The Vulnerability of Technological Culture*

Wiebe E. Bijker

The attacks on New York and Washington, 11 September 2001 ('9/11'), as well as other attacks since, have demonstrated how vulnerable our modern societies are.[1] These events shattered many people's basic feelings of security and safeness, though 9/11 probably did not radically change the view of scholars in science, technology, and society studies (STS). Work on this chapter started in response to 9/11, when several historians and sociologists of technology and science asked in what ways their research could be relevant to understand these events.[2] I will argue that it is worth to investigate the vulnerability of technological culture, and that this can be done fruitfully from an STS perspective. My main point, however, is different. I want to suggest that vulnerability is not to be taken as something purely negative. Living in a technological culture, I will argue, inevitably implies to live in a vulnerable world. And vulnerability is not only an inevitable characteristic; it is even an important asset of our technological culture as a prerequisite for living with the quest for innovation. To live in an open, changing and innovative culture, we must pay the price of vulnerability.

Vulnerability is a central issue when thinking about innovation. Joseph Schumpeter's recognition that the fundamental instability of capitalism presents an ever-present possibility of entrepreneurs' seizing upon innovations can be read as an early formulation of a positive relation. Vulnerability seems to be a *condition sine qua non* for innovation, as it is the inevitable result of the instability and dynamic development that Schumpeter identified as prerequisites for innovation (Schumpeter 1939). The relation has also been made *vice versa*: innovation makes vulnerable.

---

* This is a manuscript. See for final publication: Bijker, W. E. (2006). The Vulnerability of Technological Culture. *Cultures of Technology and the Quest for Innovation*. H. Nowotny. New York, Berghahn Books**:** 52-69.

Patent law, for example, is one way of coping with the financial vulnerability that results from the large investments required for innovation.

In this chapter I want to explore the vulnerability of technological culture: a vulnerability that is at the same time an inevitable consequence of, and a necessary prerequisite for, the advanced technological society in which we live. To do so, I shall first specify what it means to investigate technological *culture* in addition to analysing technological *systems* and high-tech *society*, and then continue with an analysis the concept of vulnerability applied to, respectively, systems, society, and culture.

Studying Technological Culture

As Helga Nowotny observes in her Introduction, "to approach technology under a cultural perspective is (…) both self-evident and highly demanding."[3] Such an approach is self-evident, because "technology is perceived as the most consequential cultural practice that humankind has developed;" and it is demanding, because "the risks associated with technologies have revealed themselves to be a cultural phenomenon as well." To analyse the various types of vulnerability of technological systems and societies, it is thus necessary to use a cultural perspective; it is necessary to analyse technological culture.

This focus on technological culture is part of a more general trend in STS. In the 1970's and 1980's the focus was on case studies of scientific controversies and on technological artefacts and systems. In the 1990's, this agenda broadened to also address social, political, and cultural issues of societal relevance (Bowker and Star 1999, Edwards 1996, Hecht 1998). Accordingly, the empirical base was broadened as well: the attention to science was extended to a variety of belief systems such as indigenous knowledge (Verran 2001, Watson-Verran and Turnbull 1995), and knowledge developed by patient groups (Epstein 1996); the attention to technology was extended to social technologies, and to technologies' users (Oudshoorn and Pinch 2003). The STS research agenda now also includes such issues as democratisation, (scientific) expertise, politics of genomics, and the relation between economic development and technological knowledge (Callon et al. 2001, Wilde et al. 2002, Bal et al. 2002, Gottweis 1998, Mokyr 2002). In other words, developments in the last decade have shown a shift from the study of the (local) cultures of science and technology to the study of technological culture at large.

Why use the phrase 'technological culture'? One reason is to highlight the pervasiveness of science and technology in modern, highly developed societies. As John Law and I summarized in 1992:"All relations should be seen as both social and technical (…). Purely social relations are found only in the imaginations of sociologists, among baboons, or possibly, just possibly, on nudist beaches; and purely technical relations are found only in the wilder reaches of science fiction." (Law and Bijker 1992: 290). To conceptualise society as a combination of merely social systems and technological systems, does not adequately recognise this pervasiveness. To take, in contrast, 'technological culture' as the key focus of research helps to recognize "the basic, underlying assumption that modern societies are predominantly shaped by knowledge and technology".[4] Studying technological culture, then, means to study technologies and societies from a cultural perspective: the unit of analysis is a technological system or a (part of) modern, technology dominated society, and these are studied with specific attention to the cultural dimensions. A focus on technological culture highlights how social interaction is mediated through technologies, and how technologies can only function when embedded in societal institutions.

This usage of the term 'technological culture' is thus broader and more ambitious than the way it is used in the context of public understanding of science: there it is synonymous with 'technical literacy' and often connected to economic development and innovation.[5] The term 'technological culture' in its broader sense is in line with Manuel Castells' move to extend the analysis of the network society to an analysis of identity, democracy, power, and international relations (Castells 1996 (2000), Castells 1997, Castells 1998 (2000)). It is equally in line with recent work in philosophy that recognizes "that the characteristic traits of our culture are pervasively and irrevocably technological", and that all current public debates "involve perceptions of technology in its widest and most comprehensive sense, which is to say *technology as our culture*".[6]

I will now review in more detail what it means to study the vulnerability of technological systems and high-tech societies from a cultural perspective, and then summarize these findings by discussing the vulnerability of technological culture.

Vulnerable systems

Technological systems can be vulnerable, as is abundantly clear from a long list of accidents and accompanying scholarly treatises (Schlager 1994). Charles Perrow argued already in 1984 that in modern societies, with their large, complex, and tightly coupled technological systems, accidents are 'normal' (Perrow 1999 (1984)). Recent STS literature covers, for example, the Challenger disaster (Vaughan 1996), the Bhopal chemical plant explosion (Fortun 2001), aviation accidents (Wackers and Kørte 2003, Snook 2000, Rochlin 1991, La Porte 1988), and nuclear accidents (Rochlin 1994).

