spar case) and on the nature side (as something that obeys the laws of nature as opposed to human freedom, in the e-voting case). An investigation into the various appearances of the nature-culture distinction in technology-related controversies would be useful.

Thirdly, the notion of cultural category may appear to be rather vague. Is everything a category? And how do we establish which categories exist in a culture? How are categories related to language? From a naturalist or positivist perspective, the notion of category may appear problematic, since cultural categories, as opposed to the objective categories of nature, are harder to determine in an objective fashion. Moreover, if perception is based on cultural categories, then is it not the case that also perception of categories is itself based on categories, and therefore doomed to lack the required objectivity?

I propose to relate the concept of cultural categories to Luhmann's notion of distinction in order to resolve some of its ambiguity. Cultural categories are concepts used in a culture in order to make distinctions. They primarily serve to *communi-*

cate distinctions, but in this way also influence personal perceptions. Thus, cultural categories are hypothesised to be the social complement of personal distinctions. A further study could reveal this relation more precisely.

With respect to objectivity, Luhmann does not consider the self-reference of his theory a problem. Indeed, from a systems theoretic perspective, one will always capture the environment in terms of the distinctions available. For second-order observation, this means that the distinctions available to capture distinctions are themselves system-specific rather than objective. But from a perspective that adheres to the principle of relativity, this is the best we can do.

Even when the subtleties introduced by these questions are taken into consideration, I would argue that the explanation of the controversy around e-voting in terms of cultural categories offers a fruitful perspective on the limitations and possibilities of this new technology. Instead of producing just another risk analysis, this perspective shows us how the assessment of risks itself is based on cultural presumptions. This may lead to a more refined analysis of the challenges that the technology brings to our democracy.

Based on the application of the monster theory to e-voting, we can also understand that the actual/perceived distinction occurring in the debate is not the only manifestation of Latour's Nature that is relevant to e-voting. Apart from the appeal to Nature being used in arguments in the controversy, the distinction between nature and culture is also present as a *source* of the controversy. Nature versus culture is technology versus democracy, and this explains the monstrous character of e-voting.

There is more to the comparison of Latour's and Smits's work. The four tasks that Latour proposes for a new division of powers perplexity, consultation, hierarchy and institution (page 69) – can be linked to Smits's monster-conjuring strategies. Monster-expellers are the ones who regard institution as the most important task: things should stay as they are, based on existing facts. Monster-embracers, on the other hand, see most of all the perplexing capacities of the new phenomena. Monster-adapters think that these new actants should be fit into the hierarchy by changing their features. This leaves consultation for the monster-assimilaters, although the analogy does not appear to be as strong here. Still, the task of consultation carries the idea that different views should be incorporated, which can be seen as a promising task given the view that categories are flexible. A further study into this comparison may deepen these considerations.

From the monster theory, we can learn why e-voting can become controversial from the perspective of categories or distinctions. However, by becoming controversial, e-voting can also become a category *itself*, and thereby distinguishable from paper voting.

If e-voting can become a subject of controversy, it can thereby become seen as a completely different thing than paper voting. All the monster-conjuring strategies have in common that they clearly distinguish the new technology as something different than what already existed; this is implicit in the notion of monster. Whereas

the Dutch regarded e-voting as improvement of an existing system before, it is now seen as a real alternative to the paper system: e-voting itself has become a category, distinguished from others. Being an alternative, the technology, or rather the communication about it, has become risky, because future threats can now be attributed to decisions. A strategy likely to appear to resolve this situation is adapting the e-voting monster to existing categories by means of a paper trail.

Besides, the monster theory reinforces the need for a second-order perspective. If the alternative strategy of assimilation is to be a promising one, we have to conceive our own categories as flexible. However, if we wish to be able to adapt the categories, we need to be able to distinguish them as distinctions in the first place. This requires second-order observation, i.e. a discussion on a conceptual level.

Now that we know about the cultural origins of the e-voting debate, we can further investigate how the monstrous character frames the controversy. In the next chapter, I discuss how the appearance of the monstrous e-voting as an alternative to paper voting can change the expectations of e-voting systems. For that purpose, we need to discuss the issue of trust in information systems.

Chapter 6

Between Confidence and Trust

"I've always wanted trust, as a security person, to be a very simple thing."

– Matt Blaze (information security researcher, University of Pennsylvania)

We have seen that the existing form of discussing e-voting in terms of actual security and perceived security is problematic. Furthermore, I have pointed to cultural origins of the e-voting debate, which may make e-voting a monstrous alternative to paper voting. Rather than explaining the difference between paper voting and electronic voting in terms of actual and perceived security, the introduction of e-voting is seen as a cultural transition.

In this chapter[62], this transition process is analysed based on the notion of trust, providing an alternative to the actual/perceived distinction. I investigate the different meanings of this notion in computing science, and link these to the philosophical work of Luhmann, who distinguishes between familiarity, confidence and trust. This analysis yields several useful distinctions for discussing trust relations with respect to information technology. Based on these distinctions, I argue that the appearance of e-voting as an alternative to paper voting changed the expectations of e-voting systems. I also propose some hypotheses that can possibly explain the smooth introduction of electronic voting machines in the Netherlands in the early nineties.

6.1 Good and bad trust

We have already concluded that a philosophy of information security cannot be a philosophy of actual and perceived security. Instead, I take as a starting point the

[62] Part of this chapter has been previously published in Pieters (2006c).

idea that people, laymen or experts, *experience* an environment as relatively secure or insecure. This approach adheres to the social science principle of relativity, by making each frame of reference equivalent. Also, Luhmann's notion of observation as distinguishing indication motivates this approach: security and trust are based on distinctions in our experience. Based on this perspective, I will show how trust can be seen as the primary factor in the relations between humans and systems when it comes to security, and not as a derivative of an objective kind of security.

As already indicated in section 1.2, trust relations with respect to systems are characterised by being concerned with either safety or security. In the first case, the trust relation involves trust in the limited effects of failure; in the second case, it involves trust in the limited effects of attack. For example, trust in a nuclear power plant is composed of trust in the *safety* of the plant (e.g. it does not explode "spontaneously") and trust in the *security* of the plant (e.g. it does not explode under terrorist bombing).

A second distinction that I wish to draw here is connected to the scope of the effects of failure or attack. These effects may be either *private* or *public*. When I drive a car, I trust in the limited effects of failure of the car for my own health. When I vote, I trust in the limited effects of failure of the election system for the whole country. The same holds for the effects of attack: an attack on a nuclear power plant may have private effects (if I or some of my friends live near it) and public effects (changes in politics due to the attack).

Having set this general background, I now investigate the concept of trust itself a bit further. One of the most confusing issues appearing from the computing science literature on security is the existence of two different conceptions of trust. On occasion, they even appear in the same article (Evans and Paul, 2004). Although the analysis of trust in voting systems that is presented there covers many concrete risks involved in using these systems, the conception of trust that is used is apparently not completely coherent. In a section named "*Increasing* trust" [emphasis added], the following sentence is found: "One way to *decrease* the trust voters must place in voting machine software is to let voters physically verify that their intent is recorded correctly." [emphasis added] But was the intent not to *increase* trust? Do we wish to increase and decrease trust at the same time? What is happening here?

Apparently, computing scientists stem from a tradition in which minimising trust is the standard. "In computer security literature in general, the term is used to denote that something must be trusted [...]. That is, something trusted is something that the users are necessarily dependent on." (Nikander and Karvonen, 2001) Because we *must* trust certain parts of the system for the whole system to be verifiably correct according to the computing science models, we want to minimise the size of the parts we have to trust, thus minimising trust itself. However, from a psychological perspective, or even a marketing perspective, it is desirable that users trust the *whole* system. Maximising trust seems to lead to more fluent interaction between the user and the system, and is therefore desirable. In Nikander (2001), Matt Blaze says:

"I've always wanted trust, as a security person, to be a very simple thing: I trust something if it's allowed to violate my security; something that's trusted is something that I don't have to worry about and if it is broken, I am broken. So I want as little trust in the system as possible, and so security people are worried about minimising trust and now suddenly we have this new set of semantics that are concerned with maximising trust, and I'm terribly confused."

In the following, I try to alleviate this confusion by explicating the assumptions found in both approaches to trust, and placing them within a larger (philosophical) context. Apparently, two different interpretations of trust have to be distinguished (cf. Nikander and Karvonen (2001)):

- trust as something that is *bad*, something that people establish because they *have to*, *not* because the system is trustworthy;
- trust as something that is *good*, something that people establish because they *want to*, because the system *is* trustworthy.

How can we conceptualise this difference? In political science, there is a well-known distinction between *negative freedom* and *positive freedom*. Negative freedom means the absence of interference by others; positive freedom means the opportunity for people to pursue their own goals in a meaningful way.[63] I see a parallel here with two possible concepts of safety and security, namely a negative and a positive one:

- negative safety/security: absence of everything that is unsafe/insecure;
- positive safety/security: opportunity to engage in meaningful trust relations.

When people use a negative concept of security, trust has to be minimised, since it denotes a dependence on (possibly) insecure systems. By removing everything that is insecure, trust defined in this way can indeed be minimised. In a setting where security is defined positively, however, trust suddenly forms an essential precondition for security, because security then requires the possibility to engage in trust relations. This is precisely the approach that comes from psychology, as opposed to the dominantly negative approach of computing science (remove all insecurities).

I will label these two conceptions of trust *bad trust* and *good trust*, respectively. I deliberately avoid the terms negative and positive in my distinction of trust, because these are used in the definitions of both freedom and security as indicators of how the concepts are defined (certain things *not* being there vs. certain things *being* there), not of their desirability. Bad and good instead indicate whether we should try to minimise or maximise the associated appearance of trust. Thus, the two different interpretations of trust are linked to two different conceptions of security. Bad trust is linked to a negative conception of safety and security, and good trust to a positive conception. In philosophy, distinctions between different modes of trust have been drawn before. I will use such a distinction to further clarify the differences.

[63] Cf. Cunningham (2002), pp. 36-39. The notion was originally introduced by Isaiah Berlin (1969 [1958]).

6.2 Familiarity, confidence and trust

Luhmann (1979) provides an extensive model of trust, based on his systems theory. According to Luhmann, trust is a mechanism that helps us to reduce social complexity.[64] Without reducing complexity, we cannot properly function in a complex social environment. Luhmann distinguishes several types of trust relations.

First of all, he distinguishes between *familiarity* and *trust*. Familiarity reduces complexity by an orientation towards the past. Things that we see as familiar, because "it has always been like that", are accepted – we do engage in relations with those – and things that we see as unfamiliar are rejected – we do not engage in relations with those. For example, especially elderly people often refuse to use ATM's or ticket vending machines, precisely because they are not used to them.[65] Trust, on the contrary, has an orientation towards the future: it involves expectations. We trust in something because we expect something. For example, we use ATM's because we expect these machines to provide us with money faster and more conveniently than a bank employee behind the counter.[66]

In later work, Luhmann (1988) also draws a distinction between *trust* and *confidence*. Both confidence and trust involve the formation of expectations with respect to contingent future events. But there is a difference.

In chapter 4, I introduced Luhmann's distinction between risk and danger. In case of danger, the possible loss cannot be attributed to a decision, whereas it can in case of risk. This distinction forms the basis for distinguishing confidence from trust. According to Luhmann, trust is always based on assessment of risks, and a decision whether or not to accept those. Confidence differs from trust in the sense that it does not presuppose a situation of risk. Confidence, instead, neglects the possibility of disappointment, not only because this case is rare, but also because there is not really a choice. This is a situation of danger, not risk.[67] Examples of confidence that Luhmann gives are expectations about politicians trying to avoid war, and of cars not suddenly breaking down and hitting you. In these cases, you cannot decide for yourself whether or not to take the risk.

When there *is* a choice, trust takes over the function of confidence. Here, the risky situation is evaluated, and a decision is made about whether or not to take the risk:

[64] The function of trust as a means for reduction of complexity seems to be known in computing science. For example, Nikander and Karvonen (2001) mention this aspect. However, this paper does not refer to the work on trust by Luhmann.

[65] One may argue instead that the reason is not that they are not used to them, but rather the fact that it is harder for them to learn new things. Yet this is precisely one of the conditions that invites relying on familiarity rather than trust.

[66] Luhmann distinguishes personal trust, i.e. trust in interpersonal relations, from system trust, i.e. trust in the general functioning of a non-personal system. We may expect something from a person, or we may expect something from society as a whole or from a machine. Since the focus is on technological systems here, trust in this book is always system trust.

[67] Some native English speakers have noted that this distinction seems to be counter-intuitive. They would rather use the word "trust" for a situation which one has not analysed, and confidence for a more rational form of assurance. In order to avoid confusion in comparison with Luhmann's original text, I will still follow the terminology as introduced there.

"If you do not consider alternatives [...] you are in a situation of confidence. If you choose one action in preference to others [...], you define the situation as one of trust." (Luhmann, 1988) If you choose to drive a car by evaluating the risks and accepting them, this is a form of trust.

Apparently, Luhmann ascribes the same negative characteristics to confidence that are ascribed to bad trust from a computing science perspective, in the sense that people do not have a choice. People *have to* have confidence in "trusted" parts of the system. Moreover, what Luhmann calls trust has the positive connotation of what I called good trust, in the sense that people can decide for themselves whether they want to trust something. Trust is then necessary for a system to be successful. I have to note, however, that Luhmann does not regard confidence as a bad thing in general; it is even necessary for society to function. Still, with respect to information systems, confidence means accepting a system without knowing its risks, and computing scientists are generally not willing to do this.

Thus, Luhmann distinguishes between two kinds of relations of assurance, based on whether people engage in these relations because they have to or because they want to. Luhmann calls these two relations confidence and trust, respectively. We may also speak, in more common sense terms, of *blind trust* and *rational trust*. These observations explain the situation I described in computing science. This means that the distinction that was made between "bad trust" and "good trust" is not something that characterises social aspects of security in information systems only, but something that can be considered a general characteristic of trust relations.

From now on, I will use *relations of assurance* as a general notion. Confidence and trust will only be used in Luhmann's sense. I describe relations of assurance based on three distinctions:

- assurance with respect to safety vs. assurance with respect to security;
- assurance with respect to private effects vs. assurance with respect to public effects;
- confidence vs. trust.

Computing scientists generally try to replace confidence with trust, i.e. exchange unconscious dependence on a system for explicit evaluation of the risks, and minimising the parts in which we still have to have confidence. Philosophers (and social scientists), instead, recognise the positive aspects of confidence, and may evaluate positively people having a relation of assurance with the system without exactly knowing its risks (i.e. confidence). This is not meant as a conclusion that holds universally, but rather as an indication of the role of the scientific subcultures in the debates.

My point of view in this discussion is that, because society is too complex for everyone to understand all the risks, there should be a balance between the trust experts have in the system, based on their analysis of the risks, and the confidence the users have in the system. This ensures that there *is* knowledge of the detailed workings and risks of the system within the *social* system in which it is embedded,

but there is no need for everyone in the social system to know exactly what these risks are, precisely because there is a relation between expert trust and public confidence. How to establish such a relation is a question that I do not discuss further here.

By defining the role of scientists as one of replacing confidence with trust, we avoid the problems associated with the appeal to actual security. It is not the case that after a single scientific effort we suddenly know the facts. Neither is this the case after the security analysis of a voting machine by an activist group. Rather, the process of replacing confidence with trust is a gradual one, in which all actors make their specific contributions. Calling the result "trust" instead of "actual security" provides an alternative to the appeal to Nature and the associated polarisation of discussions.

Based on the distinctions I discussed in this section, we will now turn our attention to trust in technology.

6.3 Trust in technology

When discussing security aspects of technology, reliability and trustworthiness are often mentioned. First of all, I propose a distinction between reliability and trustworthiness. A system acquires *confidence* if it is *reliable*, and it acquires *trust* if it is *trustworthy*.[68] A reliable system is a system that people can use confidently without having to worry about the details. A trustworthy system is a system that people can assess the risks of and that they still wish to use.

There is a fairly subtle relation between reliability and trustworthiness. On the one hand, trustworthiness is a stronger notion than reliability. Before they give their trust to a system, people will perform a risk analysis. People who establish confidence in a system do not do this. In this sense, it is harder for a system to *acquire* trust than to *acquire* confidence. However, *maintaining* trust is easier than *maintaining* confidence. When people trust a certain system, they are already conscious of the risks and decide to use it anyway. This means that trust is not necessarily broken if something fails. In the case of reliability, however, people have put their confidence in a system because they do not see alternatives, and they will probably not accept any failures. Trustworthiness is therefore the stronger notion for the short term, and reliability is the stronger notion for the long term.

How are reliability and trustworthiness established? As I have made clear in the introduction, I argue that they are not objective properties of a system that are reflected in subjective confidence and trust. Instead, the objective aspects of reliability and trustworthiness and the subjective aspects of confidence and trust emerge from the relation between people and the system, the interaction between persons and their environment.[69] The way in which they are established depends on the analytic tools

[68] Reliability is used in the more limited sense of continuity of correct service in Avižienis, Laprie, Randell, and Landwehr (2004). My notion of reliability roughly corresponds to the "alternate definition of dependability" in their taxonomy, whereas trustworthiness corresponds to the "original definition of dependability".

[69] This is a phenomenological point of view: the relation between persons and a system is conceived as primary to the objective and subjective aspects (Ihde, 1990; Verbeek, 2005).

that are available to a person. If a person is just using the system, the outcome will probably be different than in case an expert performs a full security audit based on her expertise.

The relations that different people have with the system make the objective aspects of reliability and trustworthiness converge into different images of the system. These images then become "objective" properties of the system. The relations that experts have with the system determine what is often called the "actual" security of the system, but this "actual" security is still based on perception and relations of assurance, and therefore I rather avoid the term "actual".

How does this analysis of trust in technology apply to computer systems? Computer systems can be characterised as *congealed procedures*. Such procedures are typically more rigid than human-managed procedures. They are less easy to circumvent, but also less robust. Humans are easy to persuade to abandon the rules, computers are not. Humans can easily find solutions for problems that do not exactly match the rules, computers cannot. Because computers are not flexible, congealed procedures must be specified in more detail than human procedures. Every possible situation should be covered. This, and the fact that most people do not have expert knowledge about computers, makes congealed procedures hard to understand.

As we have seen before, trust in a system requires understanding of the risks involved in using a system. This is usually relatively easy to achieve in human procedures, not necessarily because the systems are less complex, but because we have a good understanding (or at least we think we have a good understanding) of how humans function. Understanding the risks of using a computer system is typically much harder. On the other hand, precisely because congealed procedures are more rigid, the associated systems are generally more reliable, in the sense that they produce fewer errors. This makes them more suitable for being reliable and acquiring confidence, while less suitable for being trustworthy and acquiring trust. Thus, automation implies a transition from public trust to public confidence. This makes it all the more important that a balance is established between expert trust and public confidence, in order to have public confidence still reflect a risk analysis in some way.

Luhmann observes the same tendency of replacing trust by confidence in functional differentiation of society. Because people in a functionally differentiated environment have knowledge of only a very small part of the complex structures that surround them, establishing trust is hard, and confidence is extremely important. This also requires procedures to be increasingly rigid, precisely because they need to maintain confidence. This may be seen as a first step in the freezing of procedures; automation is then a continuation of this process, by entering these semi-frozen procedures into machines, and thereby fixing all the details even further.[70]

[70] Interestingly, this transformation of trust in human procedures into confidence in congealed procedures goes against the tendency that Luhmann observes in liberalism. According to Luhmann (1988), "liberalism focuses on the individual responsibility for deciding between trust and distrust [...]. And it neglects the problems of attribution and the large amount of confidence required for participation in the system". From this point of view, either information technology is a threat to liberalism, or liberalism should revise its goals.

The concepts of reliability and trustworthiness extend the conceptual framework I introduced in the previous section. I will now investigate whether this framework yields new results when applying it to voting technology.

6.4 Trust in voting systems

Voting is a way to surrender oneself to a representational body in a democracy. It is at the same time a reconfirmation of the social contract between the rulers and the ruled, and a reconfirmation of the autonomous individual that engages in this contract. In this act, the Enlightenment ideals are established over and over again. The reconfirmation of the social contract and the autonomous individual has the character of a ritual. The associated relation of assurance is primarily based on familiarity, for a ritual always has an orientation towards the past.

But this ritual dimension is not the only relation of assurance in democratic politics. There are also expectations involved about the functionality of the political system, for example the expectation that the desires of the public are accurately represented in policy by this system. Engaging in political activities such as voting requires confidence or trust that these expectations will be fulfilled. Finally, there is also a need for trust or confidence in the present government, which represents the people based on expectations not about the political system in general, but about the current policy.

Thus, elections involve at least three different relations of assurance: the familiarity with democracy that is established by means of a ritual, the confidence or trust that people have in the government and confidence or trust in the political system.[71]

However, trust or confidence in the election procedures themselves is also necessary. These in turn co-evolve with the relation of assurance that people have with the government and the political system. This means that a lack of trust or confidence in election procedures may reduce trust or confidence in the government or the political system, but also the other way around. The specific characteristics of this relation are a topic for further research. In this section, I will focus on trust and confidence in the election system. I will primarily discuss the differences that can be observed from this point of view between the traditional paper systems and electronic variants.

Why would we want electronic voting in the first place? The rigidity of technology is often an argument. Errors with paper ballots, as in the Florida presidential elections in 2000, may be a reason to switch to the supposedly more reliable Direct Recording Electronic (DRE) machines. Indeed, electronic machines may be more reliable with

[71] Generally, people have confidence with regard to politics rather than trust, in Luhmann's sense. It is precisely the phenomenon of elections that may turn political confidence into trust: "A relation of confidence may turn into one of trust if it becomes possible (or is seen to be possible) to avoid that relation. Thus elections may to some extent convert political confidence into political trust, at least if your party wins. Conversely, trust can revert to mere confidence when the opinion spreads that you cannot really influence political behaviour through the ballot." (Luhmann, 1988).

respect to *safety* than paper systems are, because possibilities for error, both in casting and in counting, are reduced.

However, reliability and trustworthiness with respect to *security* are not as straightforward, especially when there is little transparency in the design, e.g. when the source code is kept secret. Acquiring trust in security, as opposed to trust in safety, is hard when things are secret. If independent institutions check the design of the machines, and no-one would want to manipulate anything, it can be assumed that they are safe. However, if we believe that evil people exist, things change. Insider attacks against security, e.g. an employee of the manufacturer changing something in the software before installing it on the machines, are indeed pretty easy in such a case, and experts evaluating the risks will at some point realise this. This not only includes possibilities for altering the results, but also the possibility to deduce a relation between a voter and a vote. This lack of transparency may make it hard as well to maintain public confidence in the long run, since this confidence is often influenced by expert trust.

Next to the distinction between security and safety, I also proposed a distinction between private effects and public effects. Assurance with respect to private effects in voting amounts to trust or confidence that one's own vote is handled correctly, e.g. kept confidential. Assurance with respect to public effects means trust or confidence that the results are calculated correctly. *Both* kinds need to be acquired by an election system. People may have confidence in electronic systems in the sense that they calculate the results correctly in general, but if they are not sure what happens to their own vote – e.g. doubt the secrecy of their vote – the whole system may not acquire confidence anyway.

In the previous section, I argued that congealed procedures are more suitable for confidence, whereas human procedures are more suitable for trust. Still, because the paper system has been the only option for a long time, the relation of assurance people had with the paper system was largely based on confidence. Confidence in the election system, confidence in the government and confidence in the political system supported each other. Now, what happens when electronic voting comes into play?

Electronic voting systems *may* be seen as alternatives to the existing system. Whether this is indeed the case depends on the situation, for example on whether the monstrous character of the technology has been exposed. If they are seen as alternatives, people suddenly get the option to *choose* a voting system. This invites actively assessing 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. This, again, leads to the traditional paper system becoming *more* attractive, because it is based on human procedures, and human procedures more easily acquire trust than congealed procedures. 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.

If various alternatives are available, and citizens cannot assess the risks themselves,

it can be desirable to establish a balance between expert trust and public confidence, in order to establish a relation of assurance between citizens and the election system again. This is important for maintaining people's confidence in the government and the political system. However, if people do not see these options as alternatives, risk analysis may instead break their confidence in the existing system by exposing the risks, and thereby destroy confidence. Thus, the role of the expert in these matters is extremely important.

As an example of the value of this approach for the analysis of concrete developments, I propose some hypotheses as explanations for the fact that in the Netherlands, electronic voting machines have been introduced in 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. Possible hypotheses for the smooth and uncontroversial introduction are:

- the ritual of going to the polling station, identifying oneself and casting a vote remained fairly stable (as opposed to online voting), maintaining familiarity;[72] also, the Dutch machines have a layout that is very similar to the paper ballots used before;[73]

- confidence in the government was relatively high, which led to confidence in the election systems proposed by the government as well;

- trust and confidence in information systems were more related to safety than to security at the time; people knew that calculators were reliable, and probably no one had ever attacked a calculator;

- voters paid more attention to the election outcome (public effects) than to what happened to their own vote (private effects); they knew that computers were able to calculate reliably, and therefore had confidence in the computers with respect to the public effects; focusing instead on the private effects of a machine "stealing" or revealing one's vote will expose the lack of transparency and probably undermine confidence;

- 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 to the new systems; nowadays, trust *is* an issue in many countries, including the Netherlands: e-voting is really seen as an *alternative*, instead of just automating a known process;

[72] In relatively new democracies, such as Estonia, tradition (and thus familiarity) are less important. This may explain why Estonia already implemented Internet voting. See e.g. `http://www.euractiv.com/Article?tcmuri=tcm:29-145735-16&type=News`, consulted November 17, 2005.

[73] This means, among other things, that all candidates have their own button on the machine, as opposed to PC software in which one first chooses a party and then a candidate.

– risk evaluation of computer systems was not as mature at the time as it is now; this made it harder for computing scientists to transform confidence into trust by making explicit the risks involved.

Each of these possible causes, which are based on the philosophical analysis in this chapter, can serve as a hypothesis for empirical research. Also, the fact that voting machines are now under discussion in the Netherlands as well may be explained by a change in situation with respect to these hypotheses. The anti-e-voting activist group was set up after the founders experienced e-voting for the first time themselves, in Amsterdam. They made a distinction, and thereby created a set of alternatives, thereby changing the expectations from reliability to trustworthiness. These hypotheses show the relevance of the current conceptual framework for voting system sciences in general. Of course, some of them are related, and further research, both theoretical and empirical, would be useful to determine these interdependencies.

6.5 Conclusions

In this chapter, I described a framework for discussing trust in relation to voting procedures. Instead of distinguishing between actual and perceived security, I took a phenomenological approach, in which subjective and objective aspects of security are seen as constituted from the relation between the people and systems involved. The main concepts were discussed both from a computing science point of view and from a philosophical perspective. Luhmann was the primary source for the latter.

Based on the theory of Luhmann, I distinguished between familiarity, confidence and trust. Luhmann understands these concepts as means for the reduction of social complexity. Familiarity has an orientation towards the past, whereas confidence and trust are based on expectations and thus oriented towards the future. People trust because they want to, based on risk evaluation. People have confidence because they have to, not because they understand the risks. Confidence is related to danger, and trust to risk: trust requires comparison of alternatives, and a decision.

The concepts of confidence and trust are related to the different views on trust that can be found in the computing science literature, namely bad and good trust. These are again related to negative and positive conceptions of security, respectively. Computing scientists generally try to replace confidence with trust by making explicit the risks involved in using the system. This, again, allows the public to base their confidence on expert trust.

The "objective" aspects related to the "subjective" aspects of confidence and trust were labelled reliability and trustworthiness. Human procedures are typically good at being trustworthy (and thus at acquiring trust), whereas the congealed procedures of computers are good at being reliable (and thus at acquiring confidence). The terminology around confidence and trust is summarised in table 6.1.

In elections, the traditional election system, whatever it may be, always invites confidence, precisely because it is the established system, and people are not conscious of

confidence	trust
danger	risk
reliability	trustworthiness
no choice	alternatives
habit	analysis

Table 6.1: Confidence and trust: an overview

alternatives. When new technologies for elections are presented, these may be seen as alternatives. Then, election systems suddenly have to be trustworthy instead of reliable only. This is one of the reasons why the demands posed on new election technologies are often more severe than those posed on existing systems. However, the fact that alternatives are now available may also undermine confidence in the existing system, and require this system to earn trust as well.

In this situation, an interdisciplinary approach to matters of trust in election systems is indispensable. The hypotheses I offered for the smooth early introduction of voting machines in the Netherlands serve as a modest attempt at illustrating possible results. I hope to have justified trust in the benefits of such an approach here.

For our analysis, these conclusions mean that the exposure of the monstrous character of e-voting can lead to new requirements for e-voting systems: they need to be trustworthy instead of reliable only, both with respect to safety and with respect to security, because they are now seen as an alternative to paper voting. This holds for both safety and security.

These requirements, however, are related to the way in which we tame the monster. Embracing, expelling and assimilating can be done without clearly distinguishing between alternatives, and therefore without trust. Monster embracing only requires confidence in the new technology; monster expelling requires confidence in the existing arrangements. Even monster adaptation can be understood in terms of a combination of the two types of confidence: if we do not believe that e-voting can be secure, but we do have confidence in its benefits, we need a paper trail. In a sense, these strategies serve to undo the need for trust, by diminishing the visibility of alternatives, and thereby reducing the need to adapt our categories.

As long as we do not wish to challenge the existing categories, we can do without trust in Luhmann's sense. Once we choose monster assimilation, however, trust is necessary rather than confidence. We cannot adapt our categories to a new technology without comparing it – as an alternative – to existing ones. In the process of comparing, new categories can be formed to describe and analyse the new phenomenon, and relate it to existing ones, at the same time establishing trust (or distrust).

Trust cannot be established without comparing, without analysing. If e-voting is to be trusted, we therefore need ways to analyse its features, especially its security. This means that society will have to find means for analysing the requirements that the systems have to meet. Computing and information sciences can play a role here.

What I will do next is study in more detail the way in which scientists transform confidence into trust. In order to do this, they need to define very precisely the requirements that have to be met. This allows them to compare alternatives, and base trust on a risk analysis of the chosen alternative. How do they do this?

