Journal of Risk Research

ISSN: 1366-9877 (Print) 1466-4461 (Online) Journal homepage: http://www.tandfonline.com/loi/rjrr20

The role of expertise in risk communication: laypeople's and expert's perception of the millennium bug risk in The Netherlands

Jan M. Gutteling & MargÔt Kuttschreuter

To cite this article: Jan M. Gutteling & MargÔt Kuttschreuter (2002) The role of expertise in risk communication: laypeople's and expert's perception of the millennium bug risk in The Netherlands, Journal of Risk Research, 5:1, 35-47, DOI: 10.1080/13669870010029639

To link to this article: https://doi.org/10.1080/13669870010029639

Published online: 15 Apr 2011.

Journal of Risk Research **5** (1), 35–47 (2002)

The role of expertise in risk communication: laypeople's and expert's perception of the millennium bug risk in The Netherlands

JAN M. GUTTELING* AND MARGÔT KUTTSCHREUTER
University of Twente, Department of Communication Studies, The Netherlands

Abstract

This paper focuses on the discussion of the role of expertise in risk communication. It describes empirical data on the risks posed by the Millennium bug in 1999 in the Netherlands. The study systematically examined the risk perception of both general public and computer experts with respect to the Millennium bug, assessing a potential discrepancy between the layman's and the expert's judgement, as has been observed in other risk areas. Two surveys were fielded, the first aimed at a random sample of the Dutch population ($n = 253$), the second at a sample of computer experts ($n = 91$). Results indicated that respondents did not perceive the Millennium bug to be a major threat. However, laypeople worried more, did see the issue as more personally risky, and did think the level of public awareness was higher than experts did. Computer experts felt more capable of taking mitigating actions than laypeople, and were more convinced that these actions were adequate. The implications of these findings for the role of expertise in risk communication are discussed.

KEY WORDS: risk communication, risk perception, experts, laypeople, Millennium bug

1. Introduction

The present study focuses on the role of expertise in risk communication. In the early 1980s, risk management was mainly an activity of government and industry experts. When systems became more complex, and making socially acceptable risk decisions became a problem in most western countries, also due to an increased public opposition, experts were expected to be able to communicate with the public about risks (Otway, 1987). Nowadays, experts and the public are constant in dialogue on risk decisions.

Traditionally, the risk communication strategy of government agencies, private companies, and scientific experts was to provide rational information to increase the level of knowledge of the public. The underlying rationale of this strategy is that when people are given the 'facts', their 'irrational' opinion will change, and their subjective perceptions will begin to align with scientific judgments (Liu and Smith, 1990, p. 332). This perspective on risk communication has been named the 'technical view' as opposed to the 'democratic view' (Rowan, 1994). The technical view of risk communication comprises a one-way, expert-to-lay public information flow, based on the premise that

*Author to whom correspondence should be addressed: PO BOX 217, 7500 AE Enschede, the Netherlands.
e-mail: j.m.gutteling@wmw.utwente.nl

Journal of Risk Research
ISSN 1366-9877 print ISSN 1466-4461 online © 2002 Taylor & Francis Ltd
http://www.tandf.co.uk/journals
DOI: 10.1080/1366987001002963 9

the public needs accurate (i.e. technical, quantitative, or statistical) information and scientific expertise, as technicians do themselves. Public failure to agree with the expert's view is often attributed to a misunderstanding, which would be solved by providing the correct information or by persuasion.

Cvetkovich *et al.* (1989) indicated that the technical approach fails to be an adequate type of risk communication due to at least three faulty assumptions. The first fault is to assume that the public uses the same style of analytic thought as expert risk-communication sources to elaborate on risk messages. Consistently using a rationalistic communication strategy may enhance the public's doubts about the real risk magnitudes, by accentuating small probabilities but neglecting the potentially severe consequences. Quite a few studies have indicated problems in this respect (see for an overview: Gutteling and Wiegman, 1996). Not surprisingly, the international risk communication literature contains many accounts of the public's lack of confidence in sources of risk information using a rationalistic top-down approach (see e.g., Peters *et al.*, 1997).