The common meaning of vulnerable is 'sensitive to being hurt or wounded,' and often it is applied to ecosystems or living beings. Associated connotations are: defenceless, unprepared, weak, and naked. Vulnerable, then, seems to describe an intrinsic characteristic of a being or system, quite independently of the system's concrete context. It is more fruitful, however, to analyse vulnerability as a relational concept. Writing about natural hazards, Piers Blaikie et al. offer a relational and active definition of vulnerability: the reduced "capacity to anticipate, cope with, resist, and recover from the impact of a natural hazard." (Blaikie et al. 1994: 9). Sometimes associated to this active meaning is also a more positive connotation of being vulnerable: lowering your defences, exposing your weak spots, showing your Achilles heel—which can be an expression of strength and superiority rather than weakness. In this section I will investigate these aspects—relational, active, and partly positive—by further developing the concept of vulnerability in connection to technical systems. I will do so in four steps.

Analysing the vulnerability of technical systems, Ger Wackers and Jens Kørte unpack this reduced capacity to anticipate, cope with, resist, and recover from threats, and they translate it into a reduced capability to maintain functional integration. Without such functional integrity, systems stop working; loss of functional integrity for living beings means death (Wackers and Kørte 2003). This amounts to my first step towards specifying vulnerability. With this concept of (the loss of) functional integration, Wackers and Kørte analyse the vulnerability of an offshore helicopter transport system. They show how the helicopter system *drifted* (i.e. imperceptibly changed) towards a more vulnerable state in which various elements worked at a sub-optimal level and in which seemingly practical adaptations of the prescribed protocols

resulted in an increased vulnerability of the system. The concept 'drift' has been used by a variety of authors, but Wackers and Kørte particularly draw on Scott Snook's analysis of the 1991 shoot-down of two UN peacekeeping helicopters, full of officials, in northern Irak, by two US fighters (Snook 2000). Snook describes how a 'practical drift' of local adaptations and procedures led to a steadily widening gap between the safety regulations and the practical operations of fighters, helicopters, and AWACS controllers. Individually these adaptations were inconsequential, but over a longer period this practical drift had resulted in a vulnerable system—the system had lost some of its functionality because the various sub-systems did not collaborate and integrate as they were intended to.

What exactly could we mean with the term 'vulnerable system'? Charles Perrow's analysis of normal accidents in large (technical) systems is the classic starting point to answer that question. Perrow's diagnosis is that large technical systems are more risky, and tend to run into more catastrophic accidents, when they are more complex and more tightly coupled. Complex systems—in contrast to linear systems—have many interconnected subsystems, with many feedback loops, and multiple and interacting controls. Examples are universities and nuclear plants. Tightly coupled—in contrast to loosely coupled—systems do not allow for delays in processing, follow one invariant sequence of processing steps, have little slack in supplies and personnel, and have few and built-in buffers and redundancies. Examples are hydropower dams and nuclear plants. Aircraft systems and nuclear plants are complex *and* tightly coupled systems. Using Perrow's analysis it is now possible to make a second step towards specifying the vulnerability of systems. A tightly coupled complex system is more vulnerable in two ways: (1) it is more risky in Perrow's sense of failing due to some internal component errors, and (2) it is less capable to anticipate, cope with, and recover from the impact of external disturbances which do not fit its pre-conceived lines of reaction. In other words, a loosely coupled system is less vulnerable in both senses because there is less chance that internal errors will proliferate through the system, and because there is more opportunity (in the form of buffers, time, and extra redundancies) to react to external disturbances. And a linear system can be more easily protected—and thus made less vulnerable—because it typically is spatially segregated, allows for easy substitutions of sub-systems and

components, has single purpose controls and few feedback loops, and often is better understood.

The work by Perrow, Snook, Wackers and Kørte shows how crucial it is to analyse these events at a combination of individual, group, and systems levels. Diane Vaughan adds—and that is my third step—group culture and organisational culture to those perspectives. She recognizes the Challenger disaster as a normal accident, but "this case extends Perrow's notion of system to include aspects of both environment and organisation that affect the risk assessment process and decision making." Technical experts' interpretation "of the signals is subject to errors shaped by a still-wider system that includes history, competition, scarcity, bureaucratic procedures, power, rules and norms, hierarchy, culture, and patterns of information" (Vaughan 1996: 415). Perrow criticizes, in his afterword to the 1999 publication of his 1984 book, Vaughan's focus on work group culture and safety, because she "ask[s] how we can make risky systems with catastrophic potential more safe, a question that takes for granted that they must run hotter, be bigger, be more toxic, and make super demands upon members." In addition, Perrow wants to raise the issue of power, and "the role of production pressures in increasingly privatised and deregulated systems that can evade scrutiny and accountability." (Perrow 1999 (1984): 379) I agree with Perrow's foregrounding of political choice about specific technologies and about ways of organising society, but I think he misses the key point of Vaughan's cultural analysis. Vaughan's analysis does not dismiss, I think, the importance of issues of politics and power, but it casts them in a different light.