Part IV

Science

Chapter 7

Consulting the Scientists

"The true contrast between science and myth is more nearly touched when we say that science alone is capable of verification"

– George Santayana (Spanish born American philosopher, poet and humanist, 1863–1952)

This chapter discusses from the perspective of technology and formal definition the five requirements of e-voting that were distinguished earlier based on literature study (section 2.5). Defining properties of technological systems formally, a task computing science performs in relation to information technology, is necessary to be able to compare alternatives, and thereby replace confidence with trust. After having exposed various technical means used to implement e-voting, I will describe the tasks of defining and ensuring availability, authenticity, correctness and secrecy, and various ways in which the verifiability requirement can be implemented. Following the focus of my research, verfiability is discussed most extensively, and the sections on correctness and secrecy are somewhat longer as well.

Throughout the chapter, the leading question is on how to *define* the desired properties. The question on how to *check* the properties, which is also very relevant from a computing science perspective, is of less importance in understanding the controversies, and will only be mentioned briefly.

Throughout this chapter, formal or technical details will be presented as figures in boxes like this. Readers not interested in these aspects can skip such parts.

7.1 How to secure electronic voting

Various techniques have been used to safeguard electronic voting protocols from manipulation. In advanced systems from academia, a distinction can be made (see e.g. (Hirt and Sako, 2000)) between protocols based on mix-nets, protocols based on blind signatures and protocols based on homomorphic encryption. These systems have rarely been used in elections though. More practically oriented systems have been based on public key infrastructures, randomised ballots, and hashes. If we do not focus on the electronic possibilities for securing information only, visual cryptography, voter verified paper audit trails and trusted parties can help in achieving security goals.

In order to give an overview of the field, each of these techniques will be described briefly in this section. This serves as a basis for the discussions on the five requirements in the following sections. I start with an explanation of the general use of cryptography in voting.

Cryptography

Key to all secure electronic voting systems is the use of *cryptography*, often abbreviated to "crypto": technology developed in order to protect information by manipulating the information itself. Cryptography can be used to protect the *confidentiality* or *integrity* of information. The former is realised by *encryption*, the latter by *signing*.

Encryption means scrambling data according to a certain procedure, such that they become unrecognisable. Typically, a *key* determines how the data is encrypted. A key is also needed for decryption, the recovery of the original data. This key may be the same as or different from the encryption key. The science of developing, analysing and testing encryption schemes is called *cryptology*.

If the same key is used for encryption and decryption, we speak about *symmetric* or *secret key* crypto. If different keys are required for encryption and decryption, we call this *asymmetric* or *public key* crypto. The main advantage of public key crypto is that we reduce the problem of establishing a shared key before the transaction. Instead of having to define a shared secret key for each pair of users, a *certificate* ascribes a *public key* to a person or organisation. This public key can be used to send secret messages to that agent, which only the agent itself can decrypt using its *private key*.

The other way around, the agent can use its *private key* to *sign* messages. The signature can be checked by anyone in order to verify the integrity of the data, using the *public key* in the certificate. The certificate, in its turn, is signed by a higher authority to ensure its authenticity.

Secret-key crypto is generally much faster than public-key crypto. Secure websites typically use public-key crypto for authentication, based on the site's certificate, during which a *session key* is established. The session key is used in a secret-key scheme for the remainder of the transaction.

It is important to realise that most of these techniques provide *computational*

security as opposed to *unconditional* security. This means that security is based on mathematical problems that are *hard* to solve, but not impossible. If one solves the mathematical problem, one can break the confidentiality or integrity of the messages sent. It will take more than a reasonable amount of time to solve them with current computers. If computers get faster, we may start using longer keys to keep new data secure. However, if someone for some reason stored data encrypted using the *old, short* numbers, these may then be easily recovered. If it is required that votes be stored for a long time after an election, this should be taken into account.

Future developments, such as quantum computers, may more fundamentally challenge these assumptions. If we manage to build real quantum computers, the mathematically hard problems may not be hard for these new machines at all, even if we use bigger numbers. On the other hand, new techniques are being developed that use quantum primitives to provide so-called "unconditional" security, which is not dependent on limits of computational power. If these developments are successful, they may have major consequences for e-voting systems.

PKI

PKI stands for *Public Key Infrastructure*. Voting systems based on PKI, such as the Estonian system, typically use the system of public keys and certificates also applied to for example e-commerce websites. In the Estonian system, the voter encrypts the vote with the election's public key and then signs it with her own private key to prove authenticity. Such systems require each voter to have a certificate and a private key. The private key must be available to the voter in a way that is both secure and easy to use. In the Estonian case, the private key is embedded in a smartcard. Then, voters will need a smartcard plus an installed smartcard reader to be able to vote on their own computer. Due to the limited availability of smartcard readers among voters, PKI-based systems may not be the best in terms of accessibility.

Blind signatures

Normally, one signs a message that one knows the contents of. It would be possible to put a signature on a message on carbon paper within a sealed envelope. In this way, I could decide to sign *exactly one* message for each of my friends, after identifying them.

The electronic equivalent of this procedure is called a *blind signature* (see e.g. Chaum (1983)). Blind signatures are useful if we wish to allow voters to choose their own election credentials, e.g. a key used to encrypt their vote. They can do this without having to reveal this information to the authorities, through the blinding procedure. They "blind" the information, have it signed, and "unblind" it again. By means of this method, a combination can be achieved of authenticity and anonymity of the vote. Still, the communication channel will need some extra protection, since it is otherwise easy to see from which computer a vote originates.

Mix-nets

When using a ballot box, votes come out in an order different from the order in which they went in. This ensures anonymity of the voters. How to do this electronically? In mix-nets (see e.g. Sako and Kilian (1995); Abe (1998)), encrypted messages are passed on between different authorities, making sure that no-one can derive a relation between the messages going in and the messages coming out. Basically, this is done by having each authority change the order of the votes. The authorities have to prove that the *content* of the messages is still the same after they shuffled them. After the last step, the votes are decrypted. This technique can be used in voting, to make sure that no-one can gain any information from the *order* of the votes, unless *all* of the authorities cooperate. In this way, it is made sure that votes are kept anonymous.

Homomorphic encryption

Another way to ensure anonymity is to count the votes *while encrypted*. In this way, we calculate a result from the individual votes without revealing the contents of each individual vote. This is exactly what homomorphic encryption achieves (see e.g. Cramer, Franklin, Schoenmakers, and Yung (1996); Cramer, Gennaro, and Schoenmakers (1997); Hirt and Sako (2000)). For example, we may *multiply* all the encrypted votes to ensure that if we decrypt the result, this represents the *addition* of the original votes.

Visual cryptography and randomised ballots

Many systems employ a "take-one-destroy-one" principle to ensure security. In such a scheme, the vote consists of two parts, which are kept separated, and which do not reveal the vote individually. One example is the visual crypto scheme by Chaum (2004). Here, two visual patterns can be combined to a pattern revealing the vote. Prêt-à-Voter by Chaum, Ryan, and Schneider (2005) has a similar setup. Here, the voter takes a receipt, but the order of the candidates on the ballot will be destroyed. The order is different on each ballot. The particular order belonging to a ballot can only be recovered through processing by a mix-net, such that each individual vote is kept secret, by separating the vote and the order of the candidates on the ballot. Usability may be a weak factor in these schemes, since voters will have to perform more complicated tasks. Also, voters are prevented from "preparing" their vote at home by finding the name of the candidate on a pre-published candidate list. On the other hand, putting the candidates in different order on each ballot may improve the fairness of the election.

One of the threats to online voting is the possibility of a virus on the voter's computer altering the vote. Randomised ballots may also help to prevent such attacks. Each candidate is then represented by a number, but these numbers are different on each ballot. If the ballot is sent to the voter via traditional mail, and the voter only has to enter a number on a website, it is nearly impossible for the virus to change the

voter's choice into one for the party of the virus's choice. This technique was used in the Dutch KOA online voting experiments of 2004.

Commitments

Some voting systems allow anyone to calculate the result. This can be done by providing before the election a table which can be used to count each possible individual vote. Of course, one cannot put the possible votes themselves in this table, because that would allow people to copy them and send them in as fake votes. However, there are ways to identify some piece of information uniquely (at least with very high probability), without revealing the information itself. Such arrangements are called *commitments*. What is put in the table instead is a *fingerprint*, a *hash* of each vote.

A hash is a cryptographic operation that assigns to a possibly long document a relatively small sequence of bits. The operation should satisfy the following properties:

- a hash can efficiently be computed from a document;
- it is hard to reconstruct the document from the hash;
- it is hard to find two documents with the same hash.

These properties prevent the reconstruction of valid votes from the table, but when a vote is received it can easily be looked up and counted.

Trusted parties

Not all security is technical. It is doubtful whether a technically perfect system can be built, and if so, whether it would be practical. Often, the security of the whole system is based on procedural as well as technical measures. The procedural measures should include a division of responsibilities. In this way, the voter will not have to have full faith in one organisation, but she can be confident that problems can only occur if *all* of the involved organisations cooperate. The RIES system (section 7.2) could be improved by a better separation of tasks (Hubbers et al., 2005).

Still, even in standard public key crypto, we need trusted organisations to sign the certificates that ascribe a public key to a person. Also, in some communication protocols it is assumed that one of the participants is fair. This participant is usually called a trusted third party (TTP). How much trust we should really place in such parties when it comes to voting is a legitimate question.

Voter verified paper audit trails

A solution to improve the security of electronic voting that has become very popular in the US is the Voter Verified Paper Audit Trail, as proposed by Rebecca Mercuri Mercuri (2002). More than half of the states in the US have now passed legislation making a paper trail mandatory.

Some people argue that a VVPAT does not help much in improving security, because people will have a hard time checking their vote, due to the large number of races on which they have to vote in a single election in the US. It has been suggested to use an audio trail instead (Selker and Goler, 2004). Also, an important question is what to do if the electronic trail and the paper trail differ. Which one has to be preferred? It could be argued that for small differences, the electronic trail will probably be the more *reliable* one, whereas for larger differences, the paper trail may be more *trustworthy*.

7.2 An example system

Throughout this chapter, the Rijnland Internet Election System (RIES), used in Dutch water board elections and for citizens staying abroad in the Dutch national elections in 2006, is used as an example. This is not because it is judged to be the best system, but it is certainly one of the systems the present author is most familiar with (Hubbers et al., 2005).

The RIES system uses hashes to publish a pre-election table. Once the votes have been published, anyone can calculate the result of the election from the pre-election table and the table of received votes. The system was developed by the water board of Rijnland in cooperation with the company TTPI, based on earlier work by Herman Robers (1998). Because of the use of hash functions, the system is relatively simple, offers protection of votes and allows scrutiny of the results. Whereas the hashes of all possible votes are public, it is infeasible[74] to deduce valid votes from them without the required voter key.

The system works as follows. First of all, a reference table (see figure 7.1) is published before the elections, including (anonymously) for each voter the hashes of all possible votes, linking those to the candidates. The original votes are only derivable from a secret key handed to the voter. The confidentiality of these keys is achieved via organisational security measures, in the same way that identification codes for bank cards are handed out. It is possible to compare the number of voters in this table with the number of registered voters.

In the voting phase, voters use their secret to derive a valid vote for their desired candidate. This vote is then submitted to the server via an encrypted connection.

After the elections a document with all received votes is published. This allows for two important verifications: a voter can verify his/her own vote, including the correspondence to the chosen candidate, and anyone can do an independent calculation of the result of the elections, based on this document and the reference table published before the elections. If your vote has been registered wrongly, or not at all, you can detect it. And if the result is incorrect given the received votes, you can detect it as well.[75]

[74] Infeasible here means computationally infeasible. Although this is not an absolute guarantee, the probability of being able to guess the correct values in bounded time is negligible.

[75] Of course, procedures need to be put in place to decide what will happen in case of such a claim.

```
Archive:  01010204.zip
  Length     Date   Time    Name
 --------    ----   ----    ----
     2172  08-25-04 09:32   01010204/RT_0.zip
     4017  08-25-04 09:32   01010204/RT_1.zip
     2173  08-25-04 09:32   01010204/RT_2.zip
     1865  08-25-04 09:32   01010204/RT_3.zip
     2789  08-25-04 09:32   01010204/RT_4.zip
     3097  08-25-04 09:32   01010204/RT_5.zip
     2787  08-25-04 09:32   01010204/RT_6.zip
     1559  08-25-04 09:32   01010204/RT_7.zip
     1559  08-25-04 09:32   01010204/RT_8.zip
     2480  08-25-04 09:32   01010204/RT_9.zip
     2784  08-25-04 09:32   01010204/RT_A.zip
     3405  08-25-04 09:32   01010204/RT_B.zip
     2785  08-25-04 09:32   01010204/RT_C.zip
     1867  08-25-04 09:32   01010204/RT_D.zip
     1559  08-25-04 09:32   01010204/RT_E.zip
     3403  08-25-04 09:32   01010204/RT_F.zip
        0  08-25-04 08:51   01010204/
 --------                   -------
    40301                   17 files


Archive:  RT_0.zip
  Length     Date   Time    Name
 --------    ----   ----    ----
      220  08-25-04 09:31   008AB1E98AEDFBA450A1813DDC153553
      220  08-25-04 09:31   08677B73378E1D59153DE30263A3C47C
      220  08-25-04 09:31   06CAC042AF7D6940DD8A51814E68DFF8
      220  08-25-04 09:31   00FEA51461FBF7B406554EEF2E23554D
      220  08-25-04 09:31   05C02BD8E3863DB24D6C332A17B78EFB
      220  08-25-04 09:32   070C60BFFC06B7355425E6FFADBBED30
      220  08-25-04 09:32   034C37BA687E21477D38A110954207B8
 --------                   -------
     1540                   7 files

008AB1E98AEDFBA450A1813DDC153553:

vervangend=0
verstrekt=1
vervallen=0
AC94983743058334B25452E0F63A9C20=0101020401
B0015BAC8ECF766DB67825592DC10957=0101020402
ACE42133255CA8184D18E0293FEF7EE8=0101020403
358AAB0C934757ACCF071A1CD732EDEA=0101020499
```

Figure 7.1: Reference table format. The reference table in the figure has been split into 16 parts, which reside in different archive files. Each archive file (e.g. `RT_0.zip`) contains files for different voters, indicated by the hash of the voter's identity. In these files, hashes of possible votes of such a voter are mapped to the corresponding candidates (e.g. candidate `0101020401`).

The main problem in the RIES system is the responsibility of the key generator to destroy the keys immediately after sending them to the voters. Failing to do this may compromise both the secrecy and the authenticity of votes. We may wish to improve on this issue by having the voters generate their keys themselves. Here, blind signatures may be useful: the voter can have exactly one key signed by the authorities, without making it public.

Another problem is that the verification procedure might be used to sell votes. If I let someone else verify my vote, he or she could pay me for making the right choice. If I would need a smartcard to verify a vote, this would already be less easy, but this would limit the accessibility and usability of the system.

7.3 Availability

Technical solutions to e-voting problems abound, but there is as yet no accepted standard. How can we make sure that solutions meet the requirements? I have mentioned five requirements that are often thought to apply to e-voting systems: availability, authenticity, correctness, verifiability and secrecy.

The requirement of availability states that each eligible voter should be able to cast her vote. Traditionally, this requirement has been translated into demands on the robustness of voting machines, i.e. their safety (as opposed to security). They should be able to resist shocks, high temperatures, et cetera. Moreover, availability implies that voters should be able to operate the machines. Therefore, the design of the interface of the machines should be as simple as to allow people without experience with similar devices to use them independently. Availability implies usability.

Availability is not only a safety requirement though. Malicious individuals may try to disrupt the voting services intentionally. With offline voting machines, this usually requires physical access to the devices. With online computers, whether intended for remote electronic voting or not, hackers may try to access and take down the machines from anywhere by requesting many fake connections. Such actions are called *denial of service attacks* (DoS). Hackers may even try – by means of spreading viruses or otherwise – to create a network of computers that will attack the voting services simultaneously. We then speak of a *distributed denial of service attack* (DDoS).

A question very relevant to online voting systems is whether we can prevent such (D)DoS attacks. Technical solutions, such as firewalls, will help, but possibly not enough to rule out interruptions to the service completely. The main problem is that it is in practice impossible to distinguish fake vote attempts from genuine ones. It may be necessary to implement one or more backup servers, but then we need to make sure that the servers are synchronised, i.e. that someone cannot take advantage by voting on multiple servers without being detected.

The trade-off is about centralisation versus decentralisation. We can either set up a few strongly protected servers, but if they can be made to fail, the system will be down. Or we can distribute the service over many weakly protected computers, and in this way make it difficult to take down all of them. This requires considerable communication overhead though, to make sure that each of the computers has up-to-date information about the status of the election.

Finally, the question is how we can show that a certain system meets the availability requirement. This is a more complicated issue than the same question for different requirements, because availability depends on many different factors (hardware, software, user interface, environment). Availability in a narrow sense means that these should not break down easily, for which environmental conditions can be specified and tested. When security comes into play, it should also be tested that attackers cannot take down the system, for which "hackers" can be hired. Still, this does not mean that we know how to define and prove availability properties. Formal verification of availability properties is therefore rare.

7.4 Authenticity

The requirement of authenticity states that only eligible people can vote and that no one should be able to vote more than once. To meet these requirements, the system should provide voter *identification* and voter *authentication*. Identification means that the voter has a way to present her identity. Authentication means that the voter can *prove* that this is really her. Usually these two functions are combined, for example in presenting a passport, a username-password combination, or a smartcard.

Though largely outside the scope of my own project, authentication is a serious issue, especially in remote electronic voting. It can be done based on three types of tokens: what you *know*, what you *have* and what you *are*. The first type is typically based on some kind of password. The second can be implemented via a smartcard. The third type is usually some kind of biometric authentication, e.g. a fingerprint or a facial scan. In the order in which the types are presented here, they range from very vulnerable to impersonation to quite resistant to impersonation.

A password is very easy to transfer, a smartcard a bit more difficult and a finger hard.[76] For remote electronic voting to be feasible, probably something better than passwords has to be implemented, like the Estonian identity card. An additional advantage of the Estonian solution is that the authentication tokens can be used for many different things. This feature may be used with passwords as well. If handing over a password to someone else means that they have access to your bank account, you are less likely to do so in an election.

Verifying authenticity amounts to proving that a voter can only access the system after correct authentication, and that she can only cast one vote. Verification of authenticity properties can be found in e.g. Blanchet (2002) and Gordon and Jeffrey (2003).

7.5 Correctness

The third requirement of elections that I mentioned is the correctness of the result. Each valid vote should be counted, and only valid votes should be counted. The first part of this requirement is also called *completeness*, the second part *soundness* (Pasquinucci, 2007). When computer programs are used to cast and/or count ballots, this requirement – the count is correct given the votes cast – becomes an exemplary case of a correctness problem in computing science.

There are various levels in computing science on which one can speak about correctness. First of all, the *hardware* on which a computer program is running needs to be correct, in order to assure that calculations yield the desired result. Then, the *program* that is being run on the hardware needs to do what it is supposed to do. On an even higher level, the *communication protocol* (i.e. the specification of the messages that are sent between computers) that is implemented in the program should

[76] It is assumed that passwords, keys and biometric properties are chosen and stored in a sensible manner.

be correct with respect to the goals it aims to achieve. In this section, the focus is on correctness of programs.

There are various methods that help us to ensure that a computer program does what it is supposed to do, in this case count the votes correctly. Typically, this requires a *specification* of what the program should do, with mathematical preciseness, and an *implementation* of the program in a programming language, or even in machine language (that is, zeroes and ones). Verification of correctness then amounts to proving that the implementation conforms to the specification.

In Nijmegen, the LOOP tool (for Logic of Object-Oriented Programming) was developed for this purpose (van den Berg and Jacobs, 2001). This tool can verify if a Java program conforms to its specification, by using the PVS theorem prover (Owre, Rushby, and Shankar, 1992). There are similar efforts for other programming languages. Both the LOOP tool and EscJava2 (Kiniry and Cok, 2004) are based on a specification language for Java programs called JML (Leavens, Baker, and Ruby, 2006). EscJava2 is faster and can do automatic verification. The LOOP tool can handle more subtle cases, but requires interaction and is therefore slower and less easy to use. These tools were used to verify a counting application for the first Kiezen op Afstand (KOA) experiment of the Dutch Ministry of the Interior and Kingdom Relations (Hubbers, Jacobs, Kiniry, and Oostdijk, 2004).

However, the LOOP tool itself consists of many lines of code, and is therefore a complex piece of software architecture. If the tool is used to prove that programs are correct, how can we be sure that the tool itself is correct? Indeed, I fixed some errors in the definitions used to prove correctness, including one in the translation of the array initialisation routine.[77] This is not to say that the tool was badly designed, but it does point out the intricacies of verification efforts.

Some people argue that only a very small amount of code in such tools should be critical, meaning that if that part is correct, the whole system is correct. This small part can be checked and re-checked by hand. However, if the errors are in the *translation* of Java code to the language of the tool, correctness of the proof tool itself does not matter.

The complexity of Java semantics is itself high enough to induce more or less certain mistakes in such translations. Still, we now have two *independent* processes that should lead to the same result: the program itself, and the verification of the program. If the verification finds an error, but the program behaves as desired in precisely this case, there must be something wrong with the tool. The proof of correctness is a limited proof; it assumes that the tool itself is correct, which is an assumption that can always be challenged (if only for possible mistakes in the hardware of the machine on which it is run).

If we check the code only at the programming language level, we have the remaining problem of verifying that this code is actually run during an election. This problem is considered very hard. The compiler, the program that translates the program into machine code, needs to be correct to be sure that the machine code

[77] Arrays are programming constructs in which multiple values of the same type can be stored, e.g. a list of 10 numbers, or a table of 26 times 26 characters.

corresponds to the desired behaviour. And then we have to check that the machine code on the computer used in the election is indeed the correct code. Of course, if the computer is malicious, it can lie about this. Therefore, the verifiability requirement is very important in electronic elections: even if the wrong code is used, errors should be detectable using other means.

In order to meet the correctness requirement, the *integrity* of the votes and the results has to be protected. This is the security variant of the safety property of correctness. Whereas verifying correctness aims at preventing errors, integrity means that unauthorised persons should not be able to alter data when trying to disrupt the system. Integrity can be protected by means of encryption, hashes and digital signatures. If the program calculates correctly, and the data cannot be altered before, during or after execution, the result must be correct as well.

7.6 Privacy, secrecy and anonymity

The fourth requirement in elections is that the ballot should be secret. This means a couple of things: the identity of the voter should not be visible together with the vote and it should not be possible to link a vote back to the voter.

The following concepts may be used in connection with the secret ballot:

- secrecy: sensitive information is kept confidential;
- privacy: personal information is kept confidential;
- anonymity: personal data is not linked to other data.

In voting, the voter's identity is *not* a secret. In the end, we know which citizens voted in a given election. The vote is not secret either; it cannot be secret, for then it could not be counted. What is secret is the *relation* between voter and vote. This is an *unlinkability* property, which is usually seen as an aspect of *anonymity* (Garcia, Hasuo, Pieters, and van Rossum, 2005).

Unlinkability is not the only possible interpretation of anonymity. Different categories of anonymity have been proposed in the literature (figure 7.2).

To define anonymity properties, the symbols $\Box$ and $\Diamond$ are used. $\Box_X \phi$ means that agent X *knows* that ϕ is the case. $\Diamond_X \phi$ means that agent X *suspects* that ϕ is the case, i.e. that X does *not* know that ϕ is *not* the case. Of primary interest is what the attacker in the model knows. The attacker is called spy and the set of agents between whom the spy should not be able to distinguish (called the *anonymity set*) is denoted AS.

Definition 7.1. (Sender anonymity) Suppose that r is a run of a protocol in which an agent B receives a message m. We say that r provides *sender anonymity* with

anonymity set AS if it satisfies

$$r \models \bigwedge_{X \in \mathsf{AS}} \Diamond_B(X \text{ Originates } m).$$

This means that, as far as B is concerned, every agent in the anonymity set could have sent the message.

Definition 7.2. (Unlinkability) We say that a run r provides *unlinkability* for agents A and B with anonymity set AS if

$$r \models \big(\neg\Box_{\mathsf{spy}}\varphi_0(A,B)\big) \wedge \bigwedge_{X \in \mathsf{AS}} \Diamond_{\mathsf{spy}}\varphi_0(X,B)\ ,$$

where $\varphi_0(X,Y) = \exists n.\ \big(X \text{ Sends } n \wedge Y \text{ Possesses } n\big)$. Intuitively, the left side of the conjunction means that the adversary is not certain that A sent something to B. The right side means that every other user could have sent something to B. Similarly, unlinkability between a user A and a message m could be defined as $\models \neg\Box_{\mathsf{spy}}(A \text{ Sends } m) \wedge \bigwedge_{X \in \mathsf{AS}} \Diamond_{\mathsf{spy}}(X \text{ Sends } m)$.

Definition 7.3. (Plausible deniability) In certain circumstances (e.g., relays), agents might be interested in showing that they did not know that they had some sensitive information m. This might be modelled by the following epistemic formula:

$$r \models \Box_{\mathsf{spy}}\neg(\Box_A(A \text{ Possesses } m))\ .$$

This formula is read as: the spy knows that A does not know that she possesses m.

Figure 7.2: Definitions of anonymity by Garcia et al. (2005).

In addition to the vote being kept anonymous by the system, a voter should not be able to prove a relation between herself and a particular vote, *even if she wants to*. This requirement aims at preventing coercion and vote buying. This additional property is called *receipt-freeness* (Benaloh and Tuinstra, 1994; Delaune, Kremer, and Ryan, 2006). In remote electronic elections, it is hard to prevent a voter from having someone look over her shoulder when voting. However, we can prevent the voter from proving *remotely* what she voted for. In order to meet the requirement of receipt-freeness, the voter should not be able to store information that can reveal to a coercer *after the election* which choice she made.[78]

In the anonymity framework, the concept of anonymity set is used to define the set of users between which an observer should not be able to distinguish. To apply the

[78] She can, however, still record a video of the process, which is a problem in polling stations as well.

framework to votes, we need to adapt the concept of anonymity set. In voting, we are sure that each (actual) voter submits a vote. Therefore, the point is not whether any other user in an anonymity set could have sent the message, but *whether the voter could have submitted any other vote*. Therefore, we define an anonymity set of *messages*, AMS , instead of an anonymity set of agents. This set typically consists of all possible votes.

To be able to define receipt-freeness, we need to have a way to extend a given run with one message: the receipt. We write this as $r.(A \rightarrow B : m))$ for a given run r, message m (the receipt), sender A and receiver B. For A to be able to send the receipt, she needs to have the message in her possessions at the end of the original run ($\mathsf{Poss}_{\mathsf{IPo}}(r, A, |r| - 1)$). The new run does *not* need to be a run of the protocol. It *does* need to be legitimate with respect to the initial possession function.

Definition 7.4. (Weak receipt-freeness) A run of a protocol is *weakly receipt-free* for agent A with respect to message m iff for all $m' \in \mathsf{Poss}_{\mathsf{IPo}}(r, A, |r| - 1)$,

$$r.(A \rightarrow \mathsf{spy} : m') \models \neg\Box_{\mathsf{spy}}(A \ \mathsf{Sends} \ m)$$

Weak receipt-freeness implies that the voter cannot prove to the spy that she sent message m during the protocol, where m is the part of a message representing the vote. However, this notion is still fairly limited. For example, suppose that the spy wants the voter to vote for party X. Suppose, furthermore, that the voter instead chooses to vote Y, which is represented by message m in the above definition. Now, if the voter cannot show that she voted Y, this protocol is receipt-free with respect to the definition above. However, if the spy can acquire information which proves that the voter did *not* vote X, the spy will not be satisfied. Therefore, we introduce a stronger notion of receipt-freeness as well.

Definition 7.5. (Strong receipt-freeness) A run of a protocol is *strongly receipt-free* for agent A with respect to a message m in anonymity set AMS iff for all $m' \in \mathsf{Poss}_{\mathsf{IPo}}(r, A, |r| - 1)$,

$$r.(A \rightarrow \mathsf{spy} : m') \models (\neg\Box_{\mathsf{spy}}(A \ \mathsf{Sends} \ m)) \wedge \bigwedge_{m'' \in \mathsf{AMS}} \Diamond_{\mathsf{spy}}(A \ \mathsf{Sends} \ m'')$$

Here, no matter what information the voter supplies to the spy, *any* vote in the anonymity set is still possible. This is represented by the "suspects" symbol $\Diamond_{\mathsf{spy}}$. In other words, for all possible votes, the spy still suspects that the voter cast this particular vote; or: the spy is not certain she did *not* cast this vote.

Notice that this definition is analogous to the definition of unlinkability of Garcia et al. (2005) presented in figure 7.2.

Figure 7.3: Definitions of receipt-freeness by Jonker and Pieters (2006).

There is an even stronger version of receipt-freeness, called *coercion-resistance* (Delaune et al., 2006). In that case, the attacker is not only able to receive information (i.e. a receipt) from the voter, but she is also able to *give instructions* to the voter during the protocol. In remote electronic voting, such a situation may easily occur when the coercer can see all the actions of the voter. But in that case, the voter will *never* be free. Therefore, it is usually assumed that the voter has some private channel through which to cast the final vote: a (virtual) voting booth. Then it becomes possible to verify whether a particular voting protocol satisfies this property, given the assumption that a particular action can be done through a private channel.

An alternative way to view the anonymity debate is by focusing on probabilities. Even if an attacker cannot determine with certainty that I sent a certain message, if there is a 99% chance that I did so, I will still have a problem. Bhargava and Palamidessi (2005) introduced the notion of *probabilistic anonymity*. The definition states that a system is probabilistically anonymous if for all pairs of anonymous actions and for all possible observations by the attacker, the probability of the observation given the first action is the same as the probability of the observation given the second action.

However, this notion does not work for voting. If we know the outcome of an election, the probabilities of voters having voted a certain way changes. If, for example, the election is unanimous, we know for sure what each voter voted. Still, this does not mean that the voting system is wrong (at least not from a technical perspective). Weak probabilistic anonymity (Deng, Palamidessi, and Pang, 2005) could be a solution. Here, a value α is used to allow limited changes in probabilities. However, this solution is too ad-hoc to be suitable: the α value would depend on the number of voters.