The second fault is that this approach also wrongly assumes that many risks are apolitical. According to Kasperson (1986) often the simple transfer of risk information becomes a political issue about more fundamental risk questions. Elaborating on this notion, risk communication should be focusing on citizens' evaluations of these fundamental issues. Important factors here are the individual's values concerning the process in which judgments and decisions in society are made, and how fair risks and benefits are distributed over different groups in society. These factors are also central to the democratic perspective on risk communication (see Rowan, 1994), which is governed by rules that guarantee a just and fair process, in which all parties have maximum participation and decision-making power. In the democratic view, persuasion is out of the question, because the aim of risk communication should be mutual understanding and not the exertion of power. According to reactance theory (Brehm and Brehm, 1981), messages aimed at persuading the public to accept a particular point of view, can be a threat to this independence or curtail it, which increases reactance. Reactance will be greatest when the threatened independence is very important to the individual, and pressure is exerted on the receiver to accept a point of view, opposed to his own. This may well be the case when persuasion is attempted on a risk issue, in which people's safety, health, or well-being is at stake, making it extremely personally relevant. In these circumstances, people may maintain their initial views, or even change in the opposite direction. When this happens, fear may be increased instead of decreased, and trust may reverse in distrust.

Finally, the 'technical' approach makes the faulty assumption that the audience perceives reality in a similar fashion as the expert communicator. However, perceptions of the hazardous reality can be quite different between risk experts and laypersons. The first observations of experts' versus layperson's discrepancies in the perception of risks were reported in the early 1980s by Fischhoff *et al.* (1981a; 1981b) and subsequently addressed and analysed by others (e.g., Otway, 1987; Slovic, 1987; Kraus *et al.*, 1992; Wiegman *et al.*, 1995). The main purpose of these studies was to increase the understanding of the public perception of so-called 'low probability, high consequence' risks in various technology domains (e.g., nuclear energy and chemical industries). Important outcome of these studies, which are often described as reflecting the psychometric paradigm, was that the lay risk perception was best described by 'subjective'

determinants. In short, laypeople will worry most about risks when the perceived level of threat is high, the risk is unfamiliar, and people cannot control the risk themselves, and are exposed to the risk involuntary (see e.g., Slovic, 1987). So, laypeople are probably most interested in the personal consequences of the risk. On the other hand, experts' opinions are mainly based on 'objective', statistical, actuarial data, which focuses on societal, but not on individual consequences. Margolis (1996) refers to these two notions as the *rival rationalities view*. In contrast to the psychometric paradigm, scholars from the cultural theory have argued that layperson's opposition to expert advice about risks is based on larger concerns about how society is organized than about the relative dangers of certain activities (e.g., Kunreuther, 1997; Sjöberg, 2000 for a review of cultural theory).

The rival rationalities in risk perception may jeopardize the risk dialogue between experts and laypeople (Cvetkovich *et al.*, 1989). In particular when experts are working according to the technocratic approach, their risk information may be judged as too complex, irrelevant or just too dull for the layperson's liking. Sometimes experts are distrusted because some self interest is suspected or laypeople think experts may express a different value orientation. This is also related to what Margolis (1996) describes as the *Loss of trust*-theory, which states that risk communication problems are mainly due to the lack of trust laypeople have in scientific experts or scientific expertise, probably due to the perception that policies and notions of private and public institutions do not consider the concerns and the interests of the public.

1.1. The Millenium bug issue

Considering the opposing views on the role of experts and the determinants of the expert versus layperson discrepancy in risk perception as described above, a study was designed enabling assessment of several of the above mentioned indicators. It was assummed that the risks posed by the so-called Millennium bug in 1999 and the years before, would for several reasons be an excellent case study to focus on the role of expertise in risk communication.