This will form my fourth step in developing the concept of systems' vulnerability: Diane Vaughan links her cultural analysis explicitly to the social constructivist notion of interpretative flexibility (Bijker 1995b): "The ambiguity of the engineering craft is complicated by 'interpretative flexibility.' Not only do various tests of the same phenomenon produce differing results, but also the findings of a single test are open to more than one interpretation" (Vaughan 1996: 202). And "even the same results could be interpreted differently. Sometimes disagreements between the two communities were hard to settle because, as one long-time Marshall S&E representative put it, contractor working engineers tended to be 'defensive about their design' because they believed in their own methods and analysis." (Vaughan 1996: 87) The implication of this insight is that the vulnerability of systems cannot be

characterised in objective, context-independent terms. Vulnerability, I want to argue, is socially constructed as much as facts and artefacts are (Pinch and Bijker 1984).

To elaborate this argument, it is helpful to first consider the related concept of *risk*. The vulnerability of systems, and particularly the vulnerability due to possible internal errors and failures, can to some extent be described in terms of risks. The Health Council of the Netherlands defines risk as "the possibility (with some degree of probability) that damage (with a specific character and size) will occur to health, ecology, or goods." (Gezondheidsraad 1995: 14) (my translation). This is a deliberately broad definition, allowing for a variety of forms of damage: varying, for example, in character, magnitude, timing, and possibility to recover. It is broader than the definition that forms the basis for probabilistic risk analysis: the probability of a (damaging) event multiplied by its magnitude. The broadness of the Health Council's definition implies a form of risk analysis and management that recognizes that "risk is more than a number"—the title of another Health Council report (Gezondheidsraad 1996). This latter report recognises that risks are the consequences of human action, whether we consider nuclear energy production, chemical plants, air travelling, living below sea level, or smoking. Such human action is always aimed at some kind of profit or benefit. It is therefore necessary to assess risks and benefits within one framework: risks cannot be evaluated without also evaluating the positive effects of the actions that generate them. Additionally, the Health Council concludes that risk problems may vary fundamentally, depending on: the extent of the risk over time; its extent through space; the uncertainty about its extent, character and magnitude; and the societal relevance of the risk inducing action. All these considerations lead to the conclusion that the often-used distinction between objective risk and risk perception does not hold. Risks cannot be conceptualised as an objective, quantifiable, context-independent phenomenon; and it makes no sense either to talk of the perception of such objective risks (Asselt 2000).

Now I can specify the relation between vulnerability and risk. Vulnerability refers to a system's *condition*—to its ability to anticipate, resist, cope with, and possibly recover from events that could reduce the systems functional integrity. Risk, on the other hand, is an outcome-oriented notion. It conceptualises the *effects* of a possible, harmful event. Vulnerability, by itself, is not related to any other outcome than the breakdown of the system itself. A vulnerable system may yield certain risks,

when it could produce damage, depending on the circumstances. A risk analysis can, *vice versa,* be helpful in assessing a system's vulnerability: analysing the chances (and resulting damage) of sub-system or component failure may help to get to grips with at least the technical aspects of a system's vulnerability.

Let us now finish the fourth step—the constructivist turn—in developing a concept of vulnerability. The first move was Vaughan's recognition of the interpretative flexibility of claims about a system's characteristics and performance. The second move was to recognize that even risks are 'more than numbers', and indeed context and culture dependent. To complete this constructivist turn with a third move, I will draw on John Law's paper about the London Ladbroke Grove train disaster (Law 2003). In this tragic accident, in which 31 people died and 414 were injured, a three-carriage diesel train unit and a high speed train collided at Ladbroke Grove, two miles outside Paddington Station, on 5th October 1999. Using an actor-network analysis, Law produces a detailed description of the relevant system, including the train units, the signalling, the drivers' training programmes, the industry management, and the safety regulations and technologies. Law's analysis tells us how all elements of the network—people as well as technologies—were geared towards maintaining and improving safety. But he also shows how small changes in standard arrangements cumulatively may have 'drifted' to this disaster. There is a crucial difference, however, between Snook's handling of the concept of practical drift and Law's conclusion about the role of small disorders that led to the Ladbroke Grove disaster.

Law highlights that "the partial disorder of these not very coherent arrangements does just fine a good deal if not all of the time. (…) For every case of a Ladbroke Grove there are endless 'system breakdowns' that have no serious consequences." He shows, with detailed analysis of the use of the Driver Reminder Appliance (DRA) on the diesel train (which I cannot reproduce here), that the same measurement that strengthens the system and makes it less vulnerable in one set of circumstances, does exactly the opposite under other circumstances and then enhances the system's vulnerability. So, these measurements, technical devices, and regulations show interpretative flexibility: in one condition they improve safety, in another they increase vulnerability.

Even more crucial for my constructivist conception of vulnerability, Law argues, "there are endless system failures that help to keep the wheels turning." Law's argument here is an argument about imperfection: about its unavoidability, and about the advantages of practising imperfection. That is how complex systems have developed over time: practices and routines have developed in safety-critical contexts because they proved workable, and they thus yielded a relatively stable and invulnerable system. And some of these practices are incoherent, unruly, against narrowly interpreted safety regulations. Such unruly practices are the lubricant to keep a system going, to make a system less vulnerable by better coping with potential hazards. The conclusion, then, can only be that vulnerability is socially constructed: the same system can be deemed relatively invulnerable—when unruly behavior is interpreted as people taking their responsibility, using their experience, improvising to accommodate to changing conditions; or it is deemed vulnerable—when such unruliness is defined as violating the regulations and creating risky situations.