An alternative option is to demand that it not be detectable if two voters *swap* votes (Delaune et al., 2006). We combined their approach with the idea of probabilistic anonymity, and we propose the following definition, in which A and B are voters, i and j are votes, $v(A, i)$ is the event that voter A votes for candidate i and o is an observation (i.e. what the attacker can see, including the result of the election):

$$\forall A, B \in \mathsf{AMS}\ , \forall i, j \in \mathbb{N}, \forall o \in O :$$

$$p(o \mid v(A,i)\ \wedge\ v(B,j)) = p(o \mid v(A,j)\ \wedge\ v(B,i))$$

A similar definition could be proposed for probabilistic receipt-freeness. This is work in progress (Pieters and Jonker, 2007).

Figure 7.4: Probabilistic anonymity and receipt-freeness.

Thus, anonymity properties are important in voting protocols, and computing science research focuses on precisely (mathematically) formulating these properties. Votes need not be secret, but the relation between voter and vote should be.

However, when we use credentials such as a password or encryption key, we need those to be secret, to prevent others from voting in the name of the voter. Here, we do have a secrecy requirement in the strict sense. Typically, we do not want the password or key to be derivable from messages in the protocol. This is a *confidentiality* requirement, which is usually seen as an aspect of *non-interference* (Goguen and Meseguer, 1982; Jacobs, Pieters, and Warnier, 2005). If we send our vote to the server, we do not want the authorities to be able to derive information about our password or key. Thus, the information sent to the server should be *independent* from our password or key. It *should* be possible to verify if the password the voter enters is correct, but this should not reveal (part of) the password.

A problem in this approach is that the key may be used to encrypt the vote. Or, a hash of the password is sent to the server as a means of authentication. In these cases, the information sent to the server is *not* completely independent from the key or the password. Still, cryptographic properties guarantee that it is very difficult for the server to learn the password from the information received. We would like to allow such dependencies. Currently, research is being done into these issues. The problem is called *declassification* (Askarov and Sabelfeld, 2007).

In order to give a formal definition of confidentiality we first define a relation Rel between memory states, which is parametrised by a labeling function and confidentiality level. The higher the confidentiality level, the more confidential the information. Memory states are of type M, locations in memory are of type Loc and confidentiality levels are of type L.

Definition 7.6. Let $\mathsf{lab} : \mathsf{Loc} \to \mathsf{L}$ be a labeling function and $\mathsf{conf} \in \mathsf{L}$ a confidentiality level. Then the relation Rel is defined as

$$\mathsf{Rel}(\mathsf{conf}, \mathsf{lab}) \subseteq \mathsf{M} \times \mathsf{M} = \\ \{(x, y) \in \mathsf{M} \times \mathsf{M} \mid \forall l : \mathsf{Loc}.\mathsf{conf} \not\leqslant \mathsf{lab}(l) \Rightarrow x(l) = y(l)\}$$

Thus $\mathsf{Rel}(\mathsf{conf}, \mathsf{lab}) \ni (x, y)$ says that x and y can only differ for variables of high confidentiality (where conf is the border). Using the relation Rel we can now give a semantic definition of termination-insensitive non-interference, our notion of confidentiality.

Definition 7.7. Let p be a program and $\mathsf{lab} : \mathsf{Loc} \to \mathsf{L}$ a labeling function. Then confidentiality is defined as

$$\begin{aligned} &\mathsf{Confidential}(\mathsf{p}, \mathsf{lab}) = \\ &\quad \forall x, y : \mathsf{M}.\forall \mathsf{conf} : \mathsf{L}.\ (\quad \mathsf{Rel}(\mathsf{conf}, \mathsf{lab}) \ni (x, y) \wedge \ [\![\mathsf{p}]\!](x) \neq * \ \wedge \ [\![\mathsf{p}]\!](y) \neq *) \\ &\qquad\qquad\qquad\quad \Rightarrow \\ &\qquad\qquad\qquad\quad \mathsf{Rel}(\mathsf{conf}, \mathsf{lab}) \ni ([\![\mathsf{p}]\!](x), [\![\mathsf{p}]\!](y)) \end{aligned}$$

Definition 7.7 states that if all variables with low confidentiality level are equal for all (memory) states x and y before execution of program p, then these same variables

should again be equal in the new states obtained by executing program p for all conf. This guarantees that variables with low confidentiality level are independent of variables with high confidentiality level, and thereby excludes the possibility of leaking information.

Figure 7.5: Definition of confidentiality by Jacobs et al. (2005).

7.7 Verifiability

The fifth and last requirement in our analysis is verifiability. Here, verifiability does *not* refer to verification of programs or protocols. Rather, verifiability denotes the property that the *result of a single election* can be verified. There is a trade-off here: the stronger the guarantees on the correctness and security of the protocols and the programs, the weaker the need to implement verifiability for each election result. On the other hand, when results are verifiable, correctness and security of programs and protocols is a less important issue, although we would of course not want to find discrepancies in each election we run.[79]

In this section[80], the concept of verifiability is investigated vis-a-vis the scientific literature and the concrete developments in the Netherlands. I propose a distinction between various concepts of verifiability.

Voter-verifiable elections

Verifiability of electronic voting systems has achieved a great deal of attention in the computing science literature. In the context of electronic voting machines (DREs), much discussion has taken place around the possible introduction of a "voter verified paper audit trail" (VVPAT) (Mercuri, 2002). Typically, this includes a paper copy of each vote being kept as a backup trail for recovery or recount. This should increase trust in the proper operation of the black-box DRE machines. Also, cryptographic receipts have been proposed, e.g. in Chaum (2004).

In remote electronic voting, it is typically impossible to maintain a paper trail without re-introducing traditional means of communication, such as regular mail. Even then, it is hard to make sure that the electronic trail and the paper trail match, even in case all electronic equipment operates properly.[81] Therefore, quite some research covers fully electronic means of verification.

[79] The part of a computer system that is critical to security is sometimes called the "trusted computing base" or TCB (Lampson, Abadi, Burrows, and Wobber, 1992). Using this concept, we can also say that verifiability of election results reduces the TCB of the underlying computer system, in the sense that security is no longer dependent on the system behaving appropriately, as long as the verifiability function is not broken.

[80] A previous version of this section has been published as Pieters (2006d).

[81] Voters may intentionally send different votes to the different trails, in order to spoil the elections. See e.g. Schoenmakers (2000).

Traditionally, two types of verifiability have been distinguished in research on electronic elections. When a system establishes *individual verifiability*, every voter can check if her vote has been properly counted. In *universal verifiability*, anyone can check that the calculated result is correct (Sako and Kilian, 1995). Typically, a bulletin board or some other electronic means is used to publish a document that represents the received votes. Voters can look up their own vote there, and people interested in the results can do correctness checks on the tally.

However, these types of verifiability have been implemented in very different ways. I think that at least one more conceptual distinction is necessary to categorise the different systems appropriately. I will introduce this distinction via an analysis of the relation between verifiability and receipt-freeness.

Verifiability and receipt-freeness

If a voting system needs to be receipt-free – the voter should not receive proof of her vote – then how can we provide the voter with certainty that her vote has been counted? If we give the voter information that shows how she voted, she may also give this information to a coercer.

Some systems, among which the RIES system, do indeed allow a voter to check after the elections for which party or candidate her vote has been counted (Baiardi, Falleni, Granchi, Martinelli, Petrocchi, and Vaccarelli, 2004, 2005; Hubbers et al., 2005; Malkhi, Margo, and Pavlov, 2002; Storer and Duncan, 2004). These systems are therefore not receipt-free in the technical sense. Although the fact that people can see what they voted for after the elections may increase trust in the system, the lack of resistance against coercion and vote buying makes these systems debatable candidates in elections for which we cannot be sure that the chances of buying and coercion are low.

In many systems (Chaum, 2004; Joaquim et al., 2003; Kim and Oh, 2004), this is remedied by allowing a voter to check *that* her vote has been counted, but not *how*. The idea is that it is infeasible for an attacker to make the system count a different vote for this voter in case the check turns out to be OK. Receipt-freeness can thus be provided by limiting the information that a voter can retrieve about her vote after the election, while still assuring cryptographically that this is indeed a proof that the vote has been counted for the party or candidate that was chosen during the election.

Thus, the relation between individual verifiability and receipt-freeness gives rise to a distinction between two different types of individual verifiability. In the following, I discuss the different options for verifiability in remote electronic elections based on this observation.

Variants of verifiability

Following the analysis of the relation between individual verifiability and receipt-freeness, I propose a distinction between two kinds of individual verifiability. I will label these two types based on an analogy with the distinction between classical

logic and constructive logic. In classical logic, one can prove an existential formula without actually showing an instance in the domain that satisfies this formula.[82] In constructive logic, one has to produce an actual witness in order to prove the existential formula. There is a similarity with verifiability in electronic voting here.[83]

When a voter can only verify *that* her vote has been counted, this amounts to showing that a certain vote exists in the results that can be attributed to this voter. However, the actual witness (i.e. the choice this voter made) cannot be recovered from the verification procedure. Here, the voter will believe that her vote was recorded correctly if the election authority can show something that proves the existence of a vote by this voter in the results, without re-examining the original vote.[84] Proving the existence of something without showing a witness can be done in classical logic. I will label this type of verifiability *classical individual verifiability*.

On the other hand, some systems allow a voter to check afterwards *for which candidate* her vote has been counted. This means that the actual instance of a vote is shown as a proof to the voter. Here, the sceptical voter does not believe the election authority unless she can reproduce the original vote from the results. This corresponds to the proof of an existential formula in constructive logic. Therefore, I will label this type of verifiability *constructive individual verifiability*.[85]

Definition 7.8. Classical individual verifiability is the property of an election system that a voter can verify that her vote has been counted correctly based on a document representing the received votes, *without* being able to reconstruct her choice from that document.[86]

Definition 7.9. Constructive individual verifiability is the property of an election system that a voter can verify that her vote has been counted correctly by reconstructing her choice from a document representing the received votes.

The first type of individual verifiability has become fairly standard in computing science discussions on voting systems. However, the second type has been used in practice as well, and I think these developments deserve some consideration from both a scientific and a political perspective.

For universal verifiability we can make a similar distinction. I take universal verifiability, to prevent confusion, to mean that any observer can verify that the *final tally* is correct, *given a document representing the received votes*. Thus, universal verifiability does not necessarily mean that anyone can check that all cast votes have been included in this document.

Definition 7.10. Classical universal verifiability is the property of an election system that it can be shown that the tally is correct given a document representing the

[82] Equivalently, one shows that the negation of the formula does not hold for all instances.

[83] The analogy does not hold for computational issues around finding a witness. Still, I think that it is useful for understanding what the difference is between the two types of verifiability.

[84] Equivalently, one shows that it is not the case that one's vote has not been counted.

[85] A similar distinction is discussed by Pasquinucci (2007). The terminology used is *secret receipt* for classical individual verifiability and *plain receipt* for constructive individual verifiability.

[86] All types of proof discussed in this section may be relative to cryptographic assumptions.

received votes, without all the data necessary to perform the calculation being publicly accessible.

Definition 7.11. Constructive universal verifiability is the property of an election system that all data necessary for calculating the result from a document representing the received votes are publicly accessible, and that a verifier can compute the tally from this set independently of the election authorities.

Systems in which votes are encrypted with public keys of talliers or mix servers typically establish classical universal verifiability, e.g. via proofs by these servers that show that they did their job correctly, or via homomorphic encryption schemes. This proves that there is a set of votes corresponding to the published document and to the tally, but the calculation of the tally from the document is not public. Constructive universal verifiability is not possible in this case, unless the private keys are made public after the elections. However, this typically violates secrecy requirements; especially in the case of mix servers, the encryption is *intended* to maintain secrecy of the individual votes. In the REVS system (Joaquim et al., 2003), the private key of the election authorities *is* published, but this also sacrifices the receipt-freeness of the system.

Systems which only use public functions to calculate the result from the set of received votes typically do establish constructive universal verifiability (Hubbers et al., 2005; Malkhi et al., 2002; Storer and Duncan, 2004). However, these systems need special measures to prevent the votes from being linked to individual voters. Because the received votes are used in public calculations of results, without any intermediate trusted computations that scramble them, the link between voter and vote should be destroyed in a non-trusted environment beforehand. In the UK, the situation is even more complicated due to the requirement that this link can be recovered in special cases (see section 3.3 and Storer and Duncan (2004)).

Moreover, all the systems I included in my research that offered constructive universal verifiability, *also* offered constructive individual verifiability, and are therefore not receipt-free. For example, the RIES system used in the Netherlands (Hubbers et al., 2005) establishes both constructive individual verifiability and constructive universal verifiability. By looking up one's vote in the table of received votes and matching it to the corresponding candidate in the reference table, one can recover the content of the vote. Also, based on the same tables, an independent recount of the results is possible, involving access to all of the received votes (see section 7.2).

The RIES example shows that systems that allow constructive individual verifiability and constructive universal verifiability are beginning to be used in practice, in small-scale or low-risk elections. Meanwhile, many advanced cryptographic systems that establish classical individual verifiability and classical universal verifiability are being developed. We also saw that when the latter type of systems is adapted in order to offer constructive universal verifiability, constructive individual verifiability seems to appear as a side-effect, and receipt-freeness is thereby sacrificed.

7.8 Security and attacker models

The definitions presented in this chapter suggest that we *can* indeed be very precise when it comes to assessing security properties of information systems. Even though scientists may disagree about the precise meaning of concepts, such (mathematical) definitions make it possible to *measure* security. The definitions introduced in this chapter can be used in such a measurement in a variety of ways.

Two of the most important formal verification techniques are theorem proving and model checking. In the former strategy, one tries to prove statements about security properties of a system, either automatically or interactively. If one succeeds in proving the statement, the system can be judged to be secure with respect to the property considered. In model checking, it is being checked if the desired property holds in each state the system can be in. Advanced strategies may need to be used, since the state space (the number of states) can easily become prohibitively large. Both theorem proving and model checking help us to check properties such as correctness, anonymity and confidentiality systematically.

Apart from these formal verification techniques, testing may be used to measure security properties. Such measurements are less precise, because it is impossible to test each combination of inputs. With formal techniques, it becomes possible to cover *all* possible situations.

How does this relate to our previous discussion of the notion of actual security? First of all, making security properties precise is a valuable activity in its own right. In order to decide between alternatives, we need distinctions on which to base the observations guiding these decisions. This is what computing scientists can contribute. But why does this not count as actual security?

The theoretical argument on the limitations of observation still holds. Even with advanced distinctions based on mathematics, we may still fail to indicate other possibly relevant properties. The mathematical analysis is based on two models: a security model and an attacker model. The first states what it is that we wish to protect, for which we have seen many definitions in this chapter. The second states what an attacker can do in order to break this protection. All judgements about security are relative to these models, just as a judgement about intelligence is relative to the test model, and a judgement about waiting time is relative to the time model used in the clock. If we speak about actual security, this relativity is hidden.

Apart from security and attacker models, a model is also needed of the system that we wish to verify. As models always abstract from reality, features relevant for security may not be present in our model of the system. For example, we can verify that a program is correct, but if there is a problem with the hardware on which the program is running, the whole system may still not be secure. The limitations of such models justify caution in the use of the term “actual security”.

Besides, the appeal to actual security can easily be misused in discussions on the desirability of certain technologies. Actual security then degrades to an appeal to Nature, which hides the role we have in stating the assumptions; in modelling our goals and our enemies.

The notion of trust, in the Luhmannian sense, instead, helps us to keep in mind the assumptions we make, and to keep the symmetry in the explanation of (apparently) right and wrong judgements. In replacing confidence with trust, scientists have a role themselves, for instance by using an implicit or explicit attacker model, or by the choice of formalisation of security properties. By contrast, the notion of actual security suggests that they are merely passive. Rather than letting the facts speak for themselves, scientists act as spokespersons for the claims that they defend.

7.9 Conclusions

If people desire trust in election systems, they have to be able to speak about security properties of voting systems. Therefore, scientists try to define precisely the relevant concepts, preferably in a formal (mathematical) language. However, very different ideas and opinions about availability, authenticity, correctness, secrecy and verifiability exist in computing science. There is no consensus about the precise meaning of concepts such as secrecy and verifiability. As I have shown, they can refer to very different things. And even for correctness of programs, it is not completely clear how we can be sure that the program running on the voting machines is a correct one. Whether we can ensure availability and authenticity in remote voting is being debated heavily.

In this chapter, I distinguished between two types of individual verifiability and two types of universal verifiability in electronic elections, based on the scientific literature and on concrete developments. I made this distinction based on an analogy with proofs in classical and constructive logic, and labelled the corresponding types of verifiability classical and constructive verifiability, respectively. This distinction is meaningful both for individual and universal verifiability, and I think that it is a useful tool for explicating the hidden assumptions of the way in which verifiability is realised in concrete systems. It shows that security properties may have implicit distinctions, which may lead to omissions in technology or law if they are not recognised as such.

Different ways of measuring security may lead to discussions about the future of e-voting. Even if people would agree on the basic requirements of voting systems, it is not clear which system (or type of system) does the best job in meeting these requirements. Again, one is tempted to bring Nature into the debate to end once and for all the discussion on what constitutes for example anonymity in a computerised system. We can then explain away all deviating opinions as merely cultural distortions of the real properties. As before, I do not agree that this is the way to go.

With respect to a precisely defined security goal and a precisely formulated attacker model, it can be mathematically proved that a model of a system is secure in relation to these specifications. In this sense, there is a mathematical form of actual security. However, in the real world, security goals, attacker models *and* systems may be incorrect, incomplete or otherwise problematic. Even if we can prove “actual”

security within our mathematical model, this does not mean that the security of the real-world system is free from perception: the model may be related to a specific "view" on security, which applies certain distinctions but not others.

In the next chapter, I will turn to a cultural explanation of the scientific endeavour of information security, which is based on multinaturalism, rather than mononaturalism and multiculturalism.

Chapter 8

The Cultural Foundations of Computer Security

"Fantasy, abandoned by reason, produces impossible monsters; united with it, she is the mother of the arts and the origin of marvels."

– Goya (Spanish artist and court painter, 1746–1828)

According to the work of Mary Douglas, cultural categories provide us with a classification of objects in the world, and they necessarily involve phenomena that do not fit in the categories, which are usually regarded as impure and dangerous, or even "monstrous". Martijntje Smits applied this anthropological approach to explain controversies around the introduction of new technologies in our society, such as genetically modified food. We have already seen how we can use this theory to explain the e-voting controversy on the level of society as a whole (chapter 5). In this chapter [87], I take one step further, and apply the approach to subcultures, in our case the scientific discipline of information security. I argue that several important security threats, such as viruses in documents, can be understood as phenomena that did not fit into existing cultural categories of computing science, in this case the categories of programs and data. Based on this analysis, I describe the cultural foundations of information security research and I search for strategies for dealing with vulnerabilities-as-monsters analogous to Smits's strategies for dealing with technological monsters in society.

[87] This chapter is based on an extended abstract published as Pieters and Consoli (2006).

8.1 Science as observation

Information security can be defined as the scientific discipline that deals with protecting information and information systems against attacks. Research typically concerns (formal) methods to avoid or eliminate security vulnerabilities in information system design. Such methods are often based on mathematical models, as has been illustrated in the previous chapter.

As was argued before, scientists cannot be distinguished from others in terms of being concerned with actual security rather than perceived security. Security assessment is nevertheless an inescapable necessity, and it becomes therefore urgent to put forward a framework which makes it possible to tackle the problem in a way which is at the same time meaningful, i.e. without referring to actual security as the ultimate judge of the correctness of claims, and pro-active, meaning that the model is not only useful to assess and explain past problems, but can be used to try and be prepared for future attacks. We need to address the issue from a perspective where science is part of our culture rather than the counterpart of it, which it is when it is said to be dealing exclusively with facts rather than perceptions. This is the contribution of the present project of investigating the philosophical foundations of the scientific discipline of information security.

This project requires two reconstructions: reconstruction of the so-called perceived security from the perspective of the public, and reconstruction of the so-called actual security from the perspective of scientists. The reconstruction of the notion of perceived security has mainly been described in chapter 6, where a distinction was made between confidence and trust in order to understand the public's relation to technology. Here, I concentrate on the role of experts. Although I do *not* share the idea that there is a fundamental difference between public and scientific perception, the distinctions that are employed by experts can be quite different from those used in public discussion. Therefore, a deeper analysis is needed of the particular characteristics of security assessment by experts, formerly known as actual security.

The strategy will be as follows. As an alternative to the idea of actual security, I will reuse the concept of cultural category in the subculture of science, as a basis for understanding the difficulties of security assessment. I will then show how vulnerabilities can be interpreted in terms of clash of categories. Finally, I describe how the emerging "monsters" can be dealt with, and how this can lead to a more pro-active attitude.

8.2 Vulnerabilities as monsters

As I have discussed in chapter 5, cultural categories are classifications that help us describe and understand the world. Martijntje Smits has used this idea to explain controversies on the introduction of new technologies (Smits, 2002a,b).

I propose to generalise the concept of cultural category by using it not only in the broad context of the whole of society, as Smits does, but also in reference to practices

pertaining to specific groups, or subcultures. By subculture I mean in the context of this book a group that can be identified as sharing some basic characteristics, like for example religious beliefs, moral standings, or professional occupation, in other words properties that determine the generalised cultural categories that they share. Scientific disciplines can in this scheme also be recognised as subcultures.

The cultural categories of a subculture are not independent from the broader cultural framework in which the subculture is embedded. Here, interpreting categories in terms of distinctions is helpful. If certain distinctions are prevalent in a society, they are likely to be shared by several subcultures. However, different subcultures have their own basic distinctions, as Luhmann has shown for e.g. true/false in science (Luhmann, 2005 [1993], pp. 76, 203) and right/wrong in law (Luhmann, 2005 [1993], p. 55). The combination of the role-specific and culture-specific distinctions will establish a particular set of categories within a scientific community.

Here, the focus is on computer security and it is claimed that there is a strong analogy between the model proposed by Smits and the inherent fallibility of security assessment: the latter can also be explained in terms of cultural categories, and phenomena that do not fit in these categories.[88] The most spectacular attacks on computer systems often occur when this way of attacking has not been considered before; in other words, when the vulnerability does not fit into the existing *categories* of computer security, and therefore has not been included in security and attacker models. I argue that at least some of the vulnerabilities emerging in computer security can be characterised in terms of monsters. As much as society will always produce waste and dangers because of existing categories, computer security will always produce vulnerabilities because of existing security models.

On an even smaller scale, the cultural categories within a company may produce vulnerabilities in their information systems, when phenomena are not covered by the cultural categories of the company. To the outside world, the phenomenon appears as a failure, a mistake by the company in relation to the existing categories, usually referred to as "actual security". However, from the company's perspective, the vulnerability may present a true challenge to their categories, and therefore appear as a monster.

It is important to stress that from this analysis it follows that "mistakes", understood as errors due to poor judgment or misapplication of knowledge, are *not* to be categorised as monsters, in that they do not result from an inherent impossibility within the subculture to make sense of the phenomenon with their categories. Something is only a "monster" if it is a classification failure.

8.3 Monsters and anomalies

When one is discussing sociology of science, one needs to take into account Thomas Kuhn's ideas on scientific developments (Kuhn, 1962). According to Kuhn, science is

[88] Graff and Wyk (2003) speak about "mental models" in this context (p. 20).

not merely gradual progress fed by acquisition of knowledge. Instead, cultural frameworks develop in which scientific activity takes place. Kuhn called these frameworks "paradigms". There are three stages in the history of scientific disciplines. First, there is no paradigm yet, only some preliminary ideas, which is called prescience. After a paradigm, a set of shared ideas about the discipline, has been established, problems within the paradigm can be solved in the phase of normal science. Results that do not fit in the paradigm are called anomalies, and are ignored at first. If the number of anomalies increases, the existing paradigm may be challenged in the phase of revolutionary science. A new paradigm, explaining the anomalies, may then develop.

The way in which the concept of cultural categories is used here bears some resemblance to the paradigm idea developed by Kuhn, but is certainly not identical. Although the concepts of monster and anomaly seem similar, they have different functions in the two models. While a paradigm shift is a rather dramatic event, in which the accumulation of anomalies leads to the abrupt replacement of a world view during a "revolutionary" period, the way in which categories react to monsters does not require or imply such a mechanism. Also, Smits views the monster conjuring strategies as alternatives, whereas the different stages of science Kuhn distinguishes follow each other in a logical order. This is partly due to Kuhn's focus on the community as a whole, as contrasted with Smits's focus on strategies of individuals or smaller groups.

Moreover, Kuhn's notion of anomaly suggests something negative: it is necessarily a problem. The same holds for the computing science notion of vulnerability. This is in contrast with the monster concept discussed in chapter 5, where it was mentioned that disruptive new technologies may also be interpreted positively. This has consequences for the application of the monster-conjuring strategies to vulnerabilities, and limits the applicability of the analogy somewhat. This will be discussed in section 8.5.

8.4 Examples of the clash of categories

A typical example of a clash of categories in computer security was the issue of viruses in Microsoft Word documents (Ford, 1996; Gordon and Ford, 1995). Up to a certain point in time, viruses were supposed to hide in executable files (programs) only, not in documents (data). Then, a virus was created that was capable of affecting Microsoft Word documents: the Concept virus. It was relatively harmless and meant to demonstrate the possibility of macro virus creation (Wallich, 1995). A more recent and infamous example of virus exploiting macros in Word is the Melissa virus (Garber, 1999).

It is interesting to note that both Garber and Wallich identify these viruses as barrier-breaking and radically new objects. In our framework, we can affirm that the viruses in Word documents were a clever example of the mixing of two cultural categories in computing science: those of programs and data. As a result, a vulnerability emerged that was not recognised as such: it was "matter out of place" in the category system. A monster had been created. Following the monster theory, any classification

in computing science that affects or models security is bound to create vulnerabilities as by-products. Exploiting such vulnerabilities amounts to exploiting the limits of the classification. In this sense, the conceptual separation of programs and data produced the vulnerability that was later exploited by text document viruses.

An interesting question is who was responsible for this clash. Was it Microsoft, which allowed macros to be executed in Word documents? Was it the virus writer, who exploited this feature in order to attack systems? Or was it the computing science community, whose classifications were not suitable for all types of files? Different levels of responsibility can be identified in relation to such vulnerabilities. Of course, from a legal perspective, the virus writers are responsible for the problems caused by the virus, but that is different from responsibility for the appearance of the *vulnerability*.[89]

Another example is the separation of the hardware level and the software level in smartcards. Normally, security models addressed either the software or the hardware, but not both. This literally "produced" the power analysis attack, in which data (software level) could be read by eavesdropping on the power consumption of the card (hardware level) (Kocher, Jaffe, and Jun, 1999; Messerges, Dabbish, and Sloan, 2002). In one implementation, attacks are based on side-channel information gained by observing cache bits and misses in the current drawn by the smartcard (Fournier and Tunstall, 2006).[90] Also in this case, we can pose the responsibility question in a way parallel to the Melissa example. This indicates that the analysis can apply to a broad spectrum of situations.

In both examples we can identify several levels of responsibility. We propose that, on a more fundamental level, the subcultural categories *themselves* are responsible for providing the opportunities for attack. The community was inherently incapable of preparing itself for the new attacks. The associated vulnerabilities can be understood in terms of monsters. This observation provides one of the ingredients for a more subtle philosophy of information security.

The hardware/software distinction is also highly relevant to the main topic of this book, that of electronic voting. The following example is taken from the Dutch discussion on electronic voting machines, started by the activist group "Wij vertrouwen stemcomputers niet".

Before the campaign, the issue of vote secrecy had been primarily discussed with respect to storage of the votes. This can be seen in the requirements established in 1997 (see page 33). Individual choices should not be derivable from the memory of the voting computer, even if one would know in which order people had voted. This means that votes should be stored in random order. This is mainly a software level discussion.

The issue of tempest attacks had been known in other areas, notably defense and intelligence agencies (Eck, 1985). It was not discussed for voting machines in the Netherlands until the media offensive of the pressure group. It seems that the

[89] See also Bissett (2000) for an analysis of the motivations of virus writers.

[90] This, in turn, generated research on how to repair the vulnerability (Herbst, Oswald, and Mangard, 2006).

issue had been brought up in the German discussion on the use of the Nedaps, though. What this example shows is that in a particular context, a particular category may be in focus, inhibiting attention to similar problems in different categories, i.e. hardware threats to the secrecy of the vote. Secrecy was seen as a software problem, and it took the analysis by the activist group to create a monster by exposing the hardware problems. The monster here consists of the impossibility to classify the threat in terms of existing security requirements. After the monster appeared, a new norm for compromising emanations was soon established, and seemingly accepted by all participating actors (Hermans and Twist, 2007).[91]

The program/data distinction is also applicable to the situation in the Netherlands. Until recently, verifiability of electronic voting had only been discussed in terms of certification of the machinery and the software. The pressure group showed the vulnerability to manipulation of the program: a different program could have been installed than the one that was certified. A newer notion of verifiability emphasises the demand that each voter be able to verify that her vote is counted correctly. It is considered not enough that the programs are verified and certified; the result of *each election* should be verifiable. This extends verifiability from the program level to the data level: the type of verifiability that was discussed in section 7.7.

Thus, the tempest vulnerability was a monster in the sense that secrecy had only been addressed at the software side of the hardware/software distinction. Moreover, the lack of verifiability was a monster in the sense that verifiability had only been discussed at the program side of the program/data distinction. These two monsters framed the e-voting debate in the Netherlands. What to do with those vulnerabilities-as-monsters?

8.5 Strategies for coping with the monsters

Smits considers four different ways of dealing with monsters: embracing, expelling, adapting, and assimilating (see section 5.3). Can they be used for dealing with vulnerabilities in computer security as well?

Embracing

Embracing the monster (for example, as if it were a wonder) may be interpreted as a sign of respect or admiration. During the introduction of plastics, some people thought this new material would be some kind of salvation from the limitations of nature (Smits, 2002b, pp. 109-114). Thus, there is the possibility of admiring phenomena incompatible with the existing cultural order, and granting them a kind of holy status.

