Journal of Risk Research
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/rjrr20

Risk, vulnerability, robustness, and resilience from a decision-theoretic perspective

Roland W. Scholz [a], Yann B. Blumer [a] & Fridolin S. Brand [a]

[a] Natural and Social Science Interface, Institute for Environmental Decisions, ETH Zurich, Zurich, Switzerland

Published online: 24 Nov 2011.

To cite this article: Roland W. Scholz , Yann B. Blumer & Fridolin S. Brand (2012) Risk, vulnerability, robustness, and resilience from a decision-theoretic perspective, Journal of Risk Research, 15:3, 313-330, DOI: 10.1080/13669877.2011.634522

To link to this article: http://dx.doi.org/10.1080/13669877.2011.634522

Journal of Risk Research
Vol. 15, No. 3, March 2012, 313–330

Risk, vulnerability, robustness, and resilience from a decision-theoretic perspective

Roland W. Scholz*, Yann B. Blumer and Fridolin S. Brand

Natural and Social Science Interface, Institute for Environmental Decisions, ETH Zurich, Zurich, Switzerland

(*Received 30 November 2010; final version received 16 September 2011*)

Risk, vulnerability, robustness, and resilience are terms that are being used increasingly frequently in a large range of sciences. This paper shows how these terms can be consistently defined based on a decision-theoretic, verbal, and formal definition. Risk is conceived as an evaluation of an uncertain loss potential. The paper starts from a formal decision-theoretic definition of risk, which distinguishes between the risk situation (i.e. the risk analyst's model of the situation in which someone perceives or assesses risk) and the risk function (i.e. the risk analyst's model about how someone is perceiving and assessing risk). The approach allows scholars to link together different historical approaches to risk, such as the toxicological risk concept and the action-based approach to risk. The paper then elaborates how risk, vulnerability, and resilience are all linked to one another. In general, the vulnerability concept, such as the definition of vulnerability by the Intergovernmental Panel on Climate Change (IPCC), goes beyond risk, as it includes an adaptive capacity. Thus vulnerability is mostly seen as a dynamic concept that refers to a certain period of time. If the vulnerability of a system is viewed only at a certain point of time, vulnerability equals risk. In contrast, if we consider dynamic risk in the sense that we include actions that may follow adverse events, risk resembles vulnerability. In this case we speak about adaptive risk management. Similar to vulnerability, resilience incorporates the capability of a system to cope with the adverse effects that a system has been exposed to. Here we distinguish between specified and general resilience. Specified resilience equals (dynamic