Let me summarize my cultural analysis of the vulnerability of technological systems. The vulnerability of a technological system describes the weakness of that system's capacity to maintain functional integrity. System vulnerability is linked to the performance of sub-systems, system components, and to routines and working practices. Hence, risk analysis on component level can be helpful to assess a system's vulnerability. Practical drift may lead a system gradually to more vulnerable states, without the practitioners noticing in time. Vulnerability is a constructivist concept in the sense that it does not describe a context-independent and intrinsic quality of the system. Like the sociology of knowledge has shown for scientific statements, also vulnerability will be contested when it is at the forefront of debate, controversy, or research. This is not to say that all is merely 'in the eye of the beholder', or that there is no real base to vulnerability. Let me adapt the following metaphor, used the Harry Collins to illustrate the constructed nature of scientific knowledge: vulnerability and system are like map and landscape—vulnerability does relate to the reality of the system, but is not fully determined by it.[7]

Vulnerable societies

Technical systems function in societies. Modern, high-tech societies are indeed built on, with, around, and in technological systems. Any failure of those technical systems,

therefore, would directly impinge upon society. Vulnerable technical systems lead to a vulnerable technical society. The concept of vulnerability, as developed in the previous section, is fully applicable to societies—from its focus on functional integrity to its constructed nature.

When we describe our societies as vulnerable for a terrorist attack, we mean that there is a chance that such an attack will cause key institutions of society to stop functioning and the social fabric of society to disintegrate. In this diagnosis of vulnerability, technology plays a key role. The western societies are more vulnerable, *because* they are high-tech societies. It is exactly because such key institutions as energy distribution, communication, transportation, and trade are so complex and tightly coupled, that a high-tech society built around those institutions is so vulnerable. Most of these technological systems and social institutions have existed in some form already for a long time, but the complex and coupled character is new. As Perrow observes: "Odysseus' vessel neither polluted the Mediterranean shoreline nor could destroy much of Texas City; the World War II bombers could not crash into a building holding nuclear weapons (…); chemical plants were not as large, as close to communities, or processing such explosive and toxic chemicals; airliners were not as big, numerous, or proximate to such large communities; and it is only recently that the risk of radiation from a nuclear plant accident has been visited upon almost every densely populated section of our country." (Perrow 1999 (1984): 307) Damage may come from within or from outside the technical systems; damage may come in the form of technical errors and accidents, or in the form of social disruptions—but in all cases the complex and tightly coupled character of high-tech institutions potentially increases the devastating effect of the damage.

But the opposite is also true. Western societies have never been so well defended against natural disasters as with the current dike systems and earthquake proof buildings. Surveillance technology, intelligence, information systems, and biometrical technologies for person identification defend the USA against intruders. Modern medical technologies have increased public health to unprecedented levels. Our western societies are less vulnerable because of the technical systems that are employed. This seemingly contradictory diagnosis—that technology makes modern societies more vulnerable, while at the same time making societies more safe—would of course only be a problem for an essentialist concept of vulnerability: a society is

'really' vulnerable to some degree. The constructivist concept of vulnerability that I proposed in the previous section recognizes that a society can be constructed by certain actors, with certain aims, and under certain conditions, into being vulnerable; while the same society can be argued to be relatively invulnerable in another context or from another perspective.

Some of the recent work on vulnerability, often spurred by the terrorists' attacks, does mirror this dual character of technological societies. Apart from the recent attention to help citizens prepare themselves against terrorist attacks, much of the vulnerability related discussions and activities have focused on infrastructure (Blaikie et al. 1994) (Branscomb 2002). Often this was in the context of natural disasters such as floods and earthquakes. Recently the infrastructure of the Internet increasingly receives attention, and in all these different senses: as a potentially vulnerable infrastructure of modern society, as an infrastructure that can strengthen society's capacity to react to threats, and even as an infrastructure that can be turned into a weapon for attacks on society.[8]

To connect the notion of vulnerability with the survival of nations is of course something that has been done frequently since 9/11, and especially in the USA. Significantly, the word 'vulnerable' is hardly ever used in the documents and websites of the new US Department of Homeland Security, but it arguably is the most central concept behind this office's actions and policies. Vulnerability to 'biological, chemical, and radiation threats, and explosions and nuclear blasts' is cited as the main reason to 'be ready', 'be informed', 'make a plan', and 'make a kit of emergency supplies'.[9] Of course, among specialists (but now I am referring to army and weapon specialists rather than STS scholars) "the vulnerabilities in the United States to attacks by international terrorist or domestic groups or by such groups with domestic-international linkages" had been recognised long before (Sloan 1995:5). The emphasis was on nuclear, chemical, and biological weapons: "The proliferation of nuclear weapons and associated technologies, and the diffusion of knowledge needed to manufacture chemical and biological weapons, raises the fearful specter of mass destruction that makes concerns related to use of anthrax as a way of spreading both disease and panic pale to insignificance. The scary truth is that the United States is all too vulnerable to this kind of attack. (…) Highly symbolic targets like government buildings and corporate headquarters will be more vulnerable to attack." (Sloan

1995:7) These accounts, comments, and policies exemplify the constructed nature of vulnerability: they create one particular form of vulnerability, linked to one particular identity of the American society. Other American societies exist, and other accounts of vulnerability and resilience can be constructed accordingly, as I will show below.