In computer security, vulnerabilities are essentially negative phenomena, and the analogy is not easy to see in the case of monster embracing. Most people would

[91] Not all actors agree that the norm makes sense; for example, it was said that it did not comply with international standard levels.

agree that a vulnerability is something that needs to be resolved, and welcoming a vulnerability is difficult to imagine.

However, a vulnerability *can* be seen as a confirmation of the existing categories. This means granting a vulnerability, an inconsistency, the status of a kind of ultimate proof of the rightness of the existing order. In a way, this can be seen in the reaction of Nedap, the Dutch voting machine manufacturer, to the easy replacement of chips in their system by the activist group "Wij vertrouwen stemcomputers niet": "We noticed that it was proved that the machine works excellently. The voting machine does exactly what is commanded."[92] Thus, if the attackers make the system count incorrectly, this proves that the system is correct. The machine only performs the will of the people. This is the "it's not a bug, it's a feature" approach. It is not a monster, it's a normal animal. It is not a problem with our categories, it is a problem with *your* categorisation of the phenomenon.

Seeing a vulnerability as a confirmation of the existing order does not solve the problem, at least not from the point of view of the people who see it as a failure. Respect for the monster stands in the way of dealing with it in a way which is effective for the security *context*. However, such an attitude may happen (and even be appropriate) among hackers. They see a vulnerability they discover as a confirmation of their own place in the order of things, which is a "monstrous" place: a place which constantly seeks the border of existing categories.

Expelling

Some people regarded plastics not as salvation, but as a disaster (Smits, 2002b, pp. 114–117). Precisely the failure to fit existing classifications of materials made them filthy and dangerous. Luddites think such new technologies should be expelled or even destroyed.

Expelling the vulnerability-as-monster in computer security is in a practical way not feasible, because a threat to a computer system cannot be eliminated as easily as a new phenomenon in society, since the attacker is typically outside the control of the computer security community. There is an extra contingency here in the behaviour of the enemy, who is committed to exploiting the monster. Where technological monsters in society are expelled by saying "we don't want this", vulnerabilities-as-monsters are expelled by saying "there is no problem". Diebold Election Systems uses this strategy when they are accused of vulnerabilities in their voting machines (Gumbel, 2005, pp. 260–261), as opposed to the Nedap reaction above. It might help to deny the problem and see if everything stays quiet.

Adapting

Biodegradable plastics are an adaptation of the monstrous plastics to existing categories: they will no longer fail to rot when lying around (Smits, 2002b, p. 155). An example of monster adaptation from information technology is the requirement

[92] `http://www.nedap.com/nieuws.php?id=30`, consulted November 21, 2006, translation WP.

of a paper trail in electronic voting machines. This puts them back into the category of publicly verifiable voting systems (chapter 5). Note that the issue here is the technology-as-monster, not the vulnerabilities-as-monsters.

Adapting vulnerabilities-as-monsters may be useful as well, for example by categorizing Word documents as executable files rather than data files, which was done in virus scanners. In such an approach, the threat becomes one of a known category: a virus in an executable file. In other words, the category stays fixed and the object is re-categorised.

From a computer security point of view, this perspective does not seem to provide the pro-active attitude which is required in order to prevent new security threats. The adaptation approach presupposes a unidirectional relation between categories and the phenomena they explain. Categories are given (they represent actual security), and vulnerabilities have to fit into these categories to allow protection. This does not do justice to the complex and dynamical (bidirectional) interaction in which categories are formed and conceptualised. The approach cannot be generalised to deal with security problems, and we can see this in the virus vulnerability. The challenges of viruses in different file types, in the end, have not left the categories of virus protection unaffected, and we can now do "full scans", "smart scans", etcetera. By now, we may speak of monster assimilation.

In electronic voting, the (new) categories of program verification and data (vote) verification (see page 134) do not seem to have been recognised in the verifiability monster. Instead of discussing those new types of verifiability, it has been argued that the verifiability of the previous paper system should also be possible in e-voting. This subculture-level categorisation problem was solved by a society-level adaptation strategy. The monster was adapted to existing categories by means of a paper trail, but the categories were not adapted to the monster.

Assimilating

The last strategy Smits mentions is assimilating the monster, a pragmatic process in which both the monster and the cultural categories are being changed. An example that Smits mentions is the shifting of the border between alive and dead due to the technology of organ transplantation (Smits, 2002b, p. 159). Here, "brain dead" became a new criterion for deciding whether it would be allowed to remove usable organs from a body. Thus, a new category emerged for dealing with the new technology.

Assimilation also happens in information security. In vulnerabilities-as-monsters, power analysis attacks on smartcards now have their own field of research, and the power analysis vulnerability has changed from a side-effect to something that can be prevented using appropriate tools. This means that both the categories and the technology have been changed, by assimilating the monster of power analysis attacks.

In e-voting, the assimilation strategy was used in the tempest monster in the Netherlands. By introducing new actors (such as the intelligence agency and independent committees), new norms were created that voting systems should satisfy, in terms of acceptable levels of compromising emanations. When such new norms

are accepted by all participants, a new category in e-voting requirements emerges, in which the tempest problem finally finds its cultural place.

The strategy of assimilation provides a basis for a pro-active attitude towards security we saw missing in the adaptation strategy: members of the computer security community are not only responsible for formalising all aspects of existing categories and then announcing that they know what actual security is, but rather for contributing to the evolution of the categories themselves, so that they are better able to incorporate new phenomena, and thereby prevent new attacks.

8.6 Conclusions

The treatment of deviant phenomena in a culture is a field of research with a long tradition. Based on the theories of Mary Douglas on impurity, danger and risk, Martijntje Smits analyzes how our culture takes care of new technological phenomena. She calls this approach "monster theory". I argue that this theory does not only make sense on a broad cultural level, but also within subcultures, including scientific disciplines. These subcultures have their own sets of specific cultural categories.

I have proposed to assimilate the monster theory to the field of computer security. This enables us to frame the discussion about the interpretation of new threats and the way of reacting to them in terms of strategies for dealing with monsters. The strategies that Smits distinguishes are embracing, expelling, adapting and assimilating. These can be used to describe reactions to vulnerabilities-as-monsters in information systems. The specific strategies used determine if and how new threats are incorporated in formalisations of security properties and in attacker models, which reflect the existing subcultural categories of information security. Smits considers the assimilation strategy the most promising one, since it does not consider the cultural categories as fixed and given. I argue that assimilation is also the best strategy in computer security as a subculture, for there is no final model of information security that incorporates all vulnerabilities, as there is no final set of cultural categories that fits all phenomena.

If information security, and risk science in general, aim at better understanding of future phenomena, they cannot ignore their own culture. For it is not objective Nature that they are investigating, but their own constructed version, if only for the fact that they are dealing with the future.

Again, this conclusion challenges the distinction between actual and perceived security, because cultural categories determine if and how a threat is perceived, even in science. Based on the categories, the phenomenon is *constructed* as a threat, via the security and attacker models in which the categories are embedded. Actual security is always related to the existing categories in the subculture of information security research, rather than being culture-independent. Therefore, a discussion in terms of cultural categories could replace the common discussion in terms of actual security, even in science.

However, I do not wish to claim that threats are merely social constructions. Instead, they are determined in continuous interaction with the environment. The next chapter will deal with a vocabulary to describe this process.

Chapter 9

Reve{a,i}ling the Risks

"A man sits as many risks as he runs."

– Henry David Thoreau (American essayist, poet and philosopher, 1817–1862)

If risk assessment is based on (sub)cultural categories, but risks are not merely social constructions, how can we find a terminology of risk assessment that can replace the distinction between actual and perceived risk? Luhmann said that technology is not risky, but communication about technology is. Thus, risks *do not exist as risks* if they are not recognised as such. Instead, they are revealed as risks by the people involved. This revealing is not mainly an epistemological process, but it is ontological in nature: the revealing determines what is there, and also "reveils" other risks. Therefore, I think that we could understand the process of revealing risks in terms of Martin Heidegger's "entbergen" to grasp better the implications of the way in which risks are revealed. In this chapter, I outline a conception of risk inspired by the concept of "entbergen" and evaluate this idea. I conclude that such an understanding does a better job in explaining risk controversies than a purely representational approach.

9.1 Risks: real or relative?

In the preceding chapters, I have presented research on electronic voting systems, security verification of electronic voting systems and the origin of the associated controversies. From this research, it appears that risk is one of the most important concepts in the discussion. In chapter 4, I introduced Luhmann's distinction between risk and danger: risk can be attributed to a decision, whereas danger cannot. But where do risks come from?

Generally, the problem of determining risks is understood as a problem of representation: the risks are there, but we may not recognise them. In chapter 5, I argued that the origin of the controversies is not only to be found in alleged real threats, but most of all in cultural presumptions. Moreover, I argued that an appeal to "actual security" as opposed to "perceived security" in order to explain security debates is problematic (chapter 4). This is in line with the argument of Bruno Latour (2004) in *The Politics of Nature* (chapter 4) and Martijntje Smits (2002b) in her PhD thesis on risk controversies (chapters 5 and 8).

However, such an approach suggests that the risks discussed in the controversies are nothing more than social constructions. If risks are only social constructions, then there is no causality involved in terms of loss caused by the environment, and therefore no benefit in talking about risks in terms of preventing future loss. Against this view we can argue that the risks *can be* real threats, but then the question is how to assess which risks are real and which are not. This is backtracking to the original representational approach, in which risk assessments are more or less correct when compared to the "actual" risks. The question is then reduced to explaining why people get it wrong. This is unsatisfactory, since there is no way to step outside the debate and observe the "true" risks, which is necessary to explain the deviance.

Both authors cited reject the purely constructionist view as well. This is not the place to analyse their arguments in detail. Instead, I wish to ask a very simple question: if risks are neither objective threats nor purely social constructions, then what is the relation between not knowing the risks and knowing the risks?

It appears to me that both the representational and the social constructionist view lead to philosophical problems when trying to understand the origin of risk controversies, because we lack an adequate answer to the question above. A solution based on consensus conferences or – if one thinks it should remain an expert task – a "broadly shaped expert dispute" (Munnichs, 2004) may be satisfactory from a practical point of view, but it does not provide a theoretical understanding of how people come to differ in opinion in the first place.

In this chapter, I will try to provide a vocabulary for a discussing risk assessment from the point of view that risks are determined in a "negotiation" between humans and the environment. First of all, I will introduce the philosophical concept of "entbergen" due to Martin Heidegger (Heidegger, 1978, 1982; Tijmes, 1992). Using this concept, I will argue that risks need to be "revealed", but that this means at the same time a "reveiling" of other risks. Drawing further upon the work of Heidegger, I will try to distill the specific way in which our culture "orders" the risks, and what this means for information security. This will lead us to conclusions on the use of Heidegger's terminology in the context of risk.

9.2 Heidegger's concept of "entbergen"

This is not a thesis about Heidegger. It is a thesis about risk. The author is not a Heidegger expert either. Therefore, this section is necessarily only a sketch of the

features of Heidegger's thought that are relevant for the aim of this chapter: using a specific Heideggerian concept in an approach to risk controversies.

The philosophy of Martin Heidegger (1889–1976) is characterised by the use of many new words. In order to uncover the relation between human beings and "Being", Heidegger often intentionally used ambiguities in the German language to refer to nuances or dialectical features that cannot easily be expressed in common words. Heidegger was influenced by the phenomenology of Husserl, the existentialism of Kierkegaard and many other philosophies.

As all phenomenologists, Heidegger 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, 1978).

"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. This active part substitutes a naïve naturalism: meaning is not present in Nature itself, but actively constituted in our relation with our environment. Heidegger applied the notion of "entbergen" to the very basic relation between human beings and their environment, but, following the line I set out in terms of cultural categories, I apply it to the more specific task of security and risk assessment here, where the relation is between expert and technology.

In English, the notion of "entbergen" is usually translated as revealing. 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.[93] 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.[94]

Heidegger used his terminology to develop a rather critical interpretation of modern technological developments (Heidegger, 1982; Tijmes, 1992). He thought that modern technology incorporated more than technical devices, namely a specific way to view the world, a specific way of "entbergen": the world as a set of resources (something that was ordered: "bestellt", "herausgefordert", a "Bestand"). In his view, using the flow of the Rhine to generate electricity was a manifestation of such an attitude.

[93] Objects with ambiguous perceptual interpretation possibilities (duck-rabbit, Necker cube) establish a similar revealing-concealing relation. An interesting question is how these optical "tricks" relate to Heidegger's notion of "entbergen".

[94] In terms of Luhmann's systems theory: when we use distinctions to describe the world, we cannot *at the same time* distinguish these distinctions from others. They become *concealed* in the process of using them.

Heidegger's view on technology is now widely disputed and claimed to be too much focused on "technology" as a single and universal phenomenon. Today, we would say water power contributes to sustainable energy supply, and we would probably have to acknowledge that the role of a power station in the Rhine is equivocal. Still, the fact that technology (and also specific technologies) make us see the world in a particular way is generally recognised. The problem with Heidegger's interpretation is that it only allows 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.

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 role of technology in society, 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 I polish up the concept of "entbergen" for use in the information age.

9.3 Reve{a,i}ling the risks

What makes giving a description of risk assessment that does justice to the many intricacies of risk controversies so difficult? Maybe we do not have a word for it. I argue that this is precisely because the process of determining the risks must be understood as a process of "bringing from concealment into unconcealment". 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 revealing determines which risks become visible (and how) and which do not. Therefore, a Heidegger-inspired terminology is justified.

It can be a bit tricky to use the concept of "entbergen" in a discussion on risk assessment of technology, where Heidegger interpreted technology itself as a specific way of "entbergen". In the context of this thesis, "entbergen" does imply a making visible, although not as a general characteristic of the way of "being" in our time, but in a more pragmatic sense. It is not claimed that this fits with the strict notion as used by Heidegger; rather, it is judged to be useful for creating a vocabulary for describing the second-order perspective on security assessment.

Thus, it is not claimed 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, 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 or inhibit the revealing of certain risks.

In terms of security and attacker models, any claim about security implicitly involves such models. These models influence how risk and security are perceived, how they

are revealed, and which details can be observed. It would be possible to construct an explicit security and attacker model in order to relate the claims to basic assumptions about the structure of the problem. Still, not all aspects of the process of revealing can be made explicit in security and attacker models; some assumptions are part of a larger cultural framework of concepts, and in a sense, the concepts of risk and security themselves are part of the way in which we are able to reveal things in our environment.

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.

In information security, the process of revealing is not only mediated by security experts, but also by the intruders. 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 defense against the attack) makes the risk even more visible. It may also work the other way around: 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 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 buffer overflows are more likely to be revealed once the buffer overflow has become common knowledge.

By using the concept of "entbergen" in risk assessment, I intentionally "blur the politically necessary distinction between ontological questions and epistemological questions" (Latour, 2004, p. 36). This is to say, I reject the claim that risk assessment yields correct *representations* of an *external reality*. Instead, risk assessment *externalises* the risks by revealing them as properties of the environment (Latour, 2004; Luhmann, 2005 [1993]).

As argued above, different cultures may reveal risks in different ways. This also holds for subcultures within a society. Subcultures are characterised by possession of a specific set of cultural categories. From the perspectives of different sets of cultural categories, a system may be categorised differently, and also the risks will be revealed differently. When this happens, the system can be said to be a "monster" (Smits, 2002a,b). For example, the risks of genetic modification will be revealed differently from the perspective of human health than from the perspective of ecology. If we cannot agree on the relevant categories, we may have to adapt our categories to fit the monster. This may even include negotiating the border between nature and culture, as in the case of GM food.

Once agreement on the categories has been re-established, the monster can become a black box. According to Bruno Latour, this is something that has been "blackboxed"; a theory or technology of which the supporting network of actants has become invisible. This invisibility also hides the risks. Some risks that were exposed in the monstrous character of the technology have been taken care of, others have been reveiled by conjuring the monster. This process of blackboxing brings things back from unconcealment into concealment, by "undoing" the process of revealing.

In the reverse sense, it may be said that the way of "entbergen" determines how the inner workings of a black box are revealed. If a black box is opened in different ways, the thing may turn out to be a monster. For example, opening the black box of asbestos from the perspective of health produced a phenomenon that was hard to classify and assimilate. By now, we have companies specialising in asbestos removal.

In the Netherlands, the black box of the paper voting system had effectively reveiled the risks of proxy voting.[95] Only after the OSCE revealed this risk again, discussion re-emerged (OSCE Office for Democratic Institutions and Human Rights, 2007a). The same holds for the tracing possibility in the British voting system. E-voting, on the other hand, can only be a black box by now if it has been able to hide within the black box of the existing system. This has happened in the Netherlands. This box can now be opened in different ways, for example based on the controversy in the US, or based on the existing trust in the suppliers.

Another example is the risk of vote buying or coercion, and the accompanying security measure of the voting booth. Once buying and coercion have disappeared as a profound risk in elections, partly due to security measures, it can be "forgotten" in the introduction of a new technology, such as Internet voting. In the Netherlands, it seems to have been revealed again, whereas in the UK, it is not so much *seen* as a substantial risk.

In chapter 4, I 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 to protect against risks are blackboxed together with the risks. When security measures are blackboxed, they become invisible. This yields a distinction between "perceived security" and "non-perceived security", or "revealed security" and "reveiled security" . Here, we have a more meaningful distinction than the one between "perceived security" and "actual security". Many security measures in the paper voting system have been reveiled by now, together with the risks in elections that made them appear (e.g. ballot stuffing and its countermeasures[96]). This explains why the paper voting system appears as more secure than new electronic systems. Paper voting does not appear as more secure because it is actually more secure, but because the system has

[95] The claim that risks are reveiled implies that they are still visible from one's own perspective, otherwise one could not claim that they are there. In retrospect, one can claim that certain aspects were hidden before. This is much harder for the present situation. This will be addressed in the next chapter.

[96] A countermeasure is verifying that the box is empty before starting the voting process.

been blackboxed and risks and security measures have been reveiled: its security is non-perceived.

9.4 Ordering the risks

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 handling of risks in modern society. When applied to risk, the analysis states that modern society *forces the risks into unconcealment*. This is 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. This is a useful ambiguity that is not present in Heidegger's original term "bestellen": it makes clear that in the process of ordering, things are both revealed and structured. Bruno Latour, not particularly known for being a supporter of Heidegger, states this dual meaning as follows, in relation to his discussion on the use of the word "nature":

> "With nature, two birds are killed with one stone: a being is classified by its belonging to a certain domain of reality, and it is classified in a unified hierarchy extending from the largest being to the smallest." (Latour, 2004, p. 29)

In this phrase, "nature" can be taken to mean "what makes it possible to recapitulate the hierarchy of beings in a single ordered series" (Latour, 2004, p. 25), and this is precisely "ordered" beings; beings revealed in the special way of "ordering". Thus, "ordering" the risks, translated to Latourian terminology as an appeal to Nature, 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. "Nature" makes it possible to "recapitulate the hierarchy".

I propose to describe risk assessment as the process of "ordering" the risks into unconcealment, by revealing them with "force". This ordering is both a demand and a quest for structure, reflected in the double meaning of the term. 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 threat in accordance with Nature.

Or, in more pragmatist terms, the scientist does not have the tools to describe her discovery in a different way.

In chapter 6, I used Niklas Luhmann's distinction between confidence and trust (Luhmann, 1988) to disentangle the discussion on the relations between security and trust. Confidence, following Luhmann, was taken to mean assurance of the safety or security of a system without knowing the risks or considering alternatives. Trust means assurance by assessment of risks and alternatives. If a 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, trust (or distrust) takes the place of confidence. I argued that computer scientists, rather than investigating actual security as opposed to perceived security, are occupied with replacing confidence with trust.

We can now be a bit more precise about the relation between confidence and trust. "Ordering" the risks denotes a transition from confidence to trust. Trust in this setting means assurance based on knowledge (i.e. unconcealment) of risks and alternatives; confidence means 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.[97]

Thus, following Heidegger just far enough in his skeptical view on modern society, we can understand risk assessment in our society as "ordering" the risks, with the double meaning of a demand and a quest for structure. Scientists use this method to transform confidence into trust. Confidence, assurance without knowing risks or alternatives, corresponds to concealment. Trust corresponds to unconcealment. Moreover, by revealing the risks by means of ordering, confidence *itself* is concealed, and even seems to be unnecessary.

9.5 Revealing in the Netherlands

In the Netherlands, electronic voting machines have been in place since the early nineties. Requirements that the machines have to meet stem from 1997. Only in 2006, wide scale controversy emerged about their security, due to the activist group "Wij vertrouwen stemcomputers niet" (see section 2.4). The two main risks that this group revealed in their media offensive were the ease of replacing the chips with counting software – illustrating the lack of verifiability – and compromising emanations leaking information about the voter's choice (tempest attack). Especially the latter issue had major consequences, since the Minister decertified about 10% of the machines for this reason, after having the intelligence agency look into the problem. This in turn generated quite some attention of the media.

[97] In this regard, Heidegger is not the only one who sees something dangerous: Niklas Luhmann 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 (Luhmann, 1988).

Meanwhile, the original problem, the lack of verifiability, had been reveiled. The activists 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, and reveiling their basic argument. At the same time, they transformed the original confidence, based on the concealment of risks, into distrust. We now want trust in e-voting systems, not just confidence.

An interesting question is why politics and media took up the tempest question rather than the verifiability of the software. It may be that the former was easier to grasp, since it was known to be measurable, and there were actors who could do so. Classifying the tempest problem may thus have been easier than classifying the verifiability problem: it was easier to reveal because it fitted with existing categories.

This is just a short explanation of how the framework may be useful in explaining risk controversies. This explanation may have consequences for research on the legal framework around e-voting, and other technologies. If risks are revealed as described in this chapter, drawing up laws and requirements for e-voting 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. The main point to make here is that it would be helpful not to forget the process of revealing and reveiling that led to the particular legal texts, because it will inevitably have been steered by a particular "entbergen", in which the risks were revealed in a specific and possibly not optimal way. In the previous chapter, the examples of the hardware/software distinction with respect to the secrecy of the vote and the program/data distinction with respect to verifiability were discussed (section 8.4). Explication and flexibility of attack models is essential in pro-actively managing security. The Dutch may thus wish to avoid having the requirements fixed for another ten years without further consideration.

9.6 Conclusions

In this chapter, Heidegger's notion of "entbergen" was used as inspiration to explain how risks of technological systems are revealed in risk controversies. The point of departure was the assumption that risks are neither purely objective nor purely subjective. Based on the use of Heideggerian terminology, I discussed how risk controversies can be understood in terms of the revealing and reveiling of risks. These concepts were linked to the notion of black box, and their relation with the distinction between confidence and trust was addressed. I discussed the Dutch e-voting controversy from this perspective, and mentioned implications for law.

Following Heidegger, we could analyse modern society as one in which the importance of confidence is increasingly being concealed by the specific way in which risks are being revealed, namely by "ordering" them. This is not meant as either an absolute or nostalgic conclusion, but rather as an observation that certain aspects of experience are amplified and others reduced by the specific way in which we understand and reveal risks.

One of the main benefits of this 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.

The main disadvantage seems to be the massive and nostalgic connotation that Heideggerian terms mostly have. I hope I have made clear that I do not share such a view, but I understand that we must reveal it as a risk of this approach.

Many little monsters determine the security properties of e-voting systems. Definitions are adapted both because of new attacks and because of clashes with existing categories. Computing scientists have the task of assimilating these monsters into their models. In this way, the ontology of risks is ever changing. Being, or from a more pragmatist perspective culture, influences the way in which risks are revealed. Moreover, revealing certain risks may invite revealing similar risks, and at the same time reveil others.

By replacing the distinction actual-perceived with perceived-hidden, or revealed-reveiled, we acknowledge the idea that there exists an environment, but not as an objective "Nature". Rather, this new vocabulary helps us to become conscious of the limitations of our perceptions, based on our cultural framework. For security, this means that we can pro-actively investigate what our distinctions exclude. For example, if we write down a software-level requirement, we should immediately ask the question what an equivalent would be for the hardware level, in order to avoid reveiling hardware level risks.

The "Entbergung" of risks, rather than a fixed Nature, determines the acceptability of voting systems. But this cultural framework is in its turn influenced by the available technology, as we will see in the next chapter.

Part V

The future

Chapter 10

A Categorical Challenge to Democracy

"Any sufficiently advanced technology is indistinguishable from magic."

– Arthur C. Clarke (English writer of science fiction, b. 1917)

In this chapter[98], I develop the notions of categorical challenge and reconstructive technology assessment. These extend the analysis of the e-voting debate with the idea that the technology itself plays a role in the construction of the debate and the revealing of risks. This role of technology challenges existing categories. This challenge can be pro-actively addressed by identifying what existing distinctions reveil, and which alternatives exist. The approach can be seen as an implementation of the monster-conjuring strategy of assimilation. The focus will be on remote electronic voting.

Using the philosophical concept of technological mediation[99], as developed by Don Ihde and Peter-Paul Verbeek, I claim that Internet voting may change our experience of democracy, and transform the way we act as citizens in the democratic system. I argue that this mediating role of voting technology requires reconstruction of concepts used in discussing democracy, revealing aspects that were invisible before. My approach of reconstruction departs from the political philosophy of John Dewey. Based on his work, we can describe the political process in a democracy in terms of intellectual reconstruction and institutional reconstruction. This way of describing the process allows for a pro-active attitude towards adjusting our cultural categories.

[98] A previous version of this chapter has been published as Pieters (2006a). The original notion of "conceptual challenge" has been replaced here to conform to the terminology of previous chapters.

[99] The concept of mediation is explained in section 10.2.

Combining the concept of technological mediation and Dewey's political philosophy, I use the mediating role of online voting technology as input to the intellectual reconstruction of the discussion on voting and democracy. This approach is called *reconstructive technology assessment*, since the emerging technology itself mediates our understanding of its implications, and requires us to reconstruct our concepts and institutions. Based on the developments in the countries I studied, I present some challenges that the mediating role of online voting technology offers to existing concepts in democracy, and evaluate the benefits for social inclusion of reconstructing these concepts with respect to the new possibilities.

10.1 Dynamic democracy

Throughout history, philosophers as well as citizens have often lamented the status of democracy. While John Dewey (1991 [1927]) complained about the "eclipse of the public" in the beginning of the 20th century, the Dutch said there was a feeling of "onbehagen" or discomfort concerning politics in the period of the rise and fall of the populist party of Pim Fortuyn in 2002. The "diseases" that are diagnosed are often considered a threat to social inclusion[100] in terms of participation in the democratic process. If people are alienated from politics, it is said, representative democracies cannot function properly. Many cures to these alleged diseases have been proposed. Meanwhile, new democracies are being established in countries with different levels of development all over the world.

Since the early nineties, however, democracy has been changed by something else than political and social developments. The rise of the information and network society, and the accompanying technologies, did not leave democracy untouched. This is especially true in elections. Although mechanical voting machines have been in use for a long time, the impact of the information and network society on the voting process is and will be far more profound. The introduction of electronic voting machines has already shown this.

Today, the most challenging development is the option of online voting. People tend to do more and more of their transactions online, and the mere existence of these other technologies makes them sensitive to the trouble that casting a vote still brings, in the act of going to the polling station. In the Netherlands, two Internet surveys showed that – depending on the context of the question – between 62 and 79 % of the Dutch citizens using Internet would like to vote online (Burger@overheid publiekspanel, 2002, 2004). The will of the people seems to point towards machines. Meanwhile, relatively new democracies such as Estonia are eager to become the early adopters of such modern forms of voting (see section 2.2).

Of course, the issue whether it is desirable to make voting easier for certain groups of people, namely those who have Internet access at home or at work, is a topic of

[100] Warschauer (2004) defines social inclusion as "the extent that individuals, families and communities are able to fully participate in society and control their own destinies, taking into account a variety of factors related to economic resources, employment, health, education, housing, recreation, culture and civic engagement" (p. 8, my italics).

discussion from the point of view of social inclusion itself, in terms of turnout among different groups (Alvarez and Hall, 2004, ch. 3). In developing countries, an infrastructure of physical, digital, human and social resources is needed to be able to provide online democracy at all (Warschauer, 2004, p. 47). Also, many people have pointed out security threats to online voting systems, or electronic voting systems in general, that may be a threat to social inclusion, especially hacking, manipulation by insiders and coercion (Jefferson et al., 2004; Kohno et al., 2004; Phillips and Von Spakovsky, 2001; Weinstein, 2000).

In this chapter, however, I focus on the role of online voting technology in people's experience of democracy. Even if Internet voting can be implemented in a secure way based on technical, organisational and legal measures, and even if we do not consider the possible shift in turnout among different groups a problem, there are still many aspects in which it may have unexpected effects. The role of technology in changes in societal life has been shown in many other cases, and voting will not be an exception. This is not to say that technology is autonomous (Winner, 1977) and we follow blindly the "will of the machine". But technology is not neutral either, and if we do not take the issue into account, it will be an implicit force in future decisions on voting and democracy.

In his famous study "Do artifacts have politics?", Winner (1980) showed that technological designs may have political implications. These may occur either intentionally or unintentionally. Winner's famous example of intentional political effects concerns the building of bridges in New York between 1920 and 1970 that were too low for the buses of public transport, and therefore the lower income classes, to pass underneath. One can easily imagine similar things happening unintentionally as well. Since then, many cases of such influences have been investigated, and many theories about how they come about have been developed in philosophy of technology and science and technology studies (STS).

We may assume similar effects, be they unintentional, occurring in electronic voting technology. Electronic voting will undoubtedly, depending on the way in which it is implemented, make certain things possible and others impossible, just as the New York bridges did.

Democracy is not a static system, and many different theories about its form and function exist (Held, 1997; Cunningham, 2002). The discussion on the supposed problems of current democratic institutions cannot be intelligently conducted without knowledge of the impact of new voting technology, especially Internet voting, on the democratic process. An attempt to include technology in the debate is necessary to prevent technology from changing democracy without well-founded political discussion, which would be a serious case of social exclusion in its own right (Harbers and Bijker, 1996).