The Millennium bug, also known as year 2000 or Y2K, shared many characteristics with other so-called 'low probability, high consequence' technology-related risks. In the last few years of the 20th century, computer experts confronted the public with the pessimistic idea that on 1 January 2000 the hardware and software of essential computer systems would behave unreliably and unpredictably, due to the Millennium bug. Because computer technology has become an essential part of the western industrialized world, this risk scenario was supposed to affect all sectors of society. The Millennium bug was foremost a serious economic issue, but many risk scenarios described potential cumulative health and safety consequences. Without proper mitigation, consequences of the Millennium bug were to be expected in the financial and business world, military and health care organizations, nuclear power plants, the chemical industry, the energy supply, transport sector, in small and medium sized businesses, and finally in peoples homes.

Risk communication about the Millennium bug was a distinct and co-ordinated activity in the Netherlands, and computer experts played an important role in the communication process. In the period in which this study was fielded, a campaign was directed at several business sectors of society with the ominous slogan 'we have to take care of the Millennium problem before it takes care of us', emphasizing the potentially

severe consequences. Although the general public was not the target group for this campaign, it included advertisements in the general press and public service announcements on popular television and radio stations. It may be expected that this type of communication is likely to increase perceptions of risk and worry among the general public.

1.2. Research questions

In this study, three questions are examined in relation to the role of expertise in risk communication. The first question was whether the Millennium bug issue could be characterized by *rival rationalities* in risk perception between laypeople and experts, as has been seen with respect to other technology related risk issues. Rival rationalities in Millennium bug risk perception may have hindered risk communication on this issue. The expectation was that in general the lay public, due to the dramatic framing, might see the Millennium bug as a serious risk, although it might be felt that the probability of occurrence of problems was small. Due to the involuntary exposure to the large-scale consequences of this risk, the public might have a high level of worry and perceived threat, and perhaps a low level of optimism about their own capabilities to cope with it. It was assumed that experts, who would not base their perception of the issue on a dramatic campaign, perceived the problem as less severe than the lay public.

The second question focused on the level of public trust in (computer) experts. A loss-of-trust in computer experts, for instance due to the perception that computer experts were responsible for the existence of the problem in the first place, would also jeopardize the risk communication effort. The third and final research question was directed at the attitudes of both experts and the general public toward matters as the perceived need for information (risk communication) and the attitude toward the computer technology.

2. Method

Two surveys were fielded end of March, early April 1999. A questionnaire was sent to a random sample of 1574 Dutch households, taken by the Dutch Postal Services. The first person of 18 years of age or older in the household having his or her birthday was invited to complete and return the questionnaire. An identical questionnaire was mailed to a sample of 328 persons working in Dutch Universities at Departments of Computer Science or at Computer Support departments. Using the X-500 directory, which was accessible though the Internet, a list was compiled of all personnel working in these departments. The sample was taken by selecting every fifth name on the list. After three weeks a simple reminder was sent to all addresses.

In total, 353 people returned questionnaires. Of these respondents, 91 who indicated to be employed in the Computer Business were considered to be experts, and 253 were categorized as laypersons. Table 1 contains the response characteristics for both experts and laypersons. Comparison of the respondents from the lay public with Dutch census data indicated that this group is not to be considered representative for the Dutch population with respect to distribution of gender and educational level. Our group of laypeople contains relatively many men and people with a higher educational level. Differences between laypeople and experts are as expected. The group of experts contained relatively many young males with on average a higher educational level.

Table 1. Characteristics of respondents in this study: laypersons and experts.

Characteristics	*'Laypersons'*	*'Experts'*
N =	253	91
Overall response	18%	28%
Gender and age		
% Male	63%	93%
Average age	48 years ranging from 21–83	38 years ranging 22–69
Educational level		
Lower	32%	2%
Middle	25%	10%
Higher	41%	88%
Computer experience at home		
Much	27%	70%
Not much	73%	30%
Computer experience at work		
Much	48%	99%
Not much	52%	1%

Furthermore, experts indicated to work more with computers at home and at work than laypersons. These data indicate that the two groups are in a sense representing existing differences in the 'natural' groups of laypeople and experts. The regional distribution of laypersons and experts is similar.