Thus the concept of vulnerability as it was developed above is also applicable to societies. It may need some extension however. There are some issues that play a role when discussing the vulnerability of society, which are not prominent in discussing technological systems. The Netherlands Health Council explicitly concludes from its diagnosis that risk is more than a number: "Questions of risk management are questions about the configuration of society. Opinions about the vulnerability of nature, about the care for future generations, and about the freedom to act—they all shape the answers to these questions." (Gezondheidsraad 1996: 20) These are issues that relate to the core cultural values of a society. Perrow also notes the difficulty to handle such questions with the quantifying mathematical risk models that dominate the field of probabilistic risk analysis: this "is a narrow field, cramped by the monetarization of social good. Everything can be bought; if it cannot be bought it does not enter the sophisticated calculations. A life is worth roughly $300,000 (…); less if you are over sixty, even less if you are otherwise enfeebled." (Perrow 1999 (1984): 308)

A second element needs to be added to complete this section on vulnerable societies. This second element concerns the role of science. In his analysis of modern society as a 'risk society', Ulrich Beck identified the crucially new role that science plays in the vulnerability of modern high-tech societies (although he does not use the word 'vulnerable'): "If we were previously concerned with *externally* caused dangers (from the gods or nature), the historically novel quality of today's risks derives from *internal decision*. They depend on a simultaneously *scientific and social construction*. Science is *one of the causes, the medium of definition, and the source of solutions* to risks". (Beck 1992: 155) (italics in original). Beck's analysis gives an important reflexive twist to the conception of vulnerability as I developed sofar. The vulnerability of society is not merely a result from the growth of technological systems in number, size, complexity and tightly coupled nature, as Perrow would have it. Beck conceives the risks, accidents, and—I would add—vulnerability of modern society, as the inevitable result of the modernization process itself. The result of this

process is that the old industrial society is being replaced by a new risk society, Beck argues, in which social conflicts are less about the distribution of wealth but rather about the distribution of risks.

The Vulnerability of Technological Culture

In the previous sections I have reviewed various conceptions of vulnerability, when applied to technical systems and to societies, and I have done so from a cultural perspective. Let me now take stock of what this analysis has given us, by focusing on technological culture itself. As mentioned previously, my conception of technological culture is meant to highlight, that characteristic traits of our culture are pervasively and irrevocably technological; that our technologies are thoroughly cultural; that we can only understand our modern, high-tech society by recognizing how its dominant cultural values and its technology shape each other. A study of technological culture complements an analysis of technological society, because such a study focuses on the cultural values, identities, and practices that underpin the social institutions in these societies.

Vulnerability depends, ultimately, on values. The crudest example is a culture that does not value human lives—such a culture would be much less vulnerable to risks that may cause casualties, or to terrorist attacks that aim at killing people. Cultural values vary widely over historical time and across geographical space. The experience and the concept of vulnerability vary accordingly. It is trivial to note that over the past century an increase in hygienic conditions has decreased the human vulnerability to diseases, in the rich world; it is equally trivial to observe that the vulnerability of individual humans is very different depending on where you live. Social, economic, and health conditions are so different in Africa, as compared to richer parts of the world, that vulnerability must have a completely different meaning there. As legal philosopher Judith Shklar argues: “what is regarded as controllable and social, is often a matter of technology and of ideology or interpretation. The perceptions of victims and of those who, however remotely, might be victimizers, tend to be quite different.” (Shklar 1990: 1) Shklar builds her analysis of vulnerability and victimhood, of misfortune and injustice, on the observation that “the difference between misfortune and injustice frequently involves our willingness and our capacity

to act or not to act on behalf of the victims, to blame or to absolve, to help, mitigate, and compensate, or to just turn away." (Shklar 1990: 2)

Differences in vulnerability between various geographic regions may also be caused by political circumstances and power relations. For example, both Palestinians and Israelis feel vulnerable, but the character of their experience of vulnerability seems to be quite different. In a paper for the summit of ACP[10] Heads of State, Fei Tevi extends vulnerability to the economic and social, and wants to "define vulnerability with regards to the environment, the economy and the society in the Pacific region."[11] The basis for this extension was laid at the UNCED Conference of 1992 in Rio de Janeiro, when "the small island developing states were recognised as a special case for environment and development under Agenda 21 because of their vulnerability, fragility, small size, geographic dispersion and isolation."[12] To recognise this vulnerability is simply a matter of survival, Tevi argues. Using Wackers' and Kørte's concepts, we can now specify this 'survival': it is aimed at maintaining functional integrity as a community, as an economy, and as a people. Survival and vulnerability thus relate here to sustainability—sustainability in terms of energy and material cycles, and in terms of existential security.

The historical variability of vulnerability, as well as vulnerability being value-laden, is nicely illustrated by discussion about what should be listed as cultural heritage that needs protection. For example, the historical value of fortifications from World War II, that were built by the German occupation army in the Netherlands, were declared cultural heritage. Such a decision preserved these buildings by declaring them vulnerable and worthy of protection—although concrete fortifications are normally not thought of as being vulnerable.

The risk of epidemics like SARS can be explained in Perrow's terms, but the urgent sense of vulnerability it created in 2003 can only be described by referring to a dominant idea of complete health that exists in our technological culture. A SARS epidemic certainly can be analysed as a complex system with elements such as the selling and handling of livestock (chicken, civet cats) for consumption on crowded market places; the slaughtering of the animals in homes with subsequent exposure of humans to blood and entrails; increasing likelihood of new viruses emerging through recombination of chicken viruses and human influenza viruses; and the increased mobility of human bodies through a few hub airports (Singapore, Hong Kong). The

public impact of the 2003 SARS epidemic—also in countries in the western world where few casualties occurred—did, however, not result from citizens doing such a risk analysis. The epidemic had such an impact and created such an acute sense of vulnerability, because many in the richer parts of the world thought that infectious diseases were banned or confined to specific groups of people and types of behaviour (as in the case of AIDS).

If vulnerability is an inevitable characteristic of technological culture, as I think it is, how then do technological cultures handle this vulnerability? Surely all engineering routines, scientific methods, and managerial strategies, which we reviewed in the context of technical systems and societies, play a role. But what can be identified at the level of technological culture? I think that the precautionary approach is at least a partial answer to this question. With a precautionary approach, technological cultures can find ways to live with their vulnerability without necessarily violating their fundamental values.