This chapter is organised as follows. First, a methodology for including technology in the debate on the future of democracy is discussed, which is based on the political philosophy of John Dewey and the postphenomenological approach in philosophy

of technology. The section "Challenges to democracy" shows some results of this methodology by identifying challenges that Internet voting brings to democracy, based on the situation in the countries discussed earlier. These results can be extended by applying the methodology to other cases. In the final section, conclusions and recommendations are presented.

The conclusions regarding the methodology developed in this chapter do not depend on the specific set of countries included in this thesis. However, I certainly do not claim completeness of the list of challenges to democracy that is presented, and more (possibly comparative) case studies may yield additional results.

10.2 Technology in dynamic democracy

In this section, I present the philosophical theories used in the attempt to include voting technology in the discussion on voting and democracy. The method is based on the philosophy of John Dewey, whose views on ethics and democracy have been excellently investigated in the Dutch work by Louis Logister (2004). According to Dewey, institutional changes in a democracy are achieved by a process of reconstruction. I describe the role of technology in this reconstruction in terms of mediation, a concept developed by the postphenomenological approach of Don Ihde (1990) and Peter-Paul Verbeek (2005).

John Dewey's notion of democracy

John Dewey is a well-known philosopher from the United States, who considers himself an instrumentalist. A more widely known term for the movement that he belongs to is pragmatism. In this section, I will briefly introduce his views on the role of reconstruction in democracy. His theory cannot be covered in depth here, but I will provide references for further reading.

Dewey considers everything, including theories, norms and values, as tools that function in the context of experience, where experience means continuous interaction between a human being and her environment. "To Dewey, experience is not a mental storage place for empirical sensations, as proposed by traditional correspondence theories, but a complex integrated activity that is characterised by goal-directedness, prospectivism and growth of meaning" (Logister, 2004, p. 76, translation WP). Dewey's concept of experience necessarily contains something active and something passive, trying and perceiving.

In the context of experience, Dewey frequently uses the concept of habit. This is an acquired tendency to act in a certain way in certain situations (Logister, 2004, p. 91, referring to Dewey's *Human Nature and Conduct*). Since they are acquired, habits are socially transmitted. If a habit is common within a certain society, this common mode of action is called a custom. Habits are reflected in the institutions in a society. The most efficient way to change habits is by starting to change the institutions.

Based on these points of departure, Dewey develops his ethical and political theories. Dewey's ethics refrains from posing specific goals, and states that "growth itself is the only moral 'end'" (Dewey, 1948 [1920], p. 175). By growth, he means increasing ability to solve problems that hinder the continuous stream of experience. Politics concerns decisions on how to rearrange institutions such that growth in society becomes possible. The best way to do this is a democratic one, since it provides the best capacity for mobilising the existing problem-solving resources in a society, especially if it is arranged in a participative way (not only votes, but also direct input from the people in political discussion). "[D]emocracy is a name for a life of free and enriching communion. [...] It will have its consummation when free social inquiry is indissolubly wedded to the art of full and moving communication." (Dewey, 1991 [1927], p. 184).

Logister (2004) argues that the idea of social reconstruction, i.e. the reconstruction of the institutions in a society in order to enable growth, is at the heart of Dewey's political philosophy. He refers to the work of James Campbell (1995) in order to clarify further the idea of social reconstruction, which remains rather implicit in Dewey's own work (Logister, 2004, p. 220–226). Following Campbell, he distinguishes two aspects of Dewey's social reconstruction: intellectual reconstruction and institutional reconstruction. In democracy, intellectual reconstruction precedes institutional reconstruction. Intellectual reconstruction consists of formulating the problems that a society faces, and suggesting solutions to these problems. An important part of this task is the reconstruction of the conceptual meaning of political terms. Institutional reconstruction means evaluating the proposed concepts and solutions, and adapting existing institutions based on this evaluation. Whereas institutional reconstruction requires political discussion and should be based on democratic decisions, intellectual reconstruction is the task of philosophers and scientists.

Dewey's ideas on the role of experience and habits in society thus lead to a particular vision on how society can and should be changed. Science does the intellectual reconstruction, politics does the institutional reconstruction. I think that this separation of concerns can be fruitful for both. Moreover, the concept of intellectual reconstruction itself, as provided by Campbell and Logister based on Dewey's work, can serve as the basis for a particular way of analysing technological developments in society, namely in relation to the reconstruction of our cultural categories. Technology itself can help us to reveal aspects that were reveiled before.

Technological mediation

How can we pro-actively identify the challenges that technological developments bring to our cultural categories? A good example is the mobile phone. The mobile phone is not just a neutral means of solving a communication problem. Although it is effective with regard to its purpose, communication at non-fixed places and during travel, it has also completely changed the way in which people experience each others presence and the way in which people arrange their schedules and meetings. "I'll call you when the train leaves the station; pick me up half an hour later". This also requires people to be reachable by mobile phone. The few people who do not have one by now may

even run the risk of becoming socially excluded.

Several philosophers have described such developments from what is called the empirical turn in philosophy of technology (Achterhuis, 2001). Whereas traditional philosophy of technology had often analysed "technology" as a phenomenon *an sich*. these movements argue that we should analyse the role of concrete technological artifacts in our lives in order to understand what technology is all about. These approaches have been inspired by empirical studies into such developments.

One theory on the role of technology in our experience of our world and in the way in which we realise our existence has been described based on notions of the philosophical movement of phenomenology. Especially intentionality, the directedness of people towards their environment, has been used as a concept in describing changes in the lifeworld invoked by technological developments. It is said that technology can mediate our relation to our world by forcing itself into the intentional relation. Thereby, it may amplify as well as reduce certain aspects of our experience.

The work by Don Ihde (1990) focuses on these forms of mediation. In the mobile phone example, we can state that this technology amplifies the interpretation of known people as directly available for contact, whereas the presence of people we do not know in our direct environment (e.g. in a train) is reduced. Peter-Paul Verbeek (2005) takes one step further in the theory of mediation, and states that technology can not only change our experience, but also the way in which we act, by invitation and inhibition of certain actions. A mobile phone invites calling people when it is not strictly necessary ("I caught the train which I said I would catch"), and this may even become a social norm. At the same time, it inhibits talking to people in the train.

In the same sense, Internet voting is not only a means to make it easier to vote. It can profoundly change the relation between people and their environment, in this case the political world of democracy. Interpretations of what democracy is can be shifted, and Internet voting will invite different voting behaviour. I therefore think that the phenomenological approach can be a fruitful starting point for a description of the possible changes that Internet voting brings to democracy, which can then serve as a basis for an intellectual reconstruction of the concept of voting in the network age.

A combined approach

Pragmatism is an especially helpful philosophical approach in cases where the cultural categories are not fixed. Because of the mediating role of technology, introduction of new technologies is precisely such an issue. What is presented in this chapter is the intellectual reconstruction of the concept of voting based on the technological developments in the information society. In this reconstruction, a new balance between reveiling and revealing is established. It is an instantiation of the monster-conjuring strategy of assimilation, in which not only the technology, but also our cultural categories are considered flexible.

I investigate the mediating role of voting technology in society, and reconstruct the discussion on voting and democracy based on the challenges that technology brings. Thus, the present approach applies the theory of mediation of human experience and existence by technology, not only after the fact, but as an input to the political discussions that will guide the introduction of the new technology. This can be seen as a special approach to constructive technology assessment (Schot and Rip, 1997). I call this approach *reconstructive technology assessment*, since the emerging technology itself challenges us to reconstruct our concepts, our categories.

Technology assessment itself is constructed as well. I do not pretend to have an unmediated point of view from which to judge technology; rather, we accept the challenge of mediation, and identify the challenges the technology brings to the lifeworld it has already partly entered. Those are primarily challenges to our concepts, our distinctions, our cultural categories. Therefore, I speak of *categorical challenges*.

10.3 Challenges to democracy

The advent of Internet voting is not just a matter of changing the means of attaining certain ends. By introducing new technologies, the relation between people and their environment can be changed, in terms of experience and action. In this section, I try to intellectually reconstruct the concept of voting, based on the challenges that the mediating role of Internet voting offers to traditional conceptions of and discussions on democracy. These issues can serve as a starting point for the institutional reconstruction that Internet voting requires. I do not strive for completeness here, but I show the most important issues that were identified based on my knowledge of and experience with online voting systems in different countries. This may reveal opportunities and risks that were reveiled before. Neither do I take an exclusively positive or negative point of view here. The challenges that are identified can work out either way, depending on how we handle them.

A challenge to availability

Availability means that everyone must be able to vote in an election. Also, the costs of participation must be fairly distributed over the population. It should not be excessively more difficult to participate for certain persons than for others.

We have already seen the issues that this entails from a technical perspective. Still, from such a perspective we usually think of the electronic medium as a single channel that must be made and kept available to the citizens, and must be easy to use. If necessary, one could allow citizens to use different instances of the same type of channel in case of failure of one of them, for example voting in any polling station. However, it is now precisely this single channel concept that is being challenged.

Until now, the idea of "same channel for all" guaranteed availability for everyone. In a single district, there was only one means of voting available, with possible exceptions for those in special circumstances. Already, the use of some of these "special

channels" has been subject to liberalisation in some countries. In the Netherlands, additional channels for Dutch citizens abroad are still seen as a separate matter, but other countries have a different approach.

In the UK, the concept of multi-channel elections has already taken hold. In such a concept, the equality of access is no longer based on everybody using the *same* channel, but rather on each person using the channel that is *most convenient* to her. Whether this can be made acceptable depends on the arguments put in place to convince the public that nobody is unacceptably disadvantaged. If we allow Internet voting, we make it easier to vote for certain groups of people. Does this lead to serious disadvantages on the other side of the digital divide?

We must remember that the digital divide is a divide that has been made visible. We can also create a divide between the employed and unemployed, between the people living within 1 km from a polling station and people living further away. A polling station also has a particular "access policy", and will not make the cost of participation equal for everyone. Still, the multi-channel concept makes different divides visible and invisible, which challenges the concept of availability as "the same for everyone". If multi-channel voting is really to replace the existing arrangements, the concept of availability needs reconstruction: it is not only about securing access to one channel, but about securing equal access to multiple channels.

A challenge to authenticity

Verifying the identity of voters, in order to ensure the authenticity of votes, has been based on physical appearance of voters at polling stations. This could be combined with requiring some form of identification (a passport or ID-card), but both in the UK and the Netherlands this was not common practice. Online, impersonation can be quite easy, and the issue of personation in elections therefore needs to be addressed. Research into these issues is being done in the field called *identity management*.

Apart from technical issues of authentication, the question is whether online identities are the same as real-life identities. Psychologically speaking, one's identity is shaped by one's environment. In a different environment, people may take different roles, and express different preferences. This extended notion of identity has implications for Internet voting. The information that is presented on the Internet, the way in which people interact with a computer, the place in which they cast their vote, these may all contribute to shaping the voter's identity, including her preferences. In particular, the home is a private environment, and this is a completely different setting than the public environment of a polling station (Pieters and Becker, 2005).

Thus, Internet voting may bring to democracy a shift in the identity of the voter. Whereas voting is done in complete isolation nowadays, it may become more related to other political activities if the Internet is used, for example via links to other websites. The fact that people vote via the Internet can "link" the voting environment in their experience to all kinds of other options for exercising influence (such as discussion forums). When I vote in a polling station, there is no link at all to my contribution to a discussion on immigration policy in a forum. When I vote at home, I might have

both windows, voting and forum, open at the same time.

The technology may mediate the relation between people and democracy in such a way that the experience of different possibilities of participation is amplified, and active participation is invited, instead of isolating voting from the rest of the lifeworld by means of a voting booth. However, this is not necessarily a benefit. If voters do not have the skills to use these additional possibilities appropriately, it may increase their dependence on opinions articulated by others, e.g. in a forum. On the other hand, if voters do have the skills, it may lead to a new "e-democracy", in which social inclusion in different democratic processes becomes more common.

Authenticity is not only about *verifying* the *official* identity of the voters, but also about *constructing* their *mediated* identity when they vote. This challenge may need to be included in the debate on the future of voting.

A challenge to correctness

Correctness usually refers to the property that all valid votes are counted, and only valid votes. But what is a vote in this respect?

In common sense, democracy means one man, one vote. People are assumed to make their choices individually, based on rational deliberation. This is an individualistic vision, related to the common economic conceptions of individual desires and choices.[101] However, psychological research has indicated that people are not as individual as Enlightenment philosophers might first have thought. Dewey already noticed this, and his concept of habits can be thought of as a way to criticise individualistic theories.

Dewey indicates that by the implicit assumptions of liberalism and individualism, people are assumed to be free, whereas they are at the same time unconsciously suppressed by the very values of these isms. By stressing too much the individual capacities as opposed to social structures, traditional social ties fall apart and people become easy prey for manipulation, such as by mass media. The irony is that by focusing too much on the freedom of the individual, freedom and political discussion seem to be inhibited.

The continuation of the process of individualisation in the last century also has implications for elections. Whereas people tended to vote for the party connected to the social group they belonged to before, they are now free to vote what they want to. At the same time, it becomes more interesting to persuade voters. This is one of the reasons why elections tend to become more and more of a media circus.

Although many alternative visions on democracy are readily available in (scientific) literature, existing institutions and technologies play an important role in maintaining the status quo. Using traditional voting technology, it is hard to think of a different way of collecting votes that would introduce a less individualistic conception of voting

[101] Dewey (1991 [1927]): p. 86 and further. "The utilitarian economic theory was such an important factor in developing the theory, as distinct from the practice, of democratic government that it is worth while to expound it in outline." (p. 91)

and more consciousness of the alternatives that are available to the view that the media offer. In the online case, however, things may have a more flexible nature.

First of all, it becomes more interesting to use different methods of tallying, like weighted voting, where one can mark more than one candidate in a chosen order. Whereas the design of paper ballots or dedicated voting machines does not offer much flexibility,[102] voting via a website allows for all the flexibility that is needed to implement different voting schemes.[103] A user can be taken through different screens, where confirmation can be asked at each point, and - by consistency checking - over-voting or undervoting can be reduced to practically zero, even in case of complicated ballots (Alvarez and Hall, 2004, p. 40). This makes it quite relevant to discuss the benefits of different voting schemes again, and this can be fruitful for our consciousness of alternatives in the democratic process, since we may be allowed to select more than one candidate. When it becomes possible to cast more than one vote, also some of the rational benefit analysis is challenged, since it is no longer required to weigh for example national nature preservation against foreign policy in the choice for one party. One can choose for both, by casting two votes. The concept of voting is subject to reconstruction here.

Secondly, voting may become a more social activity. An interesting feature of the Dutch RIES system (and of other cryptographic methods as well) is that it is infeasible to create a valid vote without the appropriate access token (e.g. a password or a smartcard). In the Dutch paper ballot system, votes are created and collected in a safe place, and never leave the safe environment until they get counted. If creating false votes is impossible, this is not necessary anymore. Anyone may collect votes for her own purpose, and send them to the central counting facility later. For example, political parties may get the opportunity to collect their own votes. Also, interest groups may allow citizens who visit their site to cast a vote for the candidate that the interest group prefers (Alvarez and Hall, 2004, p. 59). One can then give a vote to an organisation that one feels sympathy for, or that one trusts, instead of weighing party views on different issues. The experience of the group character of politics is amplified here, and the individual "rational" aspects are reduced.

Whether this is desirable should be subject to political discussion. People may be more conscious of the alternative options that they have in their participation in democracy. This would be a good thing for social inclusion in terms of the amount of choices available to voters and in the reduced distance between them and the organisation they give their vote to. On the other hand, this may lead to the advent of so-called "one-issue" parties. For example, a nature protection organisation may collect votes for a political party or candidate that mainly focuses on nature, and does not have a clear opinion on immigration policy.

[102] Many people remember the "butterfly ballots" of the US presidential election in Florida, 2000 (see section 2.1). Due to bad design, many people are suspected to have chosen the wrong candidate. If designing ballots for the one man, one vote system is already hard, it is even harder to integrate different methods of tallying into the paper voting system.

[103] This is also true for non-remote forms of Internet voting, where people for example cast their vote on a protected PC located in a polling station.

These options must be considered, however, since the advent of Internet voting makes them feasible, and may mediate people's experience in such a way that these possibilities are amplified in their interpretation of voting. In the same sense in which the mobile phone morphed itself from a seemingly purely instrumental business device into a social device with extensive implications for the way in which people stay in touch, Internet voting may lead to profound changes in voting practices. By mediating the practice of voting, Internet elections may raise the public's sensitivity towards different voting methods. Although people cannot decide themselves how to vote, understanding of the possibilities may increase pressure on the government, and may in the long run change the whole system.

Already, Scotland has decided to use electronic counting by means of optical-scan voting in combination with a switch to the single transferable vote system in local elections (Koopman, Hubbers, Pieters, Poll, and de Vries, 2007). Indeed, electronic technologies may stimulate similar developments elsewhere.

A challenge to secrecy

We have seen different methods to measure confidentiality, anonymity and receipt-freeness in computer systems. But Internet voting "transcends" technical requirements. Secrecy does not only demand secrecy of the vote within the system, but also the impossibility for the voter to prove her choice, securing the freedom of the vote.

Because Internet voting does not allow for government control over the voting environment, guaranteeing secrecy of the ballot is impossible (Jefferson et al., 2004). People can always watch over your shoulder if you cast your vote at home.[104] In this sense, accepting Internet voting as technology for casting votes will change the election system. Moreover, the mediating role of the technology will change the experience of voting, and will reduce the aspect of secrecy in the experience of the voter. If people vote at home, they may be more inclined to accept that their vote is not secret. This means that the introduction of Internet voting may lead to a whole new idea about secrecy in elections. What exactly does this challenge imply?

The secret ballot can be important for two reasons: as instrumental to the freedom of the vote – in terms of prevention of vote buying and coercion – and as an intrinsic value in democracy. In the first case, it relates to social inclusion in the sense that nobody loses her vote by either being forced or selling it. In the second case, it is related to the view that nobody needs to justify her choice in an election. I discuss both reasons in relation to the loss of secrecy in the case of remote voting.

Forced voting is already possible on a small scale in the current Dutch system, since there are limited possibilities for authorising others to vote for you as a proxy.[105] One

[104] This is also known as "family voting". Of course, this also holds for postal ballots, which have been used in various countries to various extents (Alvarez and Hall, 2004, ch. 6). I do not discuss postal ballots further in this chapter.

[105] "Stemmen bij volmacht" (voting by proxy) was introduced in the Netherlands in 1928 (see section 2.4). The possibilities for authorization have been restricted over time, because, especially in local

can force someone else to sign such an authorisation.[106] For the same reason, there is already limited opportunity for vote buying and selling. The question is what will happen if these limits on the "vote market" are abandoned. Measures should be taken to regulate this market, such that the actual number of illegal transactions remains low. If manipulation is reported anyway, secret elections may be the only remedy, but experiments need to tell if people even try. Possible measures include:

- allowing voters to vote more than once, but only for different parties; this reduces the chance of one party gaining absolute majority by buying votes;
- using criminal law to make vote buying and selling less attractive;
- creating a good infrastructure for reporting misuse (e.g. pay double the price a buyer would pay if the potential seller reports it);
- making it more difficult to transfer access tokens (e.g. biometric authentication or smartcards instead of passwords).

Internet voting seems to "force the market out into the open". Whereas small scale vote buying was possible in the old Dutch system as well (due to liberalised proxy voting), the opportunities now become clear. This also requires thinking about measures to prevent force (stealing) and sale. In the old days, people were unconsciously "forced" to vote for the party everyone in their social group voted for. There was not much contact between different social groups. Vote secrecy was necessary to protect the non-conformists within the groups. Nowadays, social ties are much looser. Is vote secrecy still the solution? Or should everything be open? Some research suggests that vote buying may "survive the secret ballot" (Brusco et al., 2004), thus making the value of the secret ballot as an instrument to prevent vote buying less effective. In the same sense, one may wonder if the secret ballot helps against coercion.[107]

When secrecy is considered an intrinsic value, different arguments apply. Not being required to justify one's choice can be helpful if one has a non-conformist opinion. Even the idea that one's vote may not be secret could lead to more conformist voting (Oostveen and Van den Besselaar, 2005).[108]

Therefore, secrecy may be considered essential in order to allow people to express their "real" choice. However, secrecy may also be a source of social exclusion. Is it not true that people will have better chances of being included in the public debate if they openly present their choice? Is it not fruitful for democracy if people debate

elections, there had been cases of active vote gathering; by now, you are allowed to have only 2 authorisations (Art. L 4 Dutch Election Law).

[106] Interestingly, also the abandonment of the obligation to vote in 1970 increased the possibilities for manipulation: one can now force someone else to stay home, without anybody noticing.

[107] Does a wife vote against the will of her husband, even if she is threatened and beaten regularly? Social science research into these issues would be useful, although I am not aware of any such work.

[108] Although the suggestion is valuable, the empirical evidence Oostveen and Van den Besselaar offer is not yet convincing. As the authors suggest, further research is necessary here.

their choices in public? These questions will need renewed deliberation if we wish to implement online voting.

In the RIES system, the sacrifice of secrecy is "compensated" by a new option: it is possible to verify your vote in the results after the elections. This can only be done if your vote is not completely secret, since you need some information about your vote to be able to do the verification procedure afterwards. There is no guarantee that others may not obtain this information from you in some way. However, the verification procedure presents a completely new dimension of elections. People will be less inclined to tacitly accept the results. The technology invites people to be more active in the counting procedure, which may be a good thing for social inclusion in terms of participation in the election procedures, or at least a replacement for the involvement of people in election management at polling stations in current systems. Again, this feature of the specific technology used may influence people's interpretation of elections.

The challenge to secrecy has already been taken up. In Estonia, the law was changed to implement a new idea of secrecy in voting. It is now allowed to vote multiple times, of which only the last one counts. This prevents forced voting to a certain extent, but it led to criticism by the president in terms of inequality. This change is closely related to the concept of "optional secret voting", which we encountered in the 19th century British discussion on the introduction of the ballot (section 2.3). It remains to be seen whether this approach will become widely accepted, but it certainly is a challenge.

A challenge to verifiability

As we have seen in chapter 7, different types of verifiability exist in electronic voting systems. One can easily imagine that an Internet voting system will, depending on the types of verifiability that are offered, include different voters in different ways in the election procedure, and thereby change the image of and trust in democracy.

In this sense, choosing a particular kind of verifiability in a particular experiment is not a choice that only influences this particular system. Instead, the type of verifiability offered and the surrounding practices in the elections may mediate the idea that people have of elections. For example, if the RIES system is successful in an experiment with elections for the water boards, people may start to think that constructive individual verifiability is a good thing in general. People may also wonder why they cannot verify their choice in the same way in a later election that uses a different system.

Thus, I would like to stress that choosing a particular kind of verifiability in an experiment may have political consequences, not only for the elections that the system is being used in, but also in terms of expectations that are raised about future elections. Therefore, it would be a good idea for both scientists and politicians to consider these consequences in their decisions on designing or using a certain system.

In case we choose to implement verifiability features, we have to face the fact that people are generally *not* familiar with vote and result verification, and people will probably not be happy with their verifiability if the complete election system is turned upside down. So how can we maintain familiarity in Internet elections if people are not familiar with verification, but at the same time demand the possibility of verification of the results? The best we can do is preserve as many of the things that people are familiar with in current elections, while offering verification to make Internet elections acceptable. Two main demands, which are not only functional requirements, but also part of a ritual that establishes familiarity with elections, can be mentioned here:

- the demand of the secret ballot;[109]
- the demand of the public character of vote counting.[110]

How do these requirements relate to the various types of verifiability? In the case of individual verifiability, the demand of the secret ballot implies that constructive individual verifiability is not desirable. Thus, from the perspective of connecting to existing experiences, we should choose classical individual verifiability. This does *not* mean that I argue for this type because of functional requirements, but rather from an "if it ain't broke, don't fix it" perspective. *Unless* there is democratic consensus about the desirability of constructive individual verifiability, either from the point of view of enhancing trust or from the point of view that democracy functions better without the secret ballot (which is held for many representational bodies such as parliament and meetings such as party congresses), we had better stick to the demand of the secret ballot, and implement classical individual verifiability.

However, the existing schemes that offer classical individual verifiability, to the best of my knowledge, also offer classical universal verifiability. The limitation of the ability of result computation to dedicated parts of the system, with accompanied proofs of correctness, goes against the demand of the public character of vote counting. Typically, *any* encryption with a public key implies that the public character of vote counting is being set aside, unless the corresponding private key is made public afterwards, which is generally not the case. As much as the secret ballot is an important part of the ritual of voting, so is the public character of vote counting. Therefore, I think that *constructive* universal verifiability, in which any party can do an independent calculation of the result, is preferable, *unless* there is democratic consensus about arguments for the opposite point of view.

I argued that choices for particular kinds of verifiability in experiments may have political implications, not only for the specific election that a system is used in, but also in terms of expectations of future elections. Therefore, it is wise to attempt to arrive at political consensus about the kinds of verifiability that are desirable. I argued that even if verifiability is widely accepted as a good thing, we still have to maintain familiarity with elections in order to make the whole system acceptable. The best we

[109] Cf. Dutch constitution art. 53.2 and Dutch election law ("Kieswet") art. J 15.
[110] Cf. Dutch election law ("Kieswet") art. N 1, N 8 and N 9.

can do here is maintain the existing properties of vote secrecy and public counting. This can be done with a system that establishes classical individual verifiability and constructive universal verifiability.[111]

10.4 Implications for technology

The challenges identified in this chapter can be taken up by computer scientists and system designers. The shifts in distinctions – in cultural categories – that can be expected based on the mediating character of technology, can pro-actively be used in the design of new voting systems.

In relation to availability, an important question is how technology can be designed not only for availability, but for *equal availability*. We have always relied on polling stations to provide access to the voting procedures. Whether these are completely fair is a question not often discussed. However, when voting via the Internet is suggested, the equality argument is often advanced in relation to the digital divide. The major decision to be made is which technologies we can use in order to make the "costs" of voting as equally distributed among the population as possible in case of multi-channel voting. This has been an argument in favour of telephone voting, but precisely voting via this medium seems to be discontinued due to low usage levels. Usability is also an important issue here, and it is hard to make telephone voting comply with this requirement. Such considerations should be addressed in addition to the task of keeping the chosen channels running during the election period.

As for authenticity, the issue of identifying voters was broadened to include the mediation of the voters' identities by the channels used. The main question here is how (remote) voting systems can be designed such that people have to reflect on their choice, avoiding impulsive decisions. An important notion here could be the *virtual polling station*. In a virtual polling station, users are invited to make a well-considered rather than an impulsive decision, and they are advised to cast their votes in secret. This may reduce the problems associated with voting at home, where one invokes a private rather than a public identity.

It is tempting to limit the issue of correctness of voting systems to the electoral systems one is familiar with. Systems that have been designed for a particular electoral context, however, may not be suitable for all types of casting and counting votes, for example if homomorphic encryption is used. Such limitations should not influence the choice for an electoral system, which should be based on political deliberation instead.

[111] The recently proposed Scantegrity system (`www.scantegrity.org`) seems to aim at this combination. Two limitations need to be mentioned though. Firstly, the secrecy of the individual votes depends on procedural rather than technical measures. Secondly, whereas everyone can calculate the results, this is *not* done based on the original votes. Rather, the correspondence between the original votes and the counted votes can be shown probabilistically, where the probability of error or fraud decreases exponentially with the number of ballots.

E-voting and e-counting do enable easier transitions to different and possibly fairer electoral systems such as single transferable vote, and this should not on forehand be limited by the available technology. Also, the issue of where to receive the votes should be addressed. This not only includes decisions on the number of servers, but also the role of local authorities in running their own elections, and even possibilities to cast votes on websites other than the official ones. In all cases, responsibilities for security measures need to be clear, threats need to be identified and research needs to be done into the effects of different arrangements on voter experience and democratic standards.

To solve the issue of secrecy, it has been proposed to allow voters to overwrite their votes. Different variants of this and similar alternatives should be designed and tested, again to allow a reasonable choice. Overwriting may not be the best solution to enforce secrecy in remote voting, and it needs to be investigated how people themselves experience the secret ballot, and how this will change in case of remote voting.

For verifiability, it was argued that classical individual verifiability and constructive universal verifiability would form the most desirable combination with respect to current ideas on voting. This classification may be challenged by the development of systems with different properties. However, it would be advantageous to have electronic voting schemes available that mimic paper voting in this respect, in order to allow a well-founded decision among the different alternatives, and to avoid blindly following the technology.

Instead of the current scientific focus on public key crypto systems, which do not have the property of constructive universal verifiability, and the practical focus on RIES-like systems, which are not receipt-free, I would encourage scientists to investigate the possibilities for designing a system with a combination of classical individual verifiability and constructive universal verifiability. Intuitively, this means that a document is published after the elections in which voters can see that their vote is present (or absent, in case they did not vote), not what they voted for, but from which anyone can compute the final result.

10.5 Reconstructive technology assessment

In this section, I generalise the methodology used in this book, and propose an approach to technology assessment in which distinctions play a key role. They serve as the basis for discovering risks and alternatives.

Technology assessment, it is argued, is necessarily based on features of the technology already under development, and on existing regulations. These mediate our observation of relevant properties, and make reconstruction in Dewey's sense necessary. The method is therefore named *reconstructive technology assessment*. The method proposed is an abstraction of the analysis of the e-voting controversies discussed in this thesis.

Abstracting from technology and law

According to Niklas Luhmann, observation is distinguishing indication. This means that risks are perceived based on available distinctions. They are revealed in the interaction of existing distinctions with the environment. If existing distinctions are inadequate, monsters may appear, and these may lead to changes in our distinctions. We would like to be able to prevent monsters by pro-actively reflecting on our categories in risk assessment.

Technology and law are externalisations of existing distinctions. They are therefore relevant if we wish to implement reflection on categories. We should write down which implicit distinctions are present in technology and law, and thereby get an overview of which sides of distinctions are being marked at present.

Technology and law serve as mirrors of our distinctions in this approach: they tell us something about ourselves. Thereby, they can themselves contribute to updating our ethical framework to the developments they are part of. They can tell us that we could have made different choices, by presenting us with categorical challenges.