Response rates were low. So, generalizations from the data to both populations are to be made with extreme care. The number of respondents is adequate for comparative analysis between both groups.

2.1. Questionnaire

The questionnaire was an A4-booklet and contained 12 pages. The questionnaire comprised the usual demographics, and questions identifying computer literacy. Furthermore, the following variables were assessed

2.2. Risk perception and risk behaviour in six situations in which the Millennium bug might occur

The questionnaire comprised questions aimed at the perception of the Millennium risk in six different situations. These questions were primarily aimed at answering the first research question and were based primarily on the psychometric theory. The selection of situations, namely (1) the hospital, (2) financial matters, (3) retail trade, (4) transport, (5) in people's own home and (6) the energy supply, was based on a pilot study with laypeople. The pilot study indicated that the six situations differed with respect to the potential for personal injury (on 2 levels: little, much) and financial damage (on three levels: little, average, much). For each situation, first the probability of occurrence of negative consequences of the Millennium bug was assessed (on 5-point scales,

very high – very low). Next, the respondent was asked to rate eight statements with respect to the perception of the Millennium bug risk and about risk mitigating behaviour (on 5-point scales, agree – disagree). The statements are presented in Table 2. Risk perception was assessed with questions relating to the personal and societal risk of the Millennium bug, and the level of worry caused by the bug. Also the perceived level of public and expert knowledge of the consequences was measured. Risk mitigating behaviour was measured with questions relating to one's intention to take risk-mitigating actions, the self-efficacy and outcome expectancy of these behaviours. These concepts were taken from the attitude theory (e.g., Ajzen and Madden, 1986).

All variables measured on 5-point scales were aggregated over the six risk situations. The internal consistency of these summed variables is good: Cronbach's alpha > 0.80 (see table 2). For risk mitigation a summed variable was calculated indicating whether the respondents intended or not to take mitigating action. The internal consistency of this measure was acceptable (α=0.71).

Table 2. Wording of questions for risk perception and risk behaviour and internal consistency

	Concept	*Cronbach's alpha on six situations aggregated all respondents*
Risk perception related questions		
• The probability that the Millennium bug on January 1 2000 will have consequences in[1] is (very small–very high)	probability of occurrence	0.88
• The consequences of the Millennium bug in[1] are risky for society at large (disagree–agree)	societal risk	0.87
• The consequences of the Millennium bug in[1] are risky for me personally (disagree–agree)	personal risk	0.83
• The Millennium bug in[1] worries me (disagree–agree)	worry	0.87
• The exact consequences of the Millennium bug in[1] are sufficiently known to experts (disagree–agree)	assumed expert awareness	0.86
• The exact consequences of the Millennium bug in[1] are sufficiently known to the public (disagree–agree)	assumed public awareness	0.90
Risk behaviour related questions		
• I think I'm well capable of taking action against the Millennium bug in[1] (disagree–agree)	self-efficacy	0.82
• What I can do myself provides me with enough protection against the Millennium bug in[1] (disagree–agree)	outcome expectancy	0.81
• Do you intend to protect yourself against the possible consequences of the Millennium bug in[1] (disagree–agree)	behavioural intention	0.79

Note: 1. the hospital, the financial world, retail trade, the transport sector, in and around the house, and the energy sector, respectively. These alpha's differ only marginally from those calculated for 'laypersons'.

2.3. Attitude toward the Millennium bug

The respondent's attitude toward the Millennium bug was measured with 12 statements (5-point scales, agree – disagree). These questions were primarily designed to answer the second and the third research questions. The statements are presented in Table 3.