The probably most cited version of the precautionary principle is the one in the Rio declaration: "Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation". (U. Nations 1992) This implies a shift from prevention of clear and manifest dangers towards precautionary action to avoid hypothetical risks: this principle allows interfering, even when it is not clear what the risk exactly is. A wealth of literature has developed since, that translates this principle in various precautionary approaches (Klinke and Renn 2002, EEA 2001). What is important for my purposes here is that some versions of a precautionary approach not only propose ways of handling risks, but also explicitly cite core values of modern technological cultures. For example, Sue Mayer and Andy Stirling argue that their approach "acknowledges the *complexity* and *variability* of the real world and embodies a certain *humility* about scientific procedures and knowledge." (Mayer and Stirling 2002: 60) (italics in original)

These values will not necessarily be the same in all proclaimed precautionary approaches, nor will the implementation of specific values be uncontroversial and without costs. Henk van den Belt and Bart Gremmen cite Aaron Wildavski (1995), when they warn "against the illusionary belief that by adhering to the Precautionary Principle something valuable, to wit human or environmental health, could be got at

virtually no cost whatsoever, the facile assumption being that the proposed bans and regulations themselves would have no adverse health effects." (Belt and Gremmen 2002: 107) The interpretation and implementation of the precautionary principle inevitably will vary, according to the legal and scientific doctrines, and to the openness of the political culture.

Thus the particular implementation of the precautionary principle allows shaping a technological culture in a specific way. It also connects back to my opening remarks, in which I connected vulnerability to innovation. Implementing the precautionary principle forms a battleground for stimulating or restricting innovation. Critics of the precautionary principle are afraid that it will curtail innovation. "The reason is that it leads its protagonists to focus mainly on the possibility that new technologies may pose theoretical risks, always hedging against the worst possible outcomes by assuming worst case scenarios, while ignoring the potential benefits of these same technologies or the real existing risks that could be mitigated or eliminated by them." (Belt and Gremmen 2002: 106-107) The report by the European Environment Agency in which twelve cases of the use of the precautionary principle were reviewed, also links precaution to the recognition that we live in a changing world while having limited knowledge: "a key element in a precautionary approach to regulation involves a greater willingness to acknowledge the possibility of surprise. This does not mean resorting to blanket opposition to innovation." (EEA 2001:169)

A final way of tracing the meaning of vulnerability is to ask what would be its opposite. Countering vulnerability may be phrased as aiming at 'safeness' or 'security.' Clearly, the choice of words when formulating the goal of offering an alternative to the vulnerability of society is not innocent: safe society, secure society, guarded society, or resilient society—these terms yield different values and political strategies. Conceptions of vulnerability fall in two classes, depending on whether their opposite has a connotation of *control* (such as in security) or *flexibility* (such as in resilience). Examples of control-oriented reaction to vulnerability are stricter immigration rules, and administration and control technologies that have been installed in the US recently.[13] As various organizations have argued, on the long run this may hamper the development of knowledge and cross-cultural understanding among different international communities—and thus possibly increasing the vulnerability of the US in the sense of not being able to react flexibly to threats.[14]

An example of flexibility-oriented defense against vulnerability is to maintain of a variety of crops and means of living, rather than to concentrate on one economic activity. Imagine a village at Lake Victoria in Africa, where developmental aid has improved fishing technologies that offer increased control to the fishermen because, for example, they are less vulnerable to bad weather conditions. An unintended consequence, then, may be that farming activities become relatively less profitable, thus inducing people to abandon the traditional mix of economic activities. This then would make the village less flexible in reacting to changes in world market prices for fish and crops—making the village more vulnerable in that other sense.

The European Environmental Agency also links its discussion of the precautionary principle to flexibility. It recognizes that our technological cultures are in a state of 'societal ignorance' on many important issues that relate to technological and scientific developments. This societal ignorance is contrasted to 'institutional ignorance'—referring to a situation where information relevant to a decision is extant in society, but not available to the decision makers—which can be remedied by provisions for more effective communication and social learning. The "condition of societal ignorance is more intractable. This problem (…) requires rather different remedies, involving scientific research and the fostering of greater diversity, adaptability and flexibility in decision-making and technological choices." (EEA 2001: 171)

Not only vulnerability in the form of the occurrence of technological accidents and natural disasters, but also the associated experiences of misfortune or injustice are inextricably linked to the accomplishments of our technological culture: "Our technological expectations are often too high, but given what the last two generations have accomplished, we suspect wrongful indifference or injustice when there is no one to protect us against the still-untamed forces of nature. In fact, it is not the fault of scientists or public officials that little can now be done, nor are they culpably indifferent to the current epidemic. Victims, however, seem to find it easier to bear their misfortune if they can see injustice as well as bad luck." (Shklar 1990: 65) With a focus on vulnerability of technological culture we do not only study the fragile constitution of modern societies, but can also capture the fragility that is constitutive of our technological culture and thus of its core structures and values.

Rather than treating vulnerability as something to be avoided, repaired, and fought—as something that is an implicit and unquestioned starting point of action as in the case of the current US policies I mentioned previously—I propose to treat vulnerability with the intellectual respect it deserves.[15] Whatever the current general obsession with safety and security may be, we will never be in a state of complete invulnerability. Indeed, I would not wish to live in such a society. Studying the vulnerability of technological culture may thus help us to understand our current highly developed societies.

References

J. Arquilla, D. F. Ronfeldt and U. S. Department of Defense, *Networks and netwars : the future of terror, crime, and militancy (*Santa Monica, CA, 2001).

M. B. A. v. Asselt, *Perspectives on Uncertainty and Risk. The PRIMA Approach to Decision Support (*Dordrecht, 2000).

R. Bal, W. E. Bijker and R. Hendriks, *Paradox van wetenschappelijk gezag. Over de maatschappelijke invloed van adviezen van de Gezondheidsraad, 1985-2001 (*Den Haag, 2002).