Can we mark the other side?

In order to reflect on our distinctions in technology assessment, we should investigate existing technological artifacts, scientific theories and legal arrangements. Then, we write down associations that categorise the specific legal or technological feature within our existing cultural framework. We try to find counterconcepts to the concepts that we wrote down, and thereby challenge the existing categorisation.

On a general level, this chapter has shown how challenges to our concepts can be identified by looking into the "other side" of authenticity, or the "other side" of availability. Identity can be more than something to verify, and availability will mean a different thing in the context of multi-channel voting. However, this approach can also work on a lower level.

For example, if we look at the RIES system, we find that one can verify how one's vote has been counted. Possible associations with this procedure include the concept of proof from logic. In RIES, the presence of your vote is proved by providing a witness (your vote), as in constructive logic. As a counterconcept, we have a proof without a witness, as in classical logic. Could this be used as an alternative? Such systems already exist in the scientific literature. Are these more desirable, more practical or cheaper?

An example from law is the Dutch e-voting regulation. There is a requirement that the way of storing the vote should not allow reconstruction of individual choices (see page 33). Possible associations with "way of storing" include memory and software. If we mark the other side of the distinctions, we may find something like processing and hardware. Is it relevant to include clauses on these aspects as well? Or instead a more general formulation? Such reasoning could have led to the idea of tempest attacks, associated with processing and hardware, or otherwise to a more general formulation of the requirements that would have covered the issue.

As categorical challenges, both new technological options and new legal options can emerge from this process. These constitute alternatives for existing arrangements. Finally, we evaluate the benefits of alternatives that are revealed by means of this process. This includes evaluation of desirability, feasibility and cost.

Reconstructive technology assessment can help us to reveal pro-actively what existing distinctions hide, and how this affects our understanding of the new technology under consideration. Precise methods for implementing this process require further research. Of course, both technology and law need not be implemented in the real world before this process can take place.

Letting go of Nature

In reconstructive technology assessment, we recognise that technology is not merely an external reality, but rather part of a process to which we contribute by means of our categorisation of phenomena. This replaces the distinction between nature and culture by an interactive process, in which many stakeholders can have a role. Even scientists are no longer occupied with Nature, but they join forces in the replacement of confidence with trust. This makes possible different separations of powers, for which Latour already gave some indications (section 4.4). If this helps to reveal different risks by means of different distinctions or categories, instead of amplifying the Nature of existing ones, the discussion on e-voting and other technologies may take a quite different form.

10.6 Conclusions

Following John Dewey, I described the political process in a democracy in terms of intellectual reconstruction and institutional reconstruction. It is important to consider technological developments in the process of intellectual reconstruction, to prevent technology from becoming an unconscious force that changes our world unexpectedly by processes of mediation. In this case, I focused on the role of (remote) electronic voting in reconstructing the concepts involved in discussing elections. Based on this analysis, I argue that there is much more to social inclusion in Internet voting than turnout or security threats: it is not only about making sure that people are not disenfranchised, it is also about new conceptualisations of elections.

There are two types of conclusions to draw: conclusions regarding the methodology developed, and conclusions regarding the results of this methodology in the (limited) analysis of the present chapter. I start with the methodology, which I consider to have been fruitful for the following reasons.

First, the methodology developed in this chapter provides a way to reflect on the mediating role of technology before it is actually introduced, analogous to constructive technology assessment. Second, it connects technological developments with developments in our conceptual framework, or cultural categories (Smits, 2002a,b),

in a pro-active way. I argue that the technology being developed changes the vocabulary used to describe the technology and its requirements, and therefore demands reconstruction.

Reconstructive technology assessment will accept the continuous interaction of the externalisation of our concepts into technology and the internalisation of technology into our concepts. This approach therefore has the potential to explicate challenges on a conceptual level – rather than a technological level only – before they present themselves in the real world. The results of this chapter regarding the categorical challenges of Internet voting illustrate some of the benefits.

The approach can be seen as a special implementation of the monster-conjuring strategy of assimilation, as discussed in chapter 5. It allows us to pro-actively adapt our categories or distinctions to fit the features of new technologies. On a high level, it may contribute to the general categories in our culture. On a lower level, it may contribute to the categories that scientists use in evaluating different alternatives that come up in the discussion.

The results of applying the methodology in this chapter consist of five challenges that Internet voting brings to democracy, which require intellectual reconstruction of the involved concepts. These results are based on the situation in the countries that were studied, and further case studies may provide additional challenges, or refine the ones identified here.

Firstly, the extended idea of availability as equality of the effort of voting is challenged. If new or multiple channels are offered, the current division of costs of voting will be changed. In the case of one new channel, this will lead to a new balance. However, if the idea of multi-channel voting becomes common, continuous advances in technology can lead to a permanent variation in the costs of voting for different groups.

Secondly, the technical challenge of online voter authentication can be supplemented with the question of what constitutes an online identity, and how this is different from identity in the polling station. The voting environment can influence the voters' perception of identity, and may thereby influence their choices. What this means for our idea of democracy needs to be investigated.

Thirdly, Internet voting may require reconstruction of our idea of voting as a completely individual rational choice, a correct count being the addition of these choices, thereby representing the will of the people as calculated by the machine. Internet voting may, by the extremely flexible nature of its user interface, make us more conscious of the different election systems that are possible, ranging from different tallying methods to completely new ways of transferring votes to the central counting facility, e.g. via interest groups. Such possibilities may change our ideas about what a "correct" election is. In all these cases, a shift may occur in the interpretation of voting from the individual weighing of benefits to the collective weighing of alternatives, which may change the way in which social inclusion in democracy is understood and realised.

Fourthly, online voting may require rethinking the concept of vote secrecy. The

mediating role of the technology will change the experience of voting, and will reduce the aspect of secrecy in the traditional sense. One may argue that this concept stems from a social situation that has been changed profoundly since, and even if Internet voting cannot guarantee complete secrecy in the old meaning, this may not be a problem in our new social situation. The questions that this transition raises are how we wish to protect voters from undue influence exercised by others, and how we wish to balance the benefits of secrecy and the benefits of openness for social inclusion. There are many solutions to these problems, and the traditional idea of vote secrecy combined with voluntary party membership is just one of the options.

Finally, we will need a new concept of verifiability in elections. Electronic channels offer more possibilities than paper channels in terms of verifying if a vote has really been counted. If sensible technological choices are made, recounts may still be possible, without requiring a paper trail. However, some forms of verifiability may conflict with existing concepts of secrecy. The relation between secrecy and verifiability therefore requires continued attention.

I investigated which concepts used in discussing democracy require reconstruction from the perspective of the new technology of Internet voting. These challenges to democracy are both opportunities and risks, depending on how they are appropriated within the existing democratic system. Additional case studies may yield more challenges than the ones I identified. I hope I have broadened the discussion on social inclusion in Internet elections from security and turnout to social inclusion in technology-mediated democracy in a broad sense; i.e. to the aspect of civic engagement that is a vital part of being a full member of society.

It is to be recommended to incorporate this broader view into the political discussion on the future of democracy, which may lead to institutional reconstruction based on the concepts sketched here. New technologies may turn out to be a more important factor in the improvement of social inclusion in democracy than changes in procedural aspects of democracy. If we do not take these developments seriously, we cannot steer the adoption of the technology in a proper way, which means that we will have the same situation as in the case of the introduction of voting machines: suddenly the technology is there, and nobody knows whether we really wanted it.

Part VI

Conclusions

Chapter 11

Conclusions and Discussion

"The only possible conclusion the social sciences can draw is: some do, some don't."

– Ernest Rutherford (New Zealander born British chemist, 1871–1937)

In this last chapter, the argument of this thesis is summarised. I will also discuss limitations of the approach and possibilities for future research.

11.1 Conclusions

The main research question was formulated as follows: How can we explain the controversies on e-voting in terms of the conceptual or theoretical dimension of risk, trust and security? There were four subquestions:

1. Which are the similarities and differences between conceptualisations of e-voting in controversies in different countries?

2. Which reasons on the conceptual level make e-voting become a controversial topic for the public?

3. What is the role of (computing) scientists in such discussions?

4. How can we pro-actively use this conceptual level to improve the discussion on e-voting and similar topics?

The answer to each of the questions will be provided in a subsection below.

The cultural construction of controversy

There is a controversy about e-voting in many countries. Some argue that e-voting is fundamentally insecure, scientists propose advanced systems, manufacturers claim that there is nothing wrong. This controversy has to be seen in the wider context of the history of democracy. Most people seem to agree on the major themes of availability, authenticity, correctness, verifiability and secrecy, but these are refined very differently in different cultural contexts (chapter 2). Especially in the UK and the Netherlands, we have seen how history and culture frame the conceptualisations in the e-voting debate; this explains for example the lack of interest in a paper trail in the UK (chapter 3).

Trust in the monster

In most of the literature, social aspects of e-voting are explained in terms of actual security versus perceived security. This distinction can be criticised from the point of view of science and technology studies. From such a perspective, this distinction is a form of "ontological gerrymandering": the drawing of an arbitrary boundary between facts and claims. In this thesis, it has been replaced with a theory that adheres to the social science principle of relativity: social laws should be the same in all reference frames. The basic notions in this framework were adopted from the philosophy of Niklas Luhmann. Central in this approach is the concept of observation as distinguishing indication (chapter 4).

Distinctions have cultural origins. Martijntje Smits argues that technologies that do not fit existing categorisations may be perceived as "monstrous." The severity of the e-voting controversy can be explained by the discovery of the monstrous character of e-voting, in its failure to be categorised as either technological or democratic. Typical of technologies-as-monsters is the drive to adapt them to fit existing categories. The paper trail approach is an example of such a strategy, it is therefore a logical step in the cultural reaction to e-voting (chapter 5).

The recognition of the monstrous character transformed e-voting from an automation of an existing process into a possibly disastrous alternative to traditional paper voting. Measures had to be taken to tame the monster. Because e-voting is now seen as an alternative, it requires trust instead of confidence (chapter 6). Currently, the paper system is perceived as more trustworthy than electronic systems, and scientists try to improve the trustworthiness of computer-based systems by formalising and standardising the requirements, as has been done for paper voting during a long history (chapter 7).

Reve{a/i}ling the risks

However, scientists have different approaches to assess security properties such as availability, authenticity, correctness, verifiability and secrecy. The concepts used are the cultural categories, or distinctions, of the subcultures of science. The effort of science is replacing confidence ("blind trust") by trust ("rational trust"). This is

done by "revealing the risks". In this effort, the cultural categories of the subculture of information security studies play a role, accompanied by their own monsters. The tempest attack was a monster in this sense: it did not fit the existing categories of security of voting machines (chapter 8).

Understanding risk assessment as an "entbergen" means that it both reveals and reveils risks, by distinguishing some aspects but not others. I propose a distinction between "revealed security" and "reveiled security" as an alternative to the actual/perceived distinction.

This distinction denotes whether risks have been made visible or not, for example by means of security and attacker models. In the new distinction of reveiled/revealed, perceived, in the meaning of observed, has a positive connotation rather than the negative one it has in the original concept (chapter 9).

Challenges

In revealing the risks, cultural categories play a role that may themselves be transformed by technology. In this sense, the role of the new technology itself in changing the concepts should be anticipated. Technology is itself a form of "entbergen" and mediates the way in which requirements are determined and risks are revealed. Technology will partly determine its own requirements, and one cannot rely on existing demands; rather, we should try to find new ones *in interaction with the technology*. This "reconstructive technology assessment" is done by acknowledging the categorical challenge that e-voting brings to democracy (chapter 10).

I identified five challenges that remote and/or polling place e-voting bring to democracy – and science.

First of all, the concept of availability needs reconstruction, in Dewey's sense. How we provide equal access in voting to all kinds of different people depends on what we think of as equal. This can be based on the same channel for all or different channels for different people.

Secondly, e-voting technology challenges the concept of authenticity in elections, for people may have different identities in different environments. Even if we manage to make citizens prove their real-world identity online, the ones who vote may not be the same people.

Thirdly, the idea of what a correct election is may be subject to change. This may be in the form of new counting systems or new ways of registering votes. The idea of voting as a supreme act of freedom of the autonomous individual will be challenged if voting is taken from the public sphere (polling station) to the private sphere (home or work). This may mean that Arendt's category of action, of the political world as opposed to the worlds of work and labour, becomes blurred (see section 5.2). If one considers this category as a fundamental attribute of human nature, this probably justifies expelling the monster, i.e. rejecting Internet voting. If one takes a more pragmatic stance, this may also be an opportunity to bring politics closer to the citizens and their lifeworld.

Fourthly, the concept of vote secrecy as the safeguard of autonomy will change. It

is impossible for the authorities to guarantee a private voting environment in people's homes or workplaces. This means that responsibilities for maintaining secrecy will be shifted, and the attribute of secrecy associated with elections in representative democracies may lose some of its power, which may again lead to a less pronounced category of the political as opposed to other forms of human activity.

Fifthly, electronic voting reduces the possibilities for traditional scrutiny of the voting process, but it offers new means of verifying the elections. We need new concepts for verifiability in elections, and discussion needs to take place on which type of verifiability we require.

Understanding the e-voting controversy

The distinction between actual security and perceived security has many advantages. It helps us to distinguish between reported and measured properties (as in perceived waiting time versus actual waiting time). Apart from that, it also has the strategic advantage of enabling the scientist (or politician) to claim access to Nature. In a societal controversy, this can give one the necessary advantage in the debate.

However, from a critical philosophical point of view, nobody has direct access to Nature. The concept of actual security is meaningless from a second-order perspective, and has to be abandoned in order to be able to understand the e-voting controversies on this level. Only if there is very strong agreement on how to measure something – like in time – one can speak about "actual". This does not hold for security. If we still wish to use the concept of perceived security, we will have to use it in a positive sense, and opposed to the concept of non-perceived security. We may also, following the English translation of Heidegger, speak of revealed security and reveiled security.

The acknowledgement that all security is perceived security may lead to a more pragmatic as opposed to conservative attitude towards elections and the challenges that e-voting brings. Such a pragmatic attitude means a change in question from "how can we maintain democracy as it used to be?" (i.e. trying to keep it actually secure) to "where do we want to go with democracy?" Considering elections as a mediated phenomenon means that there are no "clean" or "standard" elections, which leaves room for pragmatic interventions in the changes that our democracy is bound to face. If we allow adapting our categories as well as the new technologies, the information age offers more opportunities than just automating existing procedures.

Concluding, and thereby answering the main research question, understanding the e-voting controversies from the theoretical perspective of risk can take one of two forms: actual-perceived or perceived-hidden. The first is well-known, and I have indicated some philosophical as well as practical problems of this approach. Also, current discussions in computing science about the role of trust within this framework seem to be confusing. As an alternative, an approach was developed in which distinctions do not originate from Nature itself, but from interaction between man and environment. All existing scientific theories employed in this book adhere to this general idea.

actual security	perceived security
science	society
verification	trust

Table 11.1: Traditional terminology

reveiled security	revealed security
society	science
danger	risk
confidence	trust
reliability	trustworthiness
no choice	alternatives
habit	analysis

Table 11.2: Alternative terminology

From this perspective, distinctions, or categories, differ among cultures, and subcultures. What is perceived depends on what has been revealed, and this is culture-specific. Perceived security is no longer reduced to a distortion of actual security, but it becomes a legitimate attempt at understanding security from a specific set of distinctions or categories. Even for our western culture as a whole, perception of security can be said to be based on culture-specific distinctions, such as nature-culture or technology-democracy. This partly explains the controversial character of a technology such as e-voting in this particular culture.

11.2 A summary of terminology

Table 11.1 summarises the traditional terminology used to discuss matters of security in society. In table 11.2, an overview is given of the alternative developed in this thesis. In the traditional view, the discussion starts with an actual situation, accessible by science, of which people have different perceptions. In the alternative view, the discussion starts with reveiled security. Therefore, I intentionally change the position of science to the second column in the new table.

The second table can be read as follows. There exists a situation of cultural distinctions, which reveal certain things and reveil others. This allows us to have confidence in the world as we see it. There may be certain dangers, but these can to an acceptable extent be prevented by the reliability of existing arrangements. Alternatives do not seem to be available, and habit guides the use of the systems. Security, in this situation, is largely reveiled. When alternatives seem to become available, possibly by the drive of science to replace confidence with trust, the situation becomes one of risk. Future problems are attributable to decisions, because there are alternatives. These will have to be analysed to make a trustworthy decision, and security will therefore have to be revealed by means of risk analysis. Science can either initiate the transi-

tion, or play its role later by analysing security when alternatives have already been distinguished.

The categorisation in the latter table is not meant as a necessary division; rather, elements of trust and confidence will be found both in science and in society. However, the emphasis will be different, and this is what I wish to express.

11.3 Discussion

Just as e-voting controversies are not the same in different cultural environments, this thesis would not have been the same in a different scientific environment. This need not be a weakness. Here, I will discuss some considerations about the context and method of the work.

On the role of technical contributions

In this thesis, the presentation of technical results has been limited to a couple of frames in chapter 7. Nonetheless, I think a discussion of the technical contributions is relevant to understanding the implications of the broader results.

During the research described here, I have been working in the Security of Systems group at the Radboud University Nijmegen on a project called "Program security and correctness". The aim of this project was extending the work on verifying program correctness (i.e. safety) embedded in the LOOP tool (van den Berg and Jacobs, 2001) to security properties. My main contribution to this idea has been the work on confidentiality, based on an idea by Bart Jacobs and implemented together with Martijn Warnier (Jacobs et al., 2005). Central to this paper is the notion of *information flow*: information is allowed to flow in certain ways, but not others. The earlier work of the Security of Systems group on correctness has been used by colleagues to build a verifiably correct counting application for a voting system (Hubbers et al., 2004).

Later, I worked together with other colleagues on formalising the concept of anonymity (Garcia et al., 2005), and together with Hugo Jonker from Eindhoven University of Technology on receipt-freeness (Jonker and Pieters, 2006).

What does this technical work achieve in the social controversy? First of all, it helps to enable the transformation of confidence into trust. If we have formal definitions of important concepts, this promotes cooperation between different parties on security assessment of systems. Secondly, elucidating concepts in the discussion, such as verifiability (Pieters, 2006d) makes it possible to differentiate between implementations based on these concepts.

Apart from contributing to the discussion, these concepts can also help to enhance the technology being discussed. If technology is characterised by causal closure, or insulation (Luhmann, 2005 [1993], pp. 87–88), then formalising desirable and undesirable causations can contribute to the building of systems that achieve the right amount of insulation, and prevent unwanted causations. The result of counting in an e-voting system should only depend on the votes, and nothing else, particularly not

the identities of the voters. The relation between the concepts of information flow and causal insulation is a topic for further research.

Finally, I believe that for a contribution to science and technology studies, it is necessary to understand the particular field of science in so much detail that one is able to make significant contributions to it. This is also necessary to feed the results of the STS detour back into the field one is studying, in order to facilitate further research.

On the compatibility of theories

A question that may be asked is whether phenomenology, systems theory and pragmatism do not have enough in common to be used in a single book without thorough consideration of their differences. I would respond that all approaches used in this book challenge the representational view of knowledge and the associated separation of nature and human cognition, and nature and culture, and are therefore useful to provide alternatives to the actual/perceived paradigm.

A more specific response would refer to existing research discussing the compatibility of the 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). Pragmatism is often seen as belonging to a similar movement, even though its points of departure were quite different (Rosenthal and Bourgeois, 1980). Ilharco mentions James and Dewey in his list of contributors to the intellectual tradition his phenomenological approach stems from (Ilharco, 2002, p. 15).

Thus, the combination of the theories would be justifiable from the literature, even though that is not an aim of this book. The aim was and is the understanding of the e-voting controversies. Within this context, many connections have been identified that show the compatibility of the theories in their application to e-voting. The notions of distinctions, cultural categories, revealing and mediation, though originating from different theoretical approaches, all have their role within this investigation, and help to make clear what is at stake. Future research with a more theoretical goal can explicate these relations in more detail.

What did we achieve?

Some people may think that two completely different types of results were achieved in the research described: technical, and society-related. And in a way, that is true. I started the research into societal implications as a side track. However, with the notion of distinction it is possible to see the whole framework as a single one: security in society is about distinctions, both on the societal and on the technical side. Such an approach does not differentiate *a priori* between societal and technical observations; the difference lies in, and only in, the distinctions being employed. This also allows for future research in the use of the concept of distinction in connecting societal and scientific discourses.

The main contribution of this book cannot be said to be the critique of the actual/perceived distinction. In chapter 4, we have seen how others have discussed these concepts. What has been achieved, however, is an exposition of the relevance of the philosophical literature on this issue for a concrete new development. The application to information security seems to be new, and provides valuable insights into communication about information security, such as in the electronic voting controversies. Challenging the actual/perceived paradigm helps to explain both differences between countries (chapter 3) and developments in the same country over time (chapter 10), in terms of distinctions or categories. Moreover, the research described here is – to the best of my knowledge – the first to replace the actual/perceived distinction by on the one hand trust/confidence and on the other hand perceived/non-perceived, also known as revealed/reveiled.

11.4 Opportunities for further research

Many new questions have been raised in the research described in this thesis. I already mentioned the role of technology as a category (or distinction) itself (chapter 5). In the same chapter, the issue of the relation between cultural categories and personal distinctions was raised. In chapter 8, a remark was made about the relation between the idea of categories in scientific subcultures and the notion of a scientific paradigm due to Kuhn. A further study could reveal this relation more precisely.

In computing science, one of the major questions remains the reconciliation of secrecy and verifiability in electronic voting systems. Most importantly, can we combine classical individual verifiability and constructive universal verifiability in a single practical system? Is it possible to combine public vote counting with secrecy of the individual vote? Another interesting idea is to verify the property of verifiability itself. What does it mean, in a mathematical language, that an e-voting system is verifiable?

Also, in order to accommodate a wider spectrum of vote buying activities, the notion of receipt-freeness may be strengthened by using a probabilistic definition. It should not be possible that I can derive with 99% certainty what your choice was, unless the election was nearly unanimous.

For confidentiality, it would be highly relevant to be able to incorporate cryptographic operations in the notion of information flow. Typically, these need to be excluded from causing dependency relations (declassification, Askarov and Sabelfeld (2007)). If I encrypt something, it is dependent on the encrypted information, but it it still impossible to derive anything about the original information without the key. Also, we would like to include different termination modes.[112]

As for the philosophical perspective on confidence and trust, there are opportunities for incorporating these notions in a larger framework describing the relations

[112] In Java, program statements can terminate normally or exceptionally. The way in which the execution of the program proceeds is dependent on this, and may therefore allow the inference of sensitive information.

between people and technology. When do people think of a technology as reliable? When do they consider it trustworthy? What kind of explanation is needed to provide people with assurance in using technologies? These are interesting questions for philosophical study. There are also relations between confidence and trust and the idea of a "niche". When a new technology is offered a protected environment to be experimented with, consciousness of alternatives may increase, and risks may be revealed. In this way, niches allow a transition from confidence to trust. Such an analysis can contribute to the theory of strategic niche management.

On the empirical level, further country studies, both qualitative and quantitative, could provide more information on the relevant challenges that technological developments bring to democracy. Also, empirical operationalisations of the notions of confidence and trust would contribute to enhancing the distinction-based model of information security, by allowing researchers to assess whether relations of assurance are based on confidence or trust. Ideas about the empirical study of distinctions could be helpful in providing tools for implementing the notion of reconstructive technology assessment. By explicating distinctions, we will be able to mark the other side of the distinction, and thereby prevent omissions in technology or law.

In my view, the social science principle of relativity is key to the theory of science and technology studies. One may even go further and, like Latour, treat humans and things symmetrically. It is precisely in the interdisciplinary fields of information science, science and technology studies and ethics of technology that humans and technology can only be understood in their interaction. Such insights are also essential to science and technology policy. It is to these niches of interaction that I hope to contribute in the future.

Chapter 12

Epilogue: on Phenomena

> *"All phenomena are real in some sense, unreal in some sense, meaningless in some sense, real and meaningless in some sense, unreal and meaningless in some sense, and real and unreal and meaningless in some sense."*
>
> – Robert Anton Wilson

Pheno: Is this table real?

Posi: Well, I see it, and you see it, so it must be.

Pheno: Why do we see it?

Posi: Because it is there?

Pheno: Or because we have learnt that it is there.

Posi: What is the difference?

Pheno: If we tell each other that this table exists, its existence may be a social construction.

Posi: A *what*?

Pheno: A social construction. This basically means that it is there because we agree that it is there.

Posi: But we agree that it is there *because* it is there, right? It is unlikely that we get it both wrong.

Pheno: People have thought that the Sun revolved around the Earth. They were wrong.

Posi: One can't be wrong about a table though. It's too basic.

Pheno: What does "basic" mean?

Posi: Something that you can see for yourself, without the help of others or instruments or whatever.

Pheno: You mean you have direct access to this table?

Posi: That's it! I don't need anyone to tell me that this table exists, I can see it for myself.

Pheno: Hmm, I doubt it. Is an atom real?

Posi: Why wouldn't it be?

Pheno: It seems to be just a bunch of phenomena that we label "atom". Why would it be a unity?

Posi: Because people found out that things are made up of atoms!

Pheno: Are they? Or are they made up of protons, neutrons and electrons? Or are they made up of strings?

Posi: Things are made up of atoms, atoms are made up of particles, and particles are made up of strings.

Pheno: Then we should say that things are made up of strings, not atoms.

Posi: That just depends on the level on which we look at things.

Pheno: But you do think that these levels are part of nature?

Posi: Sure.

(Silence)

Pragma: An atom is real because it works if we describe things in terms of atoms.

Posi: Oh, hi Pragma.

Pheno: But does it *exist*?

Pragma: What exists is a matter of definition. Things exist if they are useful to us.

Pheno: Is a species real?

Pragma: If God created the species they would be real.

Systhe: What exists for us is just a clueless environment. We reduce its complexity by means of our own operations. Every distinction we perceive in the environment is essentially ours.

Pheno: Is security real?

Posi: Security? What's that?

Pheno: Something about feeling safe, I guess.

Pragma: *Feeling* safe? I thought it was about bodyguards and stuff.

Pheno: Are bodyguards real?

Posi: People tend to see pink elephants, not bodyguards.

Systhe: I liked the species discussion better.

Posi: Of course, because you relativists are bad for security.

Pragma: You didn't even know what it is!

Posi: That's because nobody *defined* it properly!

Pheno: If there were a proper definition, would it be real?

Posi: Only if the statements in which the definition would be used would correspond to reality.

Pragma: Like redness is real, as long as I stick to saying that this pencil is red?

Posi: That's too easy. Red pencils do not exist, *anymore*. Or do they?

Glossary

actual security	real security, independent from human perception
anonymity	the property that interactions with a system cannot be linked to a person
authenticity	the property that actions in a system can be correctly attributed to (authorised) persons
availability	the property that a system will keep its functionality under specified conditions
ballot stuffing	the practice of filling ballot boxes with illegitimate ballots
buffer overflow	a security vulnerability caused by a failure to check the length of the text read by a program; this may allow an attacker to overwrite memory by offering extremely long input, and have his own program executed
coercion	one person forcing another to make a particular choice in an election
completeness	the property that all true statements are provable in a proof system, in elections: the property that all valid votes are counted
confidence	relation of assurance with the environment when there is no choice between alternatives involved
confidentiality	the property that access to information is limited to specified authorised persons or systems
correctness	the property that the functionality of a system conforms to its design specification

danger	possibility of future loss, caused externally, not attributed to a decision
encryption	the use of coding to make information unrecognisable for unauthorised people
entbergen	(reveal) bring from concealment into unconcealment
family voting	voting with other people present, possibly influencing one's choice
first past the post	an election system in which a single winner is chosen in a given constituency by having the most votes, regardless of whether or not he or she has a majority of votes
gerrymandering	rearranging boundaries of electoral districts to one's own political advantage
hash	a one-way function that generates a fixed-size fingerprint of some information
impersonation	performing a transaction by using a false identity
naturalism	the view that distinctions originate from the environment
niche	a protected environment for a new technology to be experimented with
ontological gerrymandering	rearranging boundaries between claims and facts to one's own political advantage
overvoting	selecting too many options for a particular race in an election
paradigm	a set of shared distinctions in a scientific discipline
perceived security	security in human perception, which is either a distortion of actual security (in the classical paradigm), or a revealing of reveiled security (in the new paradigm)
personation	voting by using a false identity

positivism	a philosophy of science which states that scientific statements can be positively affirmed through rigorous scientific methods
privacy	the property that personal information submitted to a system is not made public
proportional representation	an election system in which the number of seats that a group of candidates receives is closely related to the percentage of votes they obtain
relativism	the view that distinctions originate from human perception
revealed security	security properties that are being distinguished in the environment
reveiled security	security properties that are not being distinguished in the environment
risk	possibility of future loss, attributed to a decision between alternatives
safety	the property ascribed to a system that unintentional failure will have limited effects
secrecy	the property that sensitive information contained in a system is kept confidential
security	the property ascribed to a system that failure due to intentional tampering will have limited effects
smartcard	a card containing a chip, which can store data and run small programs
social construction	something of which the existence (entirely) depends on the social context in which it functions
soundness	the property that all statements provable in a proof system are true, in elections: the property that all counted votes are valid
trust	relation of assurance with the environment, based on analysis of alternatives
undervoting	selecting too few options for a particular race in an election
verifiability	the property that malfunction or manipulation of a system can be detected

Bibliography

M. Abe. Universally verifiable mix-net with verification work independent of the number of mix-servers. In K. Nyberg, editor, *EUROCRYPT 98*, number 1403 in Lect. Notes Comp. Sci., pages 437–447. Springer, 1998.

H. Achterhuis. Introduction: American philosophers of technology. In H. Achterhuis, editor, *American Philosophy of Technology: the Empirical Turn*, pages 1–10. Indiana University Press, 2001.

J. Adams. *Risk*. UCL Press, 1995.

Adviesommissie Inrichting Verkiezingsproces. Stemmen met vertrouwen, September 2007. Available online: `http://www.minbzk.nl/contents/pages/89927/advies.pdf`, consulted November 3, 2007.