Factor analysis indicated that four factors could be extracted with an Eigenvalue greater than 1, which together explained 63% of the variance. The first factor comprised 5 items reflecting the trust in solutions to the problem (2 items) and the reliability of Millennium tests (3 items). This factor was labelled 'trust claims and organizations'. The second factor comprised 3 items relating to informing the public. This factor is described as 'more info needed for public'. The third factor comprised 2 items reflecting a critical attitude toward computer experts. This factor is described as 'computer people to blame'. The fourth and final factor also comprised 2 items and reflected the 'attitude toward computer technology'. For these factors aggregated scores were computed with satisfactory levels of internal consistency (see Table 3).

Table 3. Wording of questions relating to the attitude toward the Millennium bug, ordered according to the results of a factor analysis (all questions 5 point scales with extremes disagree–agree.

	Cronbach's alpha for all respondents
Trust claims and organizations • The Millennium bug will be solved in time • In our country enough is done to solve the Millennium bug • When a Millennium test indicates an organisation has solved the Millennium bug, this is true • It is safe to buy a new apparatus carrying the label 'Millennium proof' • Companies and organisations stating they are 'Millennium proof', are telling the truth	0.79
More information needed for public • Government agencies should provide the public with better information on the Millennium bug • The mass media do not give enough attention to the Millennium bug • Sometimes one thinks too lightly about the consequences of the Millennium bug	0.76
Computer people to blame • Computer experts should have prevented the Millennium bug • Computer experts do not consider possible computer problems sufficiently	0.71
Attitude toward computer technology • Nowadays, society can not exist without computers • Computer technology has brought us more benefits than risks	0.62

Note: These alpha's differ only marginally from those calculated for 'laypersons'.

3. Results

3.1. Risk perceptions, risk behaviour and risk attitudes on an aggregate level

Table 4 shows the results for the aggregated risk perceptions, as well as the behaviour related and the attitude dimensions toward the issue.

The average levels of risk perception were low, indicating respondents did not perceive the Millennium bug to be a major threat. Only the levels of assumed expert awareness of the Millennium bug were high for both groups. In answering the first research question, it is observe that overall, laypersons and computer experts expressed a different level of worry about the Millennium bug, the riskiness of personal consequences, and the assumed public awareness of the issue. Laypeople worried more, perceived the issue as more personally risky, and assessed the level of public awareness as higher than experts did. However, no differences were observed for the probability of occurrence of the Millennium bug, the perceived threat to society as a whole, and the assumed expert awareness of the issue.

In the behavioural domain, significant differences were observed between laypersons and experts for the self-efficacy and outcome-expectancy measures, but not for the intention to take preventive action. Computer experts felt more capable of taking mitigating actions than laypeople, and were also more convinced about the adequacy of these actions.

With respect to the attitude dimensions toward the Millennium issue, concerning research questions 2 and 3, the following observations can be made. Laypeople and computer experts seemed to agree that computer people themselves were to blame for

Table 4. Risk perception, risk behaviour and attitudes of 'laypersons' and 'experts' toward the Millennium bug issue on an aggregate level.

	'laypersons'	*'experts'*	*F*
Risk Perception related			
Probability of occurrence [2]	2.74	2.69	< 1
Societal risky [1]	3.02	2.80	3.13
Personal risky [1]	2.47	2.22	4.57 *
Worry [1]	2.56	2.22	7.20 **
Assumed expert awareness [1]	3.99	3.84	1.97
Assumed public awareness [1]	2.68	2.30	8.03 **
Risk Behaviour related			
Self-efficacy risk mitigation [1]	2.77	3.14	8.16 **
Outcome expectancy risk mitigation [1]	2.86	3.15	4.98 *
Behavioural intention to mitigate [3]	1.11	1.12	< 1
Attitude dimensions			
Trust claims and organisations? [1]	3.63	3.17	18.38 ***
More info needed for public? [1]	3.62	3.19	6.70**
Computer people to blame? [1]	3.53	3.26	2.70
Positive attitude toward technology? [1]	4.23	4.58	9.43**

Notes: * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

1. 5-point scale with 1 disagree, 5 agree. [2]5-point scales with 1 very small, 5 very high,[3] 1 no action intended, 2. action intended.

the existence of the Millennium problem. Laypeople expressed more trust in claims that machines or organizations were 'Millennium proof'. Experts were more reserved here. Compared to experts, laypeople were more convinced that government agencies should do more to inform the public about the Millennium risk. Both laypersons and experts expressed a very positive attitude toward computer technology, however, the experts were significantly more positive than the laypersons.