U. Beck, *Risk society: towards a new modernity.*, 1992).

H. v. d. Belt and B. Gremmen, "Between Precautionary Principle and 'Sound Science': Distributing The Burdens of Proof," *Journal of Agricultural and Environmental Ethics* 15 (2002): 103-122.

W. E. Bijker, *Democratisering van de Technologische Cultuur (Inaugurele Rede) (*Maastricht, 1995a).

W. E. Bijker, *Of Bicycles, Bakelites and Bulbs. Toward a Theory of Sociotechnical Change (*Cambridge, MA, 1995b).

P. M. Blaikie, T. Cannon, I. Davis and B. Wisner, *At risk. Natural hazards, people's vulnerability, and disasters (*London; New York, 1994).

G. C. Bowker and S. L. Star, *Sorting Things Out. Classification and its Consequences (*Cambridge, MA, 1999).

L. M. Branscomb, "The Changing Relationship between Science and Government Post-September 11," in *Science and Technology in a Vulnerable World (Supplement to AAAS Science and Technology Policy Yearbook 2003)*, Eds. A. H. Teich, S. D. Nelson and S. J. Lita (Washington, DC, 2002), pp. 21-32.

M. Callon, P. Lascoumes and Y. Barthe, *Agir dans un monde incertain. Essai sur la démocratie technique (*Paris, 2001).

M. Castells, *The rise of the network society (*Malden, MA, 1996 (2000)).

M. Castells, *The power of identity (*Malden, MA, 1997).

M. Castells, *End of millennium (*Malden, MA, 1998 (2000)).

P. N. Edwards, *The Closed World. Computers and the politics of discourse in cold war America (*Cambridge, MA, 1996).

EEA, *Late Lessons from Early Warnings: The Precautionary Principle 1896-2000 (*Copenhagen, 2001).

S. Epstein, *Impure Science. Aids, Activism, and the Politics of Knowledge (*Berkeley, CA, 1996).

K. Fortun, *Advocacy after Bhopal : environmentalism, disaster, new global orders (*Chicago, IL, 2001).

Gezondheidsraad, *Niet alle risico's zijn gelijk (*Den Haag, 1995).

Gezondheidsraad, *Risico, meer dan een getal: Handreiking voor een verdere ontwikkeling van de risicobenadering in het milieubeleid (*Den Haag, 1996).

B. Godin and Y. Gingras, "What is scientific and technological culture and how is it measured? A multidimensional model," *Public Understanding of Science* 9 (2000): 43-58.

H. Gottweis, *Governing Molecules. The Discursive Politics of Genetic Engineering in Europe and the United States (*Cambridge, MA, 1998).

M. R. C. Greenwood, "Risky Business: Research Universities in the POst-September 11 Era," in *Science and Technology in a Vulnerable World (Supplement to AAAS Science and Technology Policy Yearbook 2003)*, Eds. A. H. Teich, S. D. Nelson and S. J. Lita (Washington, DC, 2002), pp. 1-20.

M. Guggenheim and H. Nowotny, "Joy in Repetition Makes the Future Disappear. A Critical Assessment of the Present State of STS," in *Social Studies of Science and Technology. Looking Back, Ahead*, Eds. B. Joerges and H. Nowotny (Dordrecht, 2003), pp. 229-258.

G. Hecht, *The Radiance of France. Nuclear Power and National Identity after World War II (*Cambridge, MA, 1998).

L. Hickman, *Philosophical tools for technological culture: putting pragmatism to work (*Bloomington, 2001).

J. Keulartz, M. Korthals, M. Schermer and T. Swierstra, eds. *Pragmatist Ethics for a Technological Culture* (Dordrecht, 2002).

J. Keulartz, M. Schermer, M. Korthals and T. Swierstra, "Ethics in Technological Culture: A Programmatic Proposal for a Pragmatist Approach," *Science, Technology and Human Values* 29 (2004): 3-29.

A. Klinke and O. Renn, "A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies," *Risk Analysis* 22 (2002): 1071-1094.

T. La Porte, "The United States air traffic system: Increasing reliability in the midst of rapid growth," in *The Development of Large Technical Systems*, Eds. R. Mayntz and T. P. Hughes (Frankfurt am Main, 1988), pp. 215-244.

J. Law, "Ladbroke Grove: Or How to Think about Failing Systems," manuscript (2003).

J. Law and W. E. Bijker, "Postscript: Technology, Stability, and Social Theory," in *Shaping Technology - Building Society. Studies in Sociotechnical Change*, Eds. W. E. Bijker and J. Law (Cambridge, Ma, 1992), pp. 290-308.

M. Levin and R. Williams, "Forum on Rethinking Technology in the Aftermath of September 11," *History and Technology* 19 (2003): 29-83.

S. Mayer and A. Stirling, "Finding a Precautionary Approach to Technological Developments — Lessons for the Evaluation of GM Crops," *Journal of Agricultural and Environmental Ethics* 15 (2002): 57-71.

J. Mokyr, *The gifts of Athena : historical origins of the knowledge economy (*Princeton, NJ, 2002).

United Nations, *Rio Declaration on Environment and Development (*New York, 1992).

N. Oudshoorn and T. J. Pinch, *How users matter: the co-construction of users and technologies (*Cambridge, MA, 2003).

C. Perrow, *Normal Accidents: Living with High-Risk Technologies (*Princeton, NJ, 1999 (1984)).

T. Pinch and W. Bijker, "The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other," *Social Studies of Science* 14 (1984): 399-441.