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

A.V. Anttiroiko. Building strong e-democracy – the role of technology in developing democracy for the information age. *Communications of the ACM*, 46(9ve):121–128, September 2003.

H. Arendt. *The Human Condition*. University of Chicago Press, Chicago, 1958.

A. Askarov and A. Sabelfeld. Gradual release: Unifying declassification, encryption and key release policies. In *IEEE Symposium on Security and Privacy, 2007*, pages 207–221. IEEE Computer Society, 20–23 May 2007.

H.H. Asquith. The ballot in England. *Political Science Quarterly*, 3(4):654–681, December 1888.

A. Avižienis, J.C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing*, 1(1):11–33, 2004.

F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, and A. Vaccarelli. SEAS: a secure e-voting applet system. In K. Futatsugi, F. Mizoguchi, and N. Yonezaki, editors, *Software security — theories and systems*, LNCS 3233, pages 318–329. Springer, Berlin, 2004.

F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, and A. Vaccarelli. SEAS, a secure e-voting protocol: design and implementation. *Computers & Security*, 24:642–652, 2005.

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.

I. Berlin. *Four concepts of liberty*. Oxford University Press, Oxford, 1969 [1958].

M. Bhargava and C. Palamidessi. Probabilistic anonymity. In Martín Abadi and Luca de Alfaro, editors, *Proceedings of CONCUR 2005*, number 3653 in Lecture Notes in Computer Science. Springer, 2005.

A. Bissett. Some human dimensions of computer virus creation and infection. *International Journal of Human-Computer Studies*, 52(5):899–913, 2000.

B. Blanchet. From secrecy to authenticity in security protocols. In *Static Analysis: 9th International Symposium, SAS 2002, Madrid, Spain, September 17-20, 2002. Proceedings*, number 2477 in Lect. Notes Comp. Sci., pages 29–78. Springer, 2002.

J. Bradbury. The policy implications of differing concepts of risk. *Science, Technology, and Human Values*, 14(4):380–399, 1989.

F. Breuer and A.H. Trechsel. E-voting in the 2005 local elections in Estonia, March 6 2006. Report for the Council of Europe. Available online: `http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/00_E-voting_news/FinalReportEvotingEstoniaCoE6_3_06.asp`.

V. Brusco, M. Nazareno, and S.C. Stokes. Vote buying in Argentina. *Latin American Research Review*, 39(2):66–88, 2004.

Burger@overheid publiekspanel. Stemmen via internet, 2002. Available online: `http://www.burger.overheid.nl/publiekspanel/?id=253`, consulted January 23, 2005.

Burger@overheid publiekspanel. Burger ziet internetstemmen zitten, 2004. Available online: `http://www.burger.overheid.nl/publiekspanel/?id=628`, consulted January 23, 2005.

J. Campbell. *Understanding John Dewey: nature and cooperative intelligence*. Open Court, Chicago, 1995.

D. Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology: Proceedings of Crypto 82*, pages 199–203. Plenum Press, 1983.

D. Chaum. Secret-ballot receipts: true voter-verifiable elections. *IEEE Security & Privacy*, 2(1):38–47, 2004.

D. Chaum, P.Y.A. Ryan, and S. Schneider. A practical voter-verifiable election scheme. In S. de Capitani di Vimercati, P.F. Syverson, and D. Gollmann, editors, *ESORICS 2005, Proceedings*, number 3679 in Lect. Notes Comp. Sci., pages 118–139. Springer, 2005.

K. Chopra and W.A. Wallace. Trust in electronic environments. In *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03)*, 2002.

R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung. Multi-authority secret-ballot elections with linear work. In *Advances in Cryptology - EUROCRYPT'96*, volume 1070 of *LNCS*, pages 72–83. Springer-Verlag, 1996.

R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. In *Advances in Cryptology - EUROCRYPT'97*, volume 1233 of *LNCS*, pages 103–118. Springer-Verlag, 1997.

F.B. Cross. The risk of reliance on perceived risk. *Risk*, 3:59, 1992.

F. Cunningham. *Theories of democracy: a critical introduction.* Routledge, London, 2002.

S. Delaune, S. Kremer, and M.D. Ryan. Coercion-resistance and receipt-freeness in electronic voting. In *Proceedings of the 19th IEEE Computer Security Foundations Workshop (CSFW'06)*, Venice, Italy, July 2006. IEEE Computer Society Press.

Y. Deng, C. Palamidessi, and J. Pang. Weak probabilistic anonymity. In *Proceedings of the 3rd International Workshop on Security Issues in Concurrency (SecCo)*, Electronic Notes in Theoretical Computer Science. Elsevier Science Publishers, 2005.

Department of Defense. Expanding the use of electronic voting technology for UOCAVA citizens, May 2007. Available online: `http://servesecurityreport.org/DoDMay2007.pdf`, consulted June 27, 2007.

J. Dewey. *Reconstruction in philosophy.* Beacon, Boston, MA, 1948 [1920].

J. Dewey. *The public and its problems.* Swallow Press / Ohio University Press, Athens, 1991 [1927].

P.J. Dobson. The philosophy of critical realism – an opportunity for information systems research. *Information System Frontiers*, 3(2):199–210, 2001.

M. Douglas. *Purity and Danger: an Analysis of the Concepts of Pollution and Taboo.* Routledge, London, 1994 [1966].

W. Drechsler. The Estonian e-voting laws discourse: Paradigmatic benchmarking for central and eastern Europe, 2003. Available online: `http://unpan1.un.org/intradoc/groups/public/documents/nispacee/unpan009212.pdf`, consulted January 11, 2006.

W. Drechsler and Ü. Madise. Electronic voting in estonia. In N. Kersting and H. Baldersheim, editors, *Electronic Voting And Democracy*. Palgrave Macmillan, New York, 2004.

W. van Eck. Electromagnetic radiation from video display units: an eavesdropping risk? *Computers & Security*, 4:269–286, 1985.

Election Reform Information Project. Voter-verified paper audit trail legislation & information, 2006. Available online: `http://electionline.org/Default.aspx?tabid=290`, consulted February 8, 2006.

Electoral Commission. Modernising elections: a strategic evaluation of the 2002 electoral pilot schemes, 2002. Available online: `http://www.electoralcommission.org.uk/templates/search/document.cfm/6170`, consulted March 22, 2007.

Electoral Commission. Summary electronic voting may 2007 electoral pilot schemes, August 2007. Available online: `http://www.electoralcommission.org.uk/templates/search/document.cfm/20114`, consulted September 21, 2007.

D. Evans and N. Paul. Election security: perception and reality. *IEEE Security & Privacy*, 2(1):24–31, January/February 2004.

Het Expertise Centrum, consultants voor overheidsinformatisering. Definitierapport kiezen op afstand, 15 September 2000.

Het Expertise Centrum, consultants voor overheidsinformatisering. Stand van zaken automatisering rond verkiezingsproces, 28 May 1999.

D. Fahrenholtz and A. Bartelt. Towards a sociological view of trust in computer science. In M. Schoop and R. Walczuch, editors, *Proceedings of the eighth research symposium on emerging electronic markets (RSEEM 01)*, 2001.

B. Fairweather and S. Rogerson. Technical options report, 2002. Available online: `http://www.dca.gov.uk/elections/e-voting/pdf/tech-report.pdf`, consulted March 22, 2007.

L. Floridi. Information ethics: on the philosophical foundation of computer ethics. *Ethics and Information Technology*, 1(1):37–56, 1999.

R. Ford. Why viruses are and always will be a problem. *NCSA News*, pages 5–7, April 1996.

J. Fournier and M. Tunstall. Cache based power analysis attacks on AES. In L.M. Batten and R. Safavi-Naini, editors, *11th Australasian Conference on Information Security and Privacy – ACISP 2006*, number 4058 in Lect. Notes Comp. Sci., pages 17–28. Springer, 2006.

L. Garber. Melissa virus creates a new type of threat. *Computer*, 32(6):16–19, June 1999.

F. D. Garcia, I. Hasuo, W. Pieters, and P. van Rossum. Provable anonymity. In Ralf Küsters and John Mitchell, editors, *3rd ACM Workshop on Formal Methods in Security Engineering (FMSE 2005)*, pages 63–72. ACM Press, 2005.

L.P. Gerlach. Protest movements and the construction of risk. In B.B. Johnson and V.T. Covello, editors, *The Social and Cultural Construction of Risk*, chapter 5, pages 103–145. D. Reidel, Dordrecht, 1987.

H. Geser. Electronic voting in switzerland. In N. Kersting and H. Baldersheim, editors, *Electronic voting and democracy: a comparative analysis*, pages 75–96. Palgrave Macmillan, 2004.

R.K. Gibson. Elections online: Assessing internet voting in light of the arizona democratic primary. *Political Science Quarterly*, 116(4):561–583, 2001.

J. Goguen and J. Meseguer. Security policies and security models. In *IEEE Symp. on Security and Privacy*, pages 11–20. IEEE Comp. Soc. Press, 1982.

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.

A.D. Gordon and A. Jeffrey. Authenticity by typing for security protocols. *Journal of Computer Security*, 11(4):451 – 519, 2003.

S. Gordon and R. Ford. Real-world anti-virus product reviews and evaluation. In *Proceedings of Security on the I-WAY*, Crystal City, Virginia, 1995. NCSA.

M.G. Graff and K.R. van Wyk. *Secure coding: principles & practices*. O'Reilly & Associates, Sebastopol, CA, 2003.

C. Gross. The early history of the ballot in England. *The American Historical Review*, 3(3):456–463, April 1898.

A. Gumbel. *Steal This Vote: Dirty Elections and the Rotten History of Democracy in America*. Nation Books, New York, 2005.

A. Hansen. Tampering with nature: 'nature' and the 'natural' in media coverage of genetics and biotechnology. *Media, Culture & Society*, 28(6):811–834, 2006.

H. Harbers and W.E. Bijker. Democratisering van de technologische cultuur. *Kennis en methode*, 20(3):308, 1996.

M. Heidegger. *Being and Time*. Blackwell Publishing, 1978.

M. Heidegger. *The Question Concerning Technology, and Other Essays*. Harper Perennial, 1982.

D. Held. *Models of democracy*. Stanford University Press, 1997.

C. Herbst, E. Oswald, and S. Mangard. An AES smart card implementation resistant to power analysis attacks. In *Applied Cryptography and Network Security, 4th International Conference, ACNS 2006, Singapore, June 6-9, 2006, Proceedings*, number 3989 in Lect. Notes Comp. Sci., pages 239–252. Springer, 2006.

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.

M. Hirt and K. Sako. Efficient receipt-free voting based on homomorphic encryption. In B Preneel, editor, *Proc. EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 539–556, 2000.

G.J. Hofstede, C.M. Jonker, S. Meijer, and Tim Verwaart. Modelling trade and trust across cultures. In K. Stølen, W.H. Winsborough, F. Martinelli, and F. Massacci, editors, *Trust Management: 4th International Conference (iTrust 2006), Proceedings*, volume 3986 of *Lect. Notes Comp. Sci.*, pages 120–134. Springer, 2006.

R. Hoogma, R. Kemp, J. Schot, and B. Truffer. *Experimenting for sustainable transport: the approach of strategic niche management*. Routledge, London, 2002.

E. Hubbers, B. Jacobs, J. Kiniry, and M. Oostdijk. Counting votes with formal methods. In C. Rattray, S. Maharaj, and C. Shankland, editors, *Algebraic Methodology and Software Technology (AMAST'04)*, number 3116 in Lect. Notes Comp. Sci., pages 241–257. Springer, 2004.

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. ISBN 0-7695-2413-3.

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

F.M. Ilharco. *Information Technology as Ontology: A Phenomenological Investigation into Information Technology and Strategy In-the-World*. PhD thesis, 2002. Available online: `http://www.lse.ac.uk/collections/informationSystems/pdf/theses/Ilharco.pdf`, consulted November 9, 2007.

B. Jacobs, W. Pieters, and M. Warnier. Statically checking confidentiality via dynamic labels. In *WITS '05: Proceedings of the 2005 workshop on Issues in the theory of security*, pages 50–56, New York, NY, USA, 2005. ACM Press. ISBN 1-58113-980-2. doi: http://doi.acm.org/10.1145/1045405.1045411.

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

D. Jefferson, A.D. Rubin, B. Simons, and D. Wagner. Analyzing internet voting security. *Communications of the ACM*, 47(10):59–64, 2004.

R. Joaquim, A. Zúquete, and P. Ferreira. REVS – a robust electronic voting system. *IADIS International Journal of WWW/Internet*, 1(2), 2003.

H.L. Jonker and W. Pieters. Receipt-freeness as a special case of anonymity in epistemic logic. In *Proceedings of the IAVoSS Workshop On Trustworthy Elections (WOTE 2006)*, Robinson College, Cambridge, June 28 – June 30 2006.

C. Karlof, N. Sastry, and D. Wagner. Cryptographic voting protocols: a systems perspective. In *Proceedings of the 14th USENIX Security Symposium*, pages 33–50, 2005.

N. Kersting, R. Leenes, and J.S. Svensson. Adopting electronic voting: context matters. In N. Kersting and H. Baldersheim, editors, *Electronic Voting And Democracy*, pages 276–205. Palgrave Macmillan, New York, 2004.

J. Keulartz, M. Korthals, M. Schermer, and T. Swierstra. Ethics in a technological culture: A proposal for a pragmatist approach. In J. Keulartz, M. Korthals, M. Schermer, and T. Swierstra, editors, *Pragmatist ethics for a technological culture*, chapter 1, pages 3–21. Kluwer Academic Publishers, 2002.

S. Kim and H. Oh. A new universally verifiable and receipt-free electronic voting scheme using one-way unwappable channels. In C.-H. Chi and K.-Y. Lam, editors, *AWCC 2002*, volume 3309 of *LNCS*, pages 337–345. Springer, 2004.

J.R. Kiniry and D. Cok. Esc/java2: Uniting esc/java and jml: Progress and issues in building and using esc/java2 and a report on a case study involving the use of esc/java2 to verify portions of an internet voting tally system. In *Proceedings of the International Workshop on the Construction and Analysis of Safe, Secure and Interoperable Smart Devices (CASSIS)*, 2004.

J.R. Kiniry, A.E. Morkan, F. Fairmichael, D. Cochran, P. Chalin, M. Oostdijk, and E. Hubbers. The koa remote voting system: A summary of work to date. In *Proceedings of Trustworthy Global Computing (TGC) 2006*, Lucca, Italy, 2006.

P.C. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, number 1666 in Lect. Notes Comp. Sci., pages 388–397. Springer, 1999.

T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach. Analysis of an electronic voting system. In *Proceedings of the 2004 IEEE Symposium on Security and Privacy*, 2004.

P. Koopman, E. Hubbers, W. Pieters, E. Poll, and R. de Vries. Testing the eSTV program for the Scottish local government elections. LaQuSO, Radboud University Nijmegen, March 30 2007.

T. S. Kuhn. *The Structure of Scientific Revolutions.* University of Chicago Press, Chicago, 1962.

B. Lampson, M. Abadi, M. Burrows, and E. Wobber. Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems*, 10(4): 265–310, November 1992.

B. Latour. A relativistic account of einstein's relativity. *Social Studies of Science*, 18 (1):3–44, Feb. 1988.

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

G.T. Leavens, A.L. Baker, and C. Ruby. Preliminary design of jml: a behavioral interface specification language for java. *ACM SIGSOFT Software Engineering Notes*, 31(3), May 2006.

H. van Lente. *Promising technology. The dynamics of expectations in technological developments.* PhD thesis, Univ. of Twente, Enschede, 1993.

L. Logister. *Creatieve democratie: John Dewey's pragmatisme als grondslag voor een democratische samenleving.* DAMON, Budel, 2004.

G. Lowe. Breaking and fixing the Needham-Schroeder public key protocol using FDR. In *Tools and algorithms for the contruction and analysis of systems*, volume 1055 of *Lect. Notes Comp. Sci.*, pages 147–166. Springer, 1996.

N. Luhmann. *Trust and power: two works by Niklas Luhmann.* Wiley, Chichester, 1979.

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

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

N. Luhmann. Familiarity, confidence, trust: problems and alternatives. In D. Gambetta, editor, *Trust: Making and breaking of cooperative relations.* Basil Blackwell, Oxford, 1988.

Ü. Madise, P. Vinkel, and E. Maaten. Internet voting at the elections of local government councils on October 2005, 2006. Available online: `http://www.vvk.ee/english/report2006.pdf`, consulted November 9, 2007.

D. Malkhi, O. Margo, and E. Pavlov. E-voting without 'cryptography'. In *Financial Cryptography '02*, 2002.

R.T. Mercuri. A better ballot box? *IEEE Spectrum*, 39(10):26–50, 2002.

R.T. Mercuri and L.J. Camp. The code of elections. *Communications of the ACM*, 47(10):53–58, 2004.

T.S. Messerges, E.A. Dabbish, and R.H. Sloan. Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, 51(5): 541–552, May 2002.

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.

J. Mohen and J. Glidden. The case for internet voting. *Communications of the ACM*, 44(1):72–85, 2001.

D.P. Moynihan. Building secure elections: E-voting, security and systems theory. *Public administration review*, 64(5), 2004.

G. Munnichs. Whom to trust? Public concerns, late modern risks and expert trustworthiness. *Journal of Agricultural and Environmental Ethics*, 17:113–130, 2004.

M. Nielsen and K. Krukow. On the formal modelling of trust in reputation-based systems. In J. Karhumäki, H. Maurer, and G. Paun, G.and Rozenberg, editors, *Theory Is Forever: Essays Dedicated to Arto Salomaa on the Occasion of His 70th Birthday*, number 3113 in Lect. Notes Comp. Sci., pages 192–204. Springer, 2004.

P. Nikander. Users and trust in cyberspace (transcript of discussion). In B. Christianson, B. Crispo, J.A. Malcolm, and M. Roe, editors, *Security Protocols: 8th International Workshop, Cambridge, UK, April 3-5, 2000, Revised Papers*, number 2133 in Lecture Notes in Computer Science, pages 36–42. Springer, 2001.

P. Nikander and K. Karvonen. Users and trust in cyberspace. In B. Christianson, B. Crispo, J.A. Malcolm, and M. Roe, editors, *Security Protocols: 8th International Workshop, Cambridge, UK, April 3-5, 2000, Revised Papers*, number 2133 in Lecture Notes in Computer Science, pages 24–35. Springer, 2001.

C.B. Nutting. Freedom of silence: constitutional protection against government intrusions in political affairs. *Michigan Law Review*, 47(2):181–222, December 1948.

A.M. Oostveen. *Context Matters: A Social Informatics Perspective on the Design and Implications of Large-Scale e-Government Systems*. PhD thesis, Univ. of Amsterdam, Amsterdam, 2007.

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

A.M. Oostveen and P. Van den Besselaar. The effects of voting technologies on voting behaviour: Issues of trust and social identity. *Social Science Computer Review*, 23 (3):304–311, 2005.

Open Rights Group. May 2007 election report: Findings of the open rights group election observation mission in scotland and england, June 2007. Available online: `http://www.openrightsgroup.org/wp-content/uploads/org_election_report.pdf`, consulted June 25, 2007.

OSCE Office for Democratic Institutions and Human Rights. The Netherlands parliamentary elections 22 November 2006: OSCE/ODIHR election assessment mission report, March 12 2007a. Available online: `http://www.osce.org/item/23602.html`, consulted March 16, 2007.

OSCE Office for Democratic Institutions and Human Rights. Republic of Estonia parliamentary elections 4 march 2007: OSCE/ODIHR election assessment mission report, June 28 2007b. Available online: `http://www.osce.org/documents/odihr/2007/07/25385_en.pdf`, consulted August 1, 2007.

S. Owre, J.M. Rushby, and N. Shankar. PVS: A prototype verification system. In D. Kapur, editor, *Proceedings of the 11th International Conference on Automated Deduction*, volume 607 of *Lect. Notes Comp. Sci.*, pages 748–752. Springer, 1992.

J.H. Park. England's controversy over the secret ballot. *Political Science Quarterly*, 46(1):51–86, March 1931.

A. Pasquinucci. Web voting, security and cryptography. *Computer Fraud and Security*, 2007(3):5–8, March 2007.

D. Phillips and H. Von Spakovsky. Gauging the risks of internet elections. *Communications of the ACM*, 44:72–85, 2001.

W. Pieters. Internet voting: a conceptual challenge to democracy. In E.M. Trauth, D. Howcroft, T. Butler, B. Fitzgerald, and J.I. DeGross, editors, *Social Inclusion: Societal & Organizational Implications for Information Systems: IFIP TC8 WG8.2 International Working Conference, July 12-15, 2006, Limerick, Ireland*, pages 89–103. Springer, 2006a.

W. Pieters. Internet voting: a monstrous alliance between democracy and technology? In F. Sudweeks, H. Hrachovec, and C. Ess, editors, *Fifth international conference on Cultural Attitudes towards Technology and Communication 2006*, pages 115–129,

Tartu, Estonia, June 28 - July 1 2006b. School of Information Technology, Murdoch University.

W. Pieters. Acceptance of voting technology: between confidence and trust. In K. Stølen, W.H. Winsborough, F. Martinelli, and F. Massacci, editors, *Trust Management: 4th International Conference (iTrust 2006), Proceedings*, volume 3986 of *Lect. Notes Comp. Sci.*, pages 283–297. Springer, 2006c.

W. Pieters. What proof do we prefer? variants of verifiability in voting. In P. Ryan, S. Anderson, T. Storer, I. Duncan, and J. Bryans, editors, *Workshop on e-Voting and e-Government in the UK*, pages 33–39, Edinburgh, February 27-28 2006d. e-Science Institute, University of St. Andrews.

W. Pieters and M. Becker. Ethics of e-voting: An essay on requirements and values in Internet elections. In P. Brey, F. Grodzinsky, and L. Introna, editors, *Ethics of New Information Technology: Proc. Sixth International Conference on Computer Ethics: Philosophical Enquiry (CEPE'05)*, pages 307–318, Enschede, 2005. Center for Telematics and Information Technology.

W. Pieters and L. Consoli. Vulnerabilities as monsters: the cultural foundations of computer security (extended abstract). In *European Computing and Philosophy Conference (E-CAP 2006)*, Trondheim, Norway, June 22-24 2006. Available online: `http://www.anvendtetikk.ntnu.no/ecap06/program/Pieters.pdf`.

W. Pieters and H.L. Jonker. Vote buying revisited: implications for receipt-freeness. In *2nd Benelux Workshop on Information and System Security (WISSec 2007)*, Luxembourg city, Luxembourg, September 20–21 2007.

W. Pieters and R. van Haren. E-voting discourses in the uk and the netherlands. Technical Report ICIS-R07020, August 2007.

L. Pratchett. *The implementation of electronic voting in the UK*. LGA Publications, London, 2002. Available online: `http://www.dca.gov.uk/elections/e-voting/pdf/e-voting.pdf`, consulted March 22, 2007.

L. Pratchett and M. Wingfield. Electronic voting in the United Kingdom: lessons and limitations from the UK experience. In N. Kersting and H. Baldersheim, editors, *Electronic Voting And Democracy*, pages 172–189. Palgrave Macmillan, New York, 2004.

C. Pursell. Belling the cat: A critique of technology assessment. *Lex en Scientia*, 10: 130–142, 1979.

B. Randell and P.Y.A. Ryan. Voting technologies and trust. Technical Report CS-TR-911, School of Computing Science, University of Newcastle upon Tyne, 2005.

Chancellerie d'Etat République et Canton de Genève. The Geneva Internet Voting System, 2003. Available online: `http://www.geneve.ch/chancellerie/e-government/doc/pre_projet_eVoting_eng.pdf`, consulted February 7, 2006.

P.A.D. Rezende. Electronic voting systems: is Brazil ahead of its time? *RSA CryptoBytes*, 7(2), 2004.

R. Riedl. Rethinking trust and confidence in European e-government: Linking the public sector with post-modern society. In *Proceedings of I3E 2004*, 2004.

A. Riera and P. Brown. Bringing confidence to electronic voting. *Electronic Journal of e-Government*, 1(1):43–50, 2003.

H. Robers. Electronic elections employing DES smartcards. Master's thesis, December 1998. Available online: `http://www.surfnet.nl/bijeenkomsten/ries/robers_scriptie_election.pdf`, consulted November 9,2007.

S.B. Rosenthal and P.L. Bourgeois. *Pragmatism and Phenomenology: a Philosophic Encounter*. John Benjamins, Amsterdam, 1980.

A.D. Rubin. Security considerations for remote electronic voting. *Communications of the ACM*, 45(12):39–44, 2002.

A.D. Rubin. *Brave New Ballot: The Battle to Safeguard Democracy in the Age of Electronic Voting*. Morgan Road, New York, 2006.

K. Sako and J. Kilian. Receipt-free mix-type voting scheme – a practical solution to the implementation of a voting booth. In L.C. Guillou and J.-J. Quisquater, editors, *EUROCRYPT'95*, volume 921 of *LNCS*, pages 393–403. Springer, 1995.

R.G. Saltman. *The History and Politics of Voting Technology*. Palgrave Macmillan, New York, 2006.

B. Schoenmakers. Compensating for a lack of transparency. In *Proc. of the 10th conference on computers, freedom and privacy*, pages 231–233. ACM, 2000.

J. Schot and A. Rip. The past and future of constructive technology assessment. *Technological forecasting and social change*, 54:251–268, 1997.

T. Selker and J. Goler. Security vulnerabilities and problems with vvpt. Caltech / MIT Voting Technology Project, Working Paper #16, 2004. Available online: `http://www.vote.caltech.edu/media/documents/wps/vtp_wp16.pdf`, consulted February 10, 2006.

B. Shneiderman. Designing trust into online experiences. *Communications of the ACM*, 43(12):57–59, 2000.

K.S. Shrader-Frechette. Perceived risks versus actual risks: Managing hazards through negotiation. *Risk*, 1:341–363, 1990.

M. Smits. Monster ethics: a pragmatist approach to risk controversies on new technology. In *Proceedings of the Research in Ethics and Engineering conference*. Technical University of Delft, April 25–27 2002a.

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

P. Southwell and J. Burchett. Survey of vote-by-mail senate election in the state of Oregon. *Political Science and Politics*, 91(1):53–37, March 1997.

T. Storer and I. Duncan. Practical remote electronic elections for the UK. In S. Marsh, editor, *Proceedings of the Second Annual Conference on Privacy, Security and Trust*, pages 41–45. National Research Council Canada, 2004.

T. Storer and I. Duncan. Electronic voting in the UK: Current trends in deployment, requirements and technologies. In A. Ghorbani and S. Marsh, editors, *Proceedings of the Third Annual Conference on Privacy, Security and Trust*, pages 249–252. University of New Brunswick, October 2005.

D.A. Thompson, P.R. Yarnold, D.R. Williams, and S.L. Adams. Effects of actual waiting time, perceived waiting time, information delivery, and expressive quality on patient satisfaction in the emergency department. *Annals of Emergency Medicine*, 28:657–665, 1996.

P. Tijmes. Martin Heidegger: techniek als metafysica. In H. Achterhuis, editor, *De maat van de techniek*, pages 65–97. Ambo, Baarn, 1992.

J. van den Berg and B. Jacobs. The LOOP compiler for Java and JML. In T. Margaria and W. Yi, editors, *Tools and Algorithms for the Construction and Analysis of Software (TACAS)*, number 2031 in Lect. Notes Comp. Sci., pages 299–312. Springer, 2001.

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

K. Vollan. Observing electronic voting. Technical Report 15/2005, NORDEM, 2005. Available online: `http://www.humanrights.uio.no/forskning/publ/nr/2005/1505.pdf`, consulted February 9, 2006.

P. Wallich. Meta-virus: Breaking the hardware species barrier. *Scientific American*, 273(5):34, 1995.

M. Warschauer. *Technology and Social Inclusion: Rethinking the Digital Divide*. MIT Press, Cambrige, MA, 2004.

M. Weber, R. Hoogma, B. Lane, and J. Schot. *Experimenting with sustainable transport innovations: a workbook for strategic niche management*. University of Twente, Enschede, 1999.

L. Weinstein. Risks of internet voting. *Communications of the ACM*, 43(6):128, 2000.

L. Winner. *Autonomous technology: technics out of control*. MIT Press, 1977.

L. Winner. Do artifacts have politics? *Daedalus*, 109(1):121–136, 1980.

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

A. Xenakis and A. Macintosh. Procedural security and social acceptance in e-voting. In *Proceedings of the 38th Hawaii International Conference on System Sciences (HICSS'05)*. IEEE Computer Society, 2005.

Appendix A

Interview Questions e-Voting Discourses

Part 1: What are the expectations and risks of e-voting as perceived from your perspective?

1. What requirements should an election satisfy?
2. What is the current status of election modernisation in your country?
3. What are, in your view, the main differences between postal voting and paper voting?
4. What are, in your view, the main differences between electronic voting and paper voting?
5. What are, in your view, the main differences between on-site electronic voting and remote electronic voting?
6. What are, in your view, the main differences between remote electronic voting and postal voting?
7. Are postal ballots a suitable replacement for paper voting?
8. Are electronic voting machines a suitable replacement for paper voting?
9. Is remote electronic voting a suitable replacement for paper voting?
10. What were your expectations of previous e-voting projects?
11. What are the main risks of e-voting? Who could be a threat?

12. Do you feel that e-voting projects in your country have been able to meet your expectations?

13. Do you feel that e-voting projects in your country have been successful in mitigating the risks?

14. What are your expectations of future e-voting projects?

Part 2: What is the role of technical experts / political experts / the media, as perceived from your perspective? Are the expectations and risks understood correctly by the other groups?

1. Who do you communicate with on e-voting?

2. What do you think these other parties expect of e-voting?

3. What do you think they judge to be the main risks?

4. What will they expect from you?

5. Who is involved in the decision on e-voting systems and experiments?

6. Who is involved in the certification of e-voting systems?

7. Do you communicate on e-voting with people in other countries?

Technology

8. Is there enough technical expertise in the current and past e-voting projects?

9. Do technical actors understand the political and societal expectations and risks?

10. Are there technical problems that have to be dealt with in (remote) electronic voting?

11. What do you expect from people with technical expertise?

12. What do they expect from you?

13. Do you feel that the technical requirements are realistic?

Politics

14. Is there enough political expertise in the current and past e-voting projects?
15. Do political actors understand the technical expectations and risks?
16. Are there political and legal problems that have to be dealt with in (remote) electronic voting?
17. What do you expect from people with political expertise?
18. What do they expect from you?
19. Do you feel that the political requirements are realistic?