3.2. Six Millennium bug situations in more detail: risk perceptions and risk behaviour

For the risk perception and risk behaviour related concepts for which significant differences between laypersons and experts on the aggregated level were found, the six situations in which the Millennium bug could manifest itself were looked at in more detail. Table 5 summarizes the findings. In general, the risks the Millennium bug posed to the energy supply were perceived as most serious, both on a personal level and for society as a whole. Problems in this sector were not seen as easily solvable. Laypeople and experts alike felt not capable to take adequate mitigating action themselves, and expected possible actions to be inadequate. So, it is not surprising that people worried most about the Millennium issue regarding the energy sector.

A Millennium problem in hospitals was also a matter of worry for many, although respondents perceived it as less risky than the energy risks. Respondents did not feel capable of taking measures themselves. Personal measures were seen as inefficient as well. Almost 25% of the respondents estimated the probability of occurrence of problems in the energy sector or the hospital as large.

The transport sector was perceived as the most likely domain for the occurrence of a Millennium problem. The Millennium problem in this area was seen as not easily solvable, and perceived as risky for society as a whole. The personal consequences were perceived as less risky, possibly because people felt rather capable of taking adequate mitigating action.

Laypeople and computer experts disagreed most about the Millennium problem in their own homes. Although both laypeople and experts perceived this situation as least risky, the laypeople worried significantly more, assessed the personal risk as higher, and felt much less capable of coping with the risks themselves. Furthermore, laypeople expressed less faith in self-applied risk mitigation at home than experts.

The Millennium problem in the retail trade was not seen as very risky and only few people expressed worry about this risk. Although the occurrence of a Millennium

Table 5. Differences in risk perception between 'laypersons' and 'experts' with respect to six specific Millennium Bug risks.

	Hospital	*Financial*	*Retail trade*	*Transport*	*Own home*	*Energy supply*
Worry	ns	ns	ns	**	***	ns
Assumed public knowledge	*	*	*	***	*	ns
Personal risky	ns	ns	ns	ns	***	ns
Self efficacy	**	ns	*	ns	***	ns
Outcome expectancy	ns	ns	ns	ns	***	ns

Notes: * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

problem in the retail trade was seen as likely by more people than the previous risk, people felt more capable of taking effective mitigating action, e.g. by laying up sufficient amounts of food.

Both laypeople and experts perceived the Millennium issue in the financial sector as not very risky for them personally. So, this issue did not bring on many worries. People were confident to be able to take adequate measures, e.g. by withdrawing some extra cash from their bank accounts.

4. Discussion and conclusions

This study started with three questions, which were inspired by the discussion on the role of expertise in the risk communication literature.

The first question focuses on determining whether rival rationalities between experts and laypersons, that is a discrepancy in risk perception and intention to take risk mitigating action, existed with respect to the Millennium bug issue, some eight months before the bug would become active. Would similar discrepancies in risk perception of the Millennium bug exist between laypeople and experts, as we have seen with respect to other technology-related risk issues? Such a discrepancy may be a threat to the dialogue between experts and laypersons about this risk issue. The lay public was expected to perceive the Millennium bug as a serious risk, causing some worry and a feeling of threat due to the involuntary exposure to it, and a certain level of pessimism about one's own capabilities to cope with it. Although the absolute level of worry in the general public was hard to predict, it was assumed to be higher than that of computer experts. The results of this study indicated that indeed several differences in risk perception and behaviour related variables existed between laypeople and experts. Laypeople worried more, did see the issue as more personally risky, and did think the level of public awareness was higher than experts did. Computer experts felt more capable of taking mitigating actions than laypeople, and were more convinced that these actions were adequate. These differences were in the direction assumed; however, in absolute terms they were rather marginal because in general, the respondents did not perceive the Millennium bug to be a major threat. No differences between laypersons and computer experts were found with respect to the estimated probability of occurrence of the negative consequences of the Millennium bug, the assessed riskiness for society at large, and the assumed level of expert awareness of the problem. Additionally, laypersons and computer experts did not show a different level of intention to take risk-mitigating actions. These results lead to the conclusion that the rival rationalities perspective was only partly supported with respect to this risk issue in The Netherlands.