G. I. Rochlin, "Iran Air Flight 655 and the USS *Vincennes*: Complex, Large-scale Military Systems and the Failure of Control," in *Social Responses to Large Technical Systems*, Ed. T. R. La Porte (Dordrecht, 1991), pp. 99-125.

G. I. Rochlin, "Broken Plowshare: System Failure and the Nuclear Power Industry," in *Changing Large Technical Systems*, Ed. J. Summerton (Boulder, CO, 1994), pp. 231-261.

N. Schlager, *When technology fails: significant technological disasters, accidents, and failures of the twentieth century (*Detroit, 1994).
J. A. Schumpeter, *Business cycles; a theoretical, historical, and statistical analysis of the capitalist process (*New York; London, 1939).
J. N. Shklar, *The faces of injustice (*New Haven, 1990).
K. S. Shrader-Frechette, *Risk and rationality : philosophical foundations for populist reforms (*Berkeley, 1991).
S. Sloan, "Terrorism: How Vulnerable is the United States?," in *Terrorism: National Security Policy and the Home Front*, Ed. S. Pelletiere (Carlisle, PA, 1995), Online available: http://nsi.org/Library/Terrorism/usterror.htm.
S. A. Snook, *Friendly fire: the accidental shootdown of U.S. Black Hawks over Northern Iraq (*Princeton, N.J., 2000).
D. Vaughan, *The Challenger Launch Decision. Risky Technology, Culture, and Deviance at NASA (*Chicago, IL, 1996).
H. Verran, *Science and an African logic (*Chicago, IL, 2001).
G. L. Wackers and J. Kørte, "Drift and Vulnerability in a Complex Technical System: Reliability of Condition Monitoring Systems in North Sea Offshore Helicopter Transport," *Int. J. of Engineering Education* 19 (2003): 192-205.
H. Watson-Verran and D. Turnbull, "Science and Other Indigenous Knowledge Systems," in *Handbook of Science and Technology Studies*, Eds. S. Jasanoff, G. E. Markle, J. C. Petersen and T. Pinch (Thousand Oaks, 1995), pp. 115-139.
A. Wildavski, *But Is It True? A Citizen's Guide to Environmental Health and Safety Issues (*Cambridge, MA, 1995).
R. d. Wilde, N. Vermeulen and M. Reithler, *Bezeten van genen. Een essay over de innovatieoorlog rondom genetisch gemodificeerd voedsel (*Den Haag, 2002).

Endnotes

[1] This paper is the result of numerous discussions with many people. I want to thank Wes Shrum, Rosalind Williams, Steve Rayner, and Steve Woolgar. I also benefited greatly from the comments by participants in the March 2002 Workshop at MIT (see note 4); the conference 'Cultures of Technology and the Quest for Innovation' in Essen, April 2003; the STS colloquium in Maastricht, May 2003; and a seminar at the Said Business School, Oxford University, June 2003. Special thanks for a discussion of the previous draft go to Karin Bijsterveld, Helga Nowotny, Ger Wackers, and Rein de Wilde.

[2] A workshop in March 2002, at the STS Program of MIT, provided a first inventory and discussion of the implications that 9/11 might have for studying technology in society (Levin and Williams 2003). To locate this research on vulnerability within current STS work, I will give more references than would be necessary for the vulnerability issue itself.

[3] **Did this sentence indeed make it from the conference programme to the book introduction?**

[4] This is the characterization that Michael Guggenheim and Helga Nowotny give of what distinguishes STS from other social sciences (Guggenheim and Nowotny 2003: 241).

[5] See for example Godin (2000). I first used the phrase 'technological culture' in my inaugural lecture: Bijker (1995a), in Dutch. See also Bijker (1995b).

[6] Italics in the original: Hickman (2001: 1-3). See also Keulartz et al. (2002, 2004).

[7] A similar constructivist account of vulnerability is discussed by Kristin Shrader-Frechette (1991). In these risk discussions, however, a contrast is created between the 'constructivist camp' and the 'realist camp' of risk assessment. I do not agree with that distinction because the underlying suggestion is that scientific data is more real that other information (Klinke and Renn 2002).

[8] The literature on the vulnerability of computers and the Internet is huge and still increasing, including complete journals and on-line databases. The use of Internet and computers for warfare and terrorism has been labelled 'cyberwar' or 'netwar'; see Arquilla (2001).

[9] See the website of the US Department of Homeland Security: http://www.ready.gov/ (12-1-2004).

[10] The developmental policy of the European Union is particularly targeted at the ACP countries: African, Caribbean, and Pacific countries.

[11] Fei Tevi, "Vulnerability: A Pacific Reality", Summit of ACP Heads of State and Government (Libreville, Gabon, 6-7 November 1997): 1.

[12] Fei Tevi, "Vulnerability: A Pacific Reality", Summit of ACP Heads of State and Government (Libreville, Gabon, 6-7 November 1997): 14.

[13] See the report by an ad hoc committee of the Society for Social Studies of Science, chaired by Gary Downey: "U.S. Visa Policies and Scholarly Work", Committee on

Immigration Policy and Scholarly Work, Society for Social Studies of Science, February 2003.

[14] See for example the chapter by M.R.C. Greenwood, chancellor of the University of California (Greenwood 2002); and the Statement from Bruce Alberts, President of the US National Academy of Sciences, Wm. A. Wulf, President of US National Academy of Engineering, and Harvey Fineberg, President of the US Institute of Medicine: 'Current Visa Restrictions Interfere with U.S. Science and Engineering Contributions to Important National Needs', 13 December 2002 (Revised 13 June 2003).

[15] I am inspired here by Shklar's plea "to treat injustice with the intellectual respect it deserves." (Shklar 1990: 17).