Media

20. Do the media represent adequately the technical and political expectations and risks?
21. Do the media represent adequately the process of the introduction of e-voting?
22. What do you expect from the media?
23. What do the media expect from you?

Part 3: Have assessments of expectations and risks changed since your involvement in e-voting?

1. What is your contribution to the current state of e-voting projects in the country?
2. How do scientific results influence the developments?
3. How do campaigns against e-voting influence the developments? Do you agree with the problems that are mentioned? Do you think these problems have been or can be solved?
4. Have your expectations and risk estimations of e-voting changed since the beginning of your involvement? If so, how and why? Who influenced your opinion?
5. Have the expectations and risk estimations of other parties changed? If so, how and why? Do you evaluate the changes positively or negatively? Did you exercise influence on these parties yourself?
6. Have developments in other countries influenced your expectations and risk estimations?

7. Have changed expectations and risk estimations influenced the projects in your country? If so, what was your contribution?
8. What will happen to democracy due to e-voting? How will it influence our voting system and our democracy?
9. Which factors are critical to a democracy in which (remote) electronic voting is possible?
10. Do you have confidence in the future of e-voting?

Index

Samenvatting (Dutch summary)

La volonté machinale: de stemcomputercontroverse verklaard

Dit proefschrift is een interdisciplinaire wetenschappelijke analyse van de controverses rond elektronisch stemmen bij verkiezingen. Deze technologie is in de afgelopen jaren in veel landen ingevoerd, en in andere landen wordt ermee geëxperimenteerd. We kunnen onderscheid maken tussen elektronisch stemmen op een stemcomputer op het stembureau, en elektronisch stemmen op afstand, bijvoorbeeld via het Internet. Veelal worden aan dergelijke systemen dezelfde eisen gesteld als aan het traditionele stemmen met biljetten: iedere kiesgerechtigde kan stemmen (beschikbaarheid), alleen kiesgerechtigden kunnen stemmen en hooguit 1 keer (authenticiteit), de uitslag moet correct zijn (correctheid), de uitslag moet controleerbaar zijn (controleerbaarheid) en de stemming moet in het geheim plaatsvinden (geheimhouding).

De controverses over elektronisch stemmen zijn empirisch onderzocht in Groot-Brittannië en Nederland door middel van interviews met sleutelfiguren in de discussie. Daarnaast is op basis van literatuur informatie verzameld over de debatten in de Verenigde Staten en Estland. Het blijkt dat experts zeer verschillende meningen hebben over de haalbaarheid en wenselijkheid van elektronische vormen van stemmen. Vaak gaat het daarbij over veiligheid en risico's. Vanwege de meningsverschillen is het zeer moeilijk vast te stellen wat de "feiten", de "werkelijke risico's" zijn.

Onderzoek naar meningsverschillen over elektronisch stemmen gaat vaak uit van een onderscheid tussen werkelijke risico's en gepercipieerde risico's, of werkelijke veiligheid en perceptie van veiligheid. Er wordt dan verklaard waarom de gepercipieerde veiligheid afwijkt van de werkelijke veiligheid. Daarbij wordt voorbijgegaan aan de redelijke observatie dat ook de wetenschappelijke claims over elektronisch stemmen, veelal aangeduid als "feiten", gebaseerd zijn op perceptie, zij het dat het daarbij veelal gaat om meer systematische obervatie van eigenschappen. Bovendien maakt een dergelijk onderscheid het mogelijk de tegenstanders te beschuldigen van het verdraaien van de feiten, waardoor de discussie gemakkelijk polariseert.

In dit proefschrift wordt een alternatieve verklaring gegeven voor het ontstaan van discussie over een nieuwe technologie zoals elektronisch stemmen. Als eerste wordt daarbij het perspectief waarin bepaalde claims een hogere status hebben ("feiten") vervangen door een perspectief waarin de *oorsprong* van de claims in onze observaties voorop staat. Hierbij vormen cultureel bepaalde mogelijkheden om een nieuwe tech-

nologie waar te nemen en te beschrijven de basis. Het blijkt mogelijk te zijn dat een nieuwe technologie leidt tot heftige controverse wanneer deze niet goed te beschrijven is binnen bestaande culturele kaders, binnen de bestaande categorieën die de cultuur gebruikt. Er wordt dan gesproken van een "monster".

Er kan beargumenteerd worden dat elektronisch stemmen zo'n monster is. Waar democratie wordt beschreven door middel van menselijke vrijheid en transparantie, wordt technologie beschreven door middel van deterministische natuurwetten en obscuriteit, en deze combinatie explodeert in de stemcomputer of Internetverkiezingen. Er wordt dan door actiegroepen gesteld dat computers fundamenteel oncontroleerbaar zijn. Men kan het monster proberen te temmen door de technologie aan te passen aan de bestaande kaders, bijvoorbeeld door stemcomputers een printje van de stem te laten maken. Daarbij wordt echter voorbijgegaan aan de specifieke nieuwe mogelijkheden die de technologie biedt, en de uitdagingen die zij biedt aan de culturele orde.

Wanneer een dergelijke explosie heeft plaatsgevonden, zoals in 2006 in Nederland, worden papieren verkiezingen en elektronische verkiezingen serieuze alternatieven, in plaats van verschillende uitwerkingen van hetzelfde proces. Het "blinde" vertrouwen (confidence) zoals dat eerst bestond moet daarom plaats maken voor een nieuw, gefundeerd, vertrouwen (trust). Dit is bij uitstek een taak die door informatici wordt uitgevoerd: zij streven ernaar het blinde vertrouwen in informatiesystemen te minimaliseren, en dit te vervangen door een bewijsbaar goed functioneren. Hoewel sommige informatici beweren dat er afgezien van een print van de stem geen goede oplossingen zijn, werken er ook veel mensen aan geavanceerde methoden om elektronische verkiezingen controleerbaar te maken. Ook naar de technische aspecten van beschikbaarheid, authenticiteit, correctheid en geheimhouding wordt door beveiligingsexperts onderzoek gedaan.

Het probleem met het bouwen van "vertrouwbare" elektronische verkiezingssystemen is dat er vele verschillende definities van de verschillende gewenste eigenschappen in gebruik zijn. Dit suggereert dat ook op wetenschappelijk niveau culturele kaders een belangrijke rol spelen en richting geven aan het onderzoek. Dit betekent dat ook hier "monsters" kunnen ontstaan: beveiligingslekken die niet passen binnen de bestaande concepten en definities, en daardoor niet goed waargenomen kunnen worden. Het behoort tot de verantwoordelijkheid van onderzoekers om zich hiervan bewust te zijn, en steeds op zoek te gaan naar verbetering van de kaders die de wereld van de informatiebeveiliging beschrijven.

We introduceren nieuwe terminologie die dit proces beschrijft. Hierbij wordt niet langer gesproken van "werkelijke veiligheid" en "gepercipieerde veiligheid", maar van "verborgen veiligheid" en "ontborgen veiligheid". Eigenschappen van systemen moeten "ontborgen" worden om zichtbaar te zijn. Deze term is afkomstig van de Duitse filosoof Martin Heidegger. Afhankelijk van hun subcultuur zullen mensen in staat zijn bepaalde aspecten van veiligheid en risico waar te nemen, maar andere aspecten niet. Dit betekent dat de zogenaamde "feiten" altijd gebaseerd zijn op de "onverborgenheid" van een bepaalde groep. Risico-analyse behelst het "bestellen" van de risico's; een geforceerde manier van "ontbergen". Hierdoor wordt het blinde

vertrouwen (confidence) omgezet in gefundeerd vertrouwen (trust), of juist gefundeerd wantrouwen.

Het proces van ontbergen wordt op haar beurt beïnvloed door de technologische ontwikkelingen. Wanneer er al geëxperimenteerd wordt met de nieuwe technologie, zal de aanwezigheid van de apparaten leiden tot verschuivingen in waarneming en de daarbij gebruikte categorieën of concepten. De observaties zullen leiden tot het stellen van nieuwe eisen, die worden geformuleerd middels nieuwe of gewijzigde categorieën of concepten. Daarom kan gesproken worden van een "categorische uitdaging" die elektronische verkiezingen bieden aan de democratie. Omdat de ontwikkelingen van de technologie en het culturele kader hand in hand gaan en elkaar beïnvloeden, is het niet mogelijk de technologie puur vanuit de bestaande kaders te evalueren. Daarom zal in de toekomst meer onderzoek gedaan moeten worden naar "reconstructive technology assessment".

De discussie over elektronisch stemmen kan niet goed begrepen worden zonder de culturele kaders en de bijbehorende concepten in de analyse te betrekken. Het zijn juist deze concepten die een verklaring kunnen bieden voor verschillen in de beoordeling van claims, omdat zij verschillende observaties mogelijk maken. In deze context biedt het onderscheid tussen "ontborgen veiligheid" en "verborgen veiligheid" een beter uitgangspunt voor het begrijpen van controverses dan het onderscheid tussen "werkelijke veiligheid" en "perceptie van veiligheid".

Summary

La volonté machinale: understanding the electronic voting controversy

This PhD thesis is an interdisciplinary scientific analysis of the controversies around electronic voting in elections. This technology has recently been introduced in many countries, and other countries are experimenting with it. We can distinguish between electronic voting by means of a voting computer at a polling station, and remote electronic voting, e.g. via the Internet. Often, these systems have to meet the same requirements as traditional voting by ballot: each voter should be able to vote (availability), only eligible voters can vote and at most once (authenticity), the result should be correct (correctness), the result should be verifiable (verifiability) and voting should be secret (secrecy).

E-voting controversies were investigated empirically in the United Kingdom and the Netherlands, by means of interviews with key persons in the discussion. Also, literature study provided information on the debates in the United States and Estonia. The results indicate that experts have very different opinions on the possibility and desirability of electronic forms of voting. Often, security and risk play a key role. Because of the differences in opinion, it is extremely hard to assess what the "facts", the "actual risks", are.

Research into different opinions on e-voting often starts from a distinction between actual risks and perceived risks, or actual security and perceived security. It is then explained why perceived security deviates from actual security. Such an approach ignores the reasonable hypothesis that scientific claims about electronic voting, usually called "facts", are based on perception as well, although this normally involves more systematic observation of properties. Besides, such a distinction makes it possible to accuse opponents of manipulating the facts, making the discussion an easy prey to polarisation.

In this thesis, an alternative explanation is given for the emergence of discussion on a new technology such as e-voting. First, the perspective in which certain claims have a higher status ("facts") is replaced by a perspective emphasising the *origin* of the claims in our observations. Culturally determined possibilities to perceive and describe a new technology play a key role. It turns out to be possible that a new technology leads to strong controversy when it cannot easily be described within existing cultural frameworks, within the existing categories that the culture employs.

We then speak of a "monster".

It can be argued that e-voting is such a monster. Whereas democracy is described by means of human freedom and transparency, technology is described by means of deterministic laws of nature and obscurity, and this combination explodes in the voting computer or Internet elections. Then, activist groups claim that computers are fundamentally unverifiable. One can try to tame the monster by adapting the technology to the existing framework, for example by having the voting computers make a print of each vote. However, this ignores the specific new possibilities that the technology provides, and the challenges it offers to the cultural order.

When such an explosion has taken place, like in 2006 in the Netherlands, the trust of the citizens is damaged. E-voting is constituted as a possibly disastrous alternative to paper voting, and the "blind" trust (*confidence*) which existed has to give way to rational trust (*trust*). This is a task that computer scientists can take care of: they aim at minimising blind trust in information systems, and replacing this by a provably correct behaviour. Although some computer scientists claim that there are no good solutions except for a print of each vote, many people work on advanced methods to provide verifiability in electronic elections. Security experts also address the technical aspects of availability, authenticity, correctness and secrecy.

The problem with building trustworthy electronic election systems is that many different definitions of the various desired properties are in use. This suggests that cultural frameworks play a role at scientific level too, and that they guide the research. This means that "monsters" can arise here as well: security weaknesses that do not fit in the existing concepts and definitions, and therefore cannot be perceived. It is part of the responsibility of researchers to be aware of this, and strive for continuous improvement of the distinctions that describe the world of information security.

We introduce new terminology that describes this process. We no longer speak of "actual security" and "perceived security", but of "reveiled security" and "revealed security". Properties of systems have to be "revealed" in order to become visible. This term is due to the German philosopher Martin Heidegger. Dependent on their subculture, people will be able to perceive certain aspects of security and risk, but not others. This means that so-called "facts" are always based on the "revealedness" of a specific group. Risk analysis involves "ordering" the risks, a forced way of "revealing". This transforms blind trust (confidence) into rational trust (trust), or rational distrust.

The process of "revealing", in its turn, is influenced by the technological developments. When the new technology is being experimented with, the presence of the devices will lead to shifts in perception and the categories or concepts employed therein. The observations will lead to new requirements, formulated by means of new or changed categories or concepts. We can therefore speak of a "categorical challenge" that electronic voting offers to democracy. Because the developments of the technology and the cultural framework go hand in hand and influence each other, it is not possible to evaluate the technology purely from the existing framework. Therefore, we need future research into "reconstructive technology assessment".

The discussion on e-voting cannot be adequately understood without including the cultural framework and the corresponding concepts and categories in the analysis.

Precisely these concepts can offer an explanation for differences in the evaluation of claims, because they enable different observations. In this context, the distinction between “revealed security” and “reveiled security” offers a better starting point for understanding the controversies than the distinction between “actual security” and “perceived security”.

Curriculum Vitae

Wolter Pieters was born in Pijnacker, the Netherlands, on February 4, 1978. After graduating from secondary school (Marnix College, Ede), he studied computer science and philosophy of science, technology and society at the University of Twente. In 2003, he joined the Security of Systems group at Radboud University Nijmegen as a Ph.D student. After having done research in program and protocol verification, he focused on the electronic voting debate. Meanwhile, he taught courses in information security and research methods. In 2006, he spent six weeks at the Department of Media and Communication at the University of Leicester to study the electronic voting debate in the UK.

Titles in the IPA Dissertation Series since 2002

M.C. van Wezel. *Neural Networks for Intelligent Data Analysis: theoretical and experimental aspects.* Faculty of Mathematics and Natural Sciences, UL. 2002-01

V. Bos and J.J.T. Kleijn. *Formal Specification and Analysis of Industrial Systems.* Faculty of Mathematics and Computer Science and Faculty of Mechanical Engineering, TU/e. 2002-02

T. Kuipers. *Techniques for Understanding Legacy Software Systems.* Faculty of Natural Sciences, Mathematics and Computer Science, UvA. 2002-03

S.P. Luttik. *Choice Quantification in Process Algebra.* Faculty of Natural Sciences, Mathematics, and Computer Science, UvA. 2002-04

R.J. Willemen. *School Timetable Construction: Algorithms and Complexity.* Faculty of Mathematics and Computer Science, TU/e. 2002-05

M.I.A. Stoelinga. *Alea Jacta Est: Verification of Probabilistic, Real-time and Parametric Systems.* Faculty of Science, Mathematics and Computer Science, KUN. 2002-06

N. van Vugt. *Models of Molecular Computing.* Faculty of Mathematics and Natural Sciences, UL. 2002-07

A. Fehnker. *Citius, Vilius, Melius: Guiding and Cost-Optimality in Model Checking of Timed and Hybrid Systems.* Faculty of Science, Mathematics and Computer Science, KUN. 2002-08

R. van Stee. *On-line Scheduling and Bin Packing.* Faculty of Mathematics and Natural Sciences, UL. 2002-09

D. Tauritz. *Adaptive Information Filtering: Concepts and Algorithms.* Faculty of Mathematics and Natural Sciences, UL. 2002-10

M.B. van der Zwaag. *Models and Logics for Process Algebra.* Faculty of Natural Sciences, Mathematics, and Computer Science, UvA. 2002-11

J.I. den Hartog. *Probabilistic Extensions of Semantical Models.* Faculty of Sciences, Division of Mathematics and Computer Science, VUA. 2002-12

L. Moonen. *Exploring Software Systems.* Faculty of Natural Sciences, Mathematics, and Computer Science, UvA. 2002-13

J.I. van Hemert. *Applying Evolutionary Computation to Constraint Satisfaction and Data Mining.* Faculty of Mathematics and Natural Sciences, UL. 2002-14

S. Andova. *Probabilistic Process Algebra.* Faculty of Mathematics and Computer Science, TU/e. 2002-15

Y.S. Usenko. *Linearization in μCRL.* Faculty of Mathematics and Computer Science, TU/e. 2002-16

J.J.D. Aerts. *Random Redundant Storage for Video on Demand.* Faculty of Mathematics and Computer Science, TU/e. 2003-01

M. de Jonge. *To Reuse or To Be Reused: Techniques for component composition and construction.* Faculty of Natural Sciences, Mathematics, and Computer Science, UvA. 2003-02

J.M.W. Visser. *Generic Traversal over Typed Source Code Representations.* Faculty of Natural Sciences,

Mathematics, and Computer Science, UvA. 2003-03

S.M. Bohte. *Spiking Neural Networks.* Faculty of Mathematics and Natural Sciences, UL. 2003-04

T.A.C. Willemse. *Semantics and Verification in Process Algebras with Data and Timing.* Faculty of Mathematics and Computer Science, TU/e. 2003-05

S.V. Nedea. *Analysis and Simulations of Catalytic Reactions.* Faculty of Mathematics and Computer Science, TU/e. 2003-06

M.E.M. Lijding. *Real-time Scheduling of Tertiary Storage.* Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2003-07

H.P. Benz. *Casual Multimedia Process Annotation – CoMPAs.* Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2003-08

D. Distefano. *On Modelchecking the Dynamics of Object-based Software: a Foundational Approach.* Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2003-09

M.H. ter Beek. *Team Automata – A Formal Approach to the Modeling of Collaboration Between System Components.* Faculty of Mathematics and Natural Sciences, UL. 2003-10

D.J.P. Leijen. *The λ Abroad – A Functional Approach to Software Components.* Faculty of Mathematics and Computer Science, UU. 2003-11

W.P.A.J. Michiels. *Performance Ratios for the Differencing Method.* Faculty of Mathematics and Computer Science, TU/e. 2004-01

G.I. Jojgov. *Incomplete Proofs and Terms and Their Use in Interactive Theorem Proving.* Faculty of Mathematics and Computer Science, TU/e. 2004-02

P. Frisco. *Theory of Molecular Computing – Splicing and Membrane systems.* Faculty of Mathematics and Natural Sciences, UL. 2004-03

S. Maneth. *Models of Tree Translation.* Faculty of Mathematics and Natural Sciences, UL. 2004-04

Y. Qian. *Data Synchronization and Browsing for Home Environments.* Faculty of Mathematics and Computer Science and Faculty of Industrial Design, TU/e. 2004-05

F. Bartels. *On Generalised Coinduction and Probabilistic Specification Formats.* Faculty of Sciences, Division of Mathematics and Computer Science, VUA. 2004-06

L. Cruz-Filipe. *Constructive Real Analysis: a Type-Theoretical Formalization and Applications.* Faculty of Science, Mathematics and Computer Science, KUN. 2004-07

E.H. Gerding. *Autonomous Agents in Bargaining Games: An Evolutionary Investigation of Fundamentals, Strategies, and Business Applications.* Faculty of Technology Management, TU/e. 2004-08

N. Goga. *Control and Selection Techniques for the Automated Testing of Reactive Systems.* Faculty of Mathematics and Computer Science, TU/e. 2004-09

M. Niqui. *Formalising Exact Arithmetic: Representations, Algorithms and Proofs.* Faculty of Science, Mathematics and Computer Science, RU. 2004-10

A. Löh. *Exploring Generic Haskell.* Faculty of Mathematics and Computer Science, UU. 2004-11

I.C.M. Flinsenberg. *Route Planning Algorithms for Car Navigation.* Faculty of Mathematics and Computer Science, TU/e. 2004-12

R.J. Bril. *Real-time Scheduling for Media Processing Using Conditionally Guaranteed Budgets.* Faculty of Mathematics and Computer Science, TU/e. 2004-13

J. Pang. *Formal Verification of Distributed Systems.* Faculty of Sciences, Division of Mathematics and Computer Science, VUA. 2004-14

F. Alkemade. *Evolutionary Agent-Based Economics.* Faculty of Technology Management, TU/e. 2004-15

E.O. Dijk. *Indoor Ultrasonic Position Estimation Using a Single Base Station.* Faculty of Mathematics and Computer Science, TU/e. 2004-16

S.M. Orzan. *On Distributed Verification and Verified Distribution.* Faculty of Sciences, Division of Mathematics and Computer Science, VUA. 2004-17

M.M. Schrage. *Proxima - A Presentation-oriented Editor for Structured Documents.* Faculty of Mathematics and Computer Science, UU. 2004-18

E. Eskenazi and A. Fyukov. *Quantitative Prediction of Quality Attributes for Component-Based Software Architectures.* Faculty of Mathematics and Computer Science, TU/e. 2004-19

P.J.L. Cuijpers. *Hybrid Process Algebra.* Faculty of Mathematics and Computer Science, TU/e. 2004-20

N.J.M. van den Nieuwelaar. *Supervisory Machine Control by Predictive-Reactive Scheduling.* Faculty of Mechanical Engineering, TU/e. 2004-21

E. Ábrahám. *An Assertional Proof System for Multithreaded Java -Theory and Tool Support-* . Faculty of Mathematics and Natural Sciences, UL. 2005-01

R. Ruimerman. *Modeling and Remodeling in Bone Tissue.* Faculty of Biomedical Engineering, TU/e. 2005-02

C.N. Chong. *Experiments in Rights Control - Expression and Enforcement.* Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2005-03

H. Gao. *Design and Verification of Lock-free Parallel Algorithms.* Faculty of Mathematics and Computing Sciences, RUG. 2005-04

H.M.A. van Beek. *Specification and Analysis of Internet Applications.* Faculty of Mathematics and Computer Science, TU/e. 2005-05

M.T. Ionita. *Scenario-Based System Architecting - A Systematic Approach to Developing Future-Proof System Architectures.* Faculty of Mathematics and Computing Sciences, TU/e. 2005-06

G. Lenzini. *Integration of Analysis Techniques in Security and Fault-Tolerance.* Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2005-07

I. Kurtev. *Adaptability of Model Transformations.* Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2005-08

T. Wolle. *Computational Aspects of Treewidth - Lower Bounds and Network*

Reliability. Faculty of Science, UU. 2005-09

O. Tveretina. *Decision Procedures for Equality Logic with Uninterpreted Functions*. Faculty of Mathematics and Computer Science, TU/e. 2005-10

A.M.L. Liekens. *Evolution of Finite Populations in Dynamic Environments*. Faculty of Biomedical Engineering, TU/e. 2005-11

J. Eggermont. *Data Mining using Genetic Programming: Classification and Symbolic Regression*. Faculty of Mathematics and Natural Sciences, UL. 2005-12

B.J. Heeren. *Top Quality Type Error Messages*. Faculty of Science, UU. 2005-13

G.F. Frehse. *Compositional Verification of Hybrid Systems using Simulation Relations*. Faculty of Science, Mathematics and Computer Science, RU. 2005-14

M.R. Mousavi. *Structuring Structural Operational Semantics*. Faculty of Mathematics and Computer Science, TU/e. 2005-15

A. Sokolova. *Coalgebraic Analysis of Probabilistic Systems*. Faculty of Mathematics and Computer Science, TU/e. 2005-16

T. Gelsema. *Effective Models for the Structure of pi-Calculus Processes with Replication*. Faculty of Mathematics and Natural Sciences, UL. 2005-17

P. Zoeteweij. *Composing Constraint Solvers*. Faculty of Natural Sciences, Mathematics, and Computer Science, UvA. 2005-18

J.J. Vinju. *Analysis and Transformation of Source Code by Parsing and Rewriting*. Faculty of Natural Sciences, Mathematics, and Computer Science, UvA. 2005-19

M.Valero Espada. *Modal Abstraction and Replication of Processes with Data*. Faculty of Sciences, Division of Mathematics and Computer Science, VUA. 2005-20

A. Dijkstra. *Stepping through Haskell*. Faculty of Science, UU. 2005-21

Y.W. Law. *Key Management and Link-Layer Security of Wireless Sensor Networks: Energy-Efficient Attack and Defense*. Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2005-22

E. Dolstra. *The Purely Functional Software Deployment Model*. Faculty of Science, UU. 2006-01

R.J. Corin. *Analysis Models for Security Protocols*. Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2006-02

P.R.A. Verbaan. *The Computational Complexity of Evolving Systems*. Faculty of Science, UU. 2006-03

K.L. Man and R.R.H. Schiffelers. *Formal Specification and Analysis of Hybrid Systems*. Faculty of Mathematics and Computer Science and Faculty of Mechanical Engineering, TU/e. 2006-04

M. Kyas. *Verifying OCL Specifications of UML Models: Tool Support and Compositionality*. Faculty of Mathematics and Natural Sciences, UL. 2006-05

M. Hendriks. *Model Checking Timed Automata - Techniques and Applications*. Faculty of Science, Mathematics and Computer Science, RU. 2006-06

J. Ketema. *Böhm-Like Trees for Rewriting*. Faculty of Sciences, VUA. 2006-07

C.-B. Breunesse. *On JML: Topics in Tool-Assisted Verification of JML Programs*. Faculty of Science, Mathematics and Computer Science, RU. 2006-08

B. Markvoort. *Towards Hybrid Molecular Simulations*. Faculty of Biomedical Engineering, TU/e. 2006-09

S.G.R. Nijssen. *Mining Structured Data*. Faculty of Mathematics and Natural Sciences, UL. 2006-10

G. Russello. *Separation and Adaptation of Concerns in a Shared Data Space*. Faculty of Mathematics and Computer Science, TU/e. 2006-11

L. Cheung. *Reconciling Nondeterministic and Probabilistic Choices*. Faculty of Science, Mathematics and Computer Science, RU. 2006-12

B. Badban. *Verification Techniques for Extensions of Equality Logic*. Faculty of Sciences, Division of Mathematics and Computer Science, VUA. 2006-13

A.J. Mooij. *Constructive Formal Methods and Protocol Standardization*. Faculty of Mathematics and Computer Science, TU/e. 2006-14

T. Krilavicius. *Hybrid Techniques for Hybrid Systems*. Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2006-15

M.E. Warnier. *Language Based Security for Java and JML*. Faculty of Science, Mathematics and Computer Science, RU. 2006-16

V. Sundramoorthy. *At Home In Service Discovery*. Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2006-17

B. Gebremichael. *Expressivity of Timed Automata Models*. Faculty of Science, Mathematics and Computer Science, RU. 2006-18

L.C.M. van Gool. *Formalising Interface Specifications*. Faculty of Mathematics and Computer Science, TU/e. 2006-19

C.J.F. Cremers. *Scyther - Semantics and Verification of Security Protocols*. Faculty of Mathematics and Computer Science, TU/e. 2006-20

J.V. Guillen Scholten. *Mobile Channels for Exogenous Coordination of Distributed Systems: Semantics, Implementation and Composition*. Faculty of Mathematics and Natural Sciences, UL. 2006-21

H.A. de Jong. *Flexible Heterogeneous Software Systems*. Faculty of Natural Sciences, Mathematics, and Computer Science, UvA. 2007-01

N.K. Kavaldjiev. *A run-time reconfigurable Network-on-Chip for streaming DSP applications*. Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2007-02

M. van Veelen. *Considerations on Modeling for Early Detection of Abnormalities in Locally Autonomous Distributed Systems*. Faculty of Mathematics and Computing Sciences, RUG. 2007-03

T.D. Vu. *Semantics and Applications of Process and Program Algebra*. Faculty of Natural Sciences, Mathematics, and Computer Science, UvA. 2007-04

L. Brandán Briones. *Theories for Model-based Testing: Real-time and*

Coverage. Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2007-05

I. Loeb. *Natural Deduction: Sharing by Presentation*. Faculty of Science, Mathematics and Computer Science, RU. 2007-06

M.W.A. Streppel. *Multifunctional Geometric Data Structures*. Faculty of Mathematics and Computer Science, TU/e. 2007-07

N. Trčka. *Silent Steps in Transition Systems and Markov Chains*. Faculty of Mathematics and Computer Science, TU/e. 2007-08

R. Brinkman. *Searching in encrypted data*. Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2007-09

A. van Weelden. *Putting types to good use*. Faculty of Science, Mathematics and Computer Science, RU. 2007-10

J.A.R. Noppen. *Imperfect Information in Software Development Processes*. Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2007-11

R. Boumen. *Integration and Test plans for Complex Manufacturing Systems*. Faculty of Mechanical Engineering, TU/e. 2007-12

A.J. Wijs. *What to do Next?: Analysing and Optimising System Behaviour in Time*. Faculty of Sciences, Division of Mathematics and Computer Science, VUA. 2007-13

C.F.J. Lange. *Assessing and Improving the Quality of Modeling: A Series of Empirical Studies about the UML*. Faculty of Mathematics and Computer Science, TU/e. 2007-14

T. van der Storm. *Component-based Configuration, Integration and Delivery*. Faculty of Natural Sciences, Mathematics, and Computer Science, UvA. 2007-15

B.S. Graaf. *Model-Driven Evolution of Software Architecturest*. Faculty of Electrical Engineering, Mathematics, and Computer Science Delft University of Technology. 2007-16

A.H.J. Mathijssen. *Logical Calculi for Reasoning with Binding*. Faculty of Mathematics and Computer Science, TU/e. 2007-17

D. Jarnikov. *QoS framework for Video Streaming in Home Networks*. Faculty of Mathematics and Computer Science, TU/e. 2007-18

M.A. Abam. *New Data Structures and Algorithms for Mobile Data*. Faculty of Mathematics and Computer Science, TU/e. 2007-19

W. Pieters. *La Volonté Machinale: Understanding the Electronic Voting Controversy*. Faculty of Science, Mathematics and Computer Science, RU. 2008-01