The second question addresses the level of trust the public expressed in (computer) experts. It finds its base in the Loss-of-trust theory, stating that the problems in risk communication are mainly due to the lack of trust laypeople have in scientific experts or scientific expertise. The study identified two factors which could be important for the further understanding of the loss-of-trust phenomenon: the trust expressed in 'safety claims' of machines and organizations, and the extent to which computer experts were held responsible for the existence of the Millennium bug in the first place. The results here were different from what those expected. Laypersons and computer experts alike blamed computer people for the problem, and remarkably, laypeople expressed more trust in Millennium proof claims of machines and organizations than computer

experts did. In the authors view, these findings cannot easily be explained from the loss-of-trust framework.

The third and final research question is directed at the attitudes of both experts and the general public toward the perceived need for information (risk communication) and the attitude toward the computer technology. On both variables, laypeople and experts expressed different preferences. Compared to experts, laypeople were more convinced that government agencies should do more to inform the public about the Millennium risk. This result seems to be in line with the somewhat higher level of worry of laypeople. Perhaps this is an indication that laypeople were convinced that risk communication could diminish the level of worry for a risk like the Millennium bug. Not surprisingly, computer experts had a significantly more positive attitude toward the computer technology than the laypersons. However, the attitude of laypersons was also very positive, indicating that this domain of technology is not disputed. Of course, many laypeople have experienced working with computers both in the own home or at work, which may have contributed to a sense of familiarity with these machines, reducing the levels of worry. So, from our data no fundamental dispute about the acceptability of computer technology risk was evident, which is clearly different from what has been reported with respect to other 'low probability, high consequence' risks.

Several explanations come to mind for the findings, which were rather different to what has been reported in earlier comparative 'laypeople versus expert' studies. These explanations focus on the characteristics of laypersons, experts, and the Millennium bug risk, respectively. A first explanation is that at the time of the study the Millennium issue was perhaps not salient enough to the general public. The low response rates found in this study may support this view. In line with this reasoning, it may well be that, due to the pro-active risk-mitigation and communication in the Netherlands, people were convinced that government and private sector were taking adequate and timely risk-mitigation measures, so no real Millennium danger was to be expected. Failure to demonstrate a loss of trust in computer experts supports this reasoning.

A second explanation is that the experts whose opinions were measured in this study were not the 'correct type' of experts. Perhaps the University-based experts were not fully aware of all problems in the Millennium practice, and were more likely – than perhaps those in the ICT-business who worked on a day-to-day basis solving Millennium bug problems – to base their opinions on this issue on the same information as the general public. This study does not allow an answer to this question with certainty; however, the sample of experts did comprise many people working in University Computer Support Departments, who were expected to be actively involved in solving Millennium bug risks on a regular basis. So, there is confidence that this particular explanation for the findings is not correct.

A third explanation is that the basic assumption, namely that the Millennium bug risk is comparable to other 'low probability, high consequences' risks, is incorrect. However, looking at the experts' risk scenarios and the compatibility of those scenarios with the factors that determine laypeople's risk perception (threat, involuntary exposure, severe and cumulative, partly unknown consequences), the authors are convinced that is not an unlikely assumption at all. On the other hand, the negative consequences of the Millennium bug risk were forecasted but never observed. In 1998 and 1999 people had not experienced any major disastrous 'computer accident' attributable to the Millennium bug. But the lack of disastrous accidents can be observed in other risks as

well, which are perceived as highly risky and controversial anyway. In the authors' view, there is only one very important distinction between the Millennium bug risk and other 'low probability, high consequence' risks: the Millennium bug is related to a domain of technology which is not disputed and where no fundamental societal or political debates exist about the technology's pros and cons. The data support this observation; both laypersons and computer experts had very positive attitudes toward the technology. It is assumed that societal debates on a particular technology highlight potential controversies of interest between stakeholders. In this process pros, but more likely cons may become more salient to the public. The pro-active approach of the Dutch government and the private sector might well have had the effect of 'covering up' emerging conflicts of interest.

This leads us to the final conclusion with respect to the discussion on expertise in risk communication. Although it is evident that the rival rationalities and loss-of-trust are important determinants of success or failure of risk communication dialogues, the study suggests that these factors will primarily be important when the risk domain itself is politically controversial. Future studies will have to look into more detail into the interrelationship of these determinants of the risk communication process.

References

Ajzen, I. and Madden, Th. J. (1986) Prediction of goal-directed behaviour: attitudes, intentions, and perceived behavioural control, *Journal of Experimental Social Psychology*, **22**, 453–74.

Brehm, S.S. and Brehm, J.W. (1981) *Psychological Reactance: A Theory of Freedom and Control*, New York: Academic Press.

Cvetkovich, G., Vlek, C.A.J. and Earle, T.C. (1989) Designing technological hazard information programs: Towards a model of risk-adaptive decision making, in C.A.J. Vlek and G. Cvetkovich (eds) *Social Decision Methodology for Technological Projects*, pp. 253–76. Dordrecht, the Netherlands, Kluwer Academic Publishers.

Fischhoff, B., Slovic, P. and Lichtenstein, S. (1981a) 'The public' vs. ' the experts': perceived vs. actual disagreement about risks, in H. Kunreuther (ed.) *Risk: A Seminar Series*, Laxenburg: IIASA.

Fischhoff, B., Slovic, P. and Lichtenstein, S. (1981b) Lay foibles and expert fables in judgements about risks, in T. O' Riordan and R. Kerry Turner (eds). *Progress in Resource Management and Environmental Planning* **3**, pp. 161–202. New York: John Wiley and Sons.

Gutteling, J.M., and Wiegman, O. (1996) *Exploring Risk Communication*, Dordrecht: Kluwer Academic.

Kasperson, R.E. (1986) Six propositions on public participation and their relevance for risk communication, *Risk Analysis* **6**, 275–81.

Kraus, N., Malmfors T., and Slovic, P. (1992). Intuitive toxicology: expert and lay judgments of chemical risks, *Risk Analysis* **12**(2), 215–32.

Kunreuther, H. (1997) Enviroment: dealing with risk: why the public and experts disagree on environmental issues, *Journal of Policy Analysis and Management* **16**(4), 654–58.

Liu, J.T. and Smith, V.K. (1990) Risk communication and attitude change: Taiwan's national debate over nuclear power, *Journal of Risk and Uncertainty* **3**, 331–49.

Margolis, H. (1996) *Dealing With Risk: Why the Public and the Experts Disagree on Environmental Issues*, Chicago: University of Chicago Press.

Otway, H. (1987) Experts, risk communication, and democracy, *Risk Analysis* **7**, 125–29.

Peters, R.G., Covello, V.T. and McCallum, D.B. (1997) The determinants of trust and credibility in environmental risk communication: an empirical study, *Risk analysis* **17**(1), 43–54.

Rowan, K.E. (1994) The technical and democratic approaches to risk situations: their appeal, limitations, and rhetorical alternative, *Argumentation* **8**, 391–409.
Sjöberg, L. (2000) Factors in risk perception, *Risk Analysis* **20**(1), 1–11.
Slovic, P. (1987) Perception of risk, *Science* **236**, 280–85.
Wiegman, O., Gutteling, J.M. and Cadet, B. (1995) Perception of nuclear energy and coal in France and the Netherlands, *Risk Analysis* **15**(4), 513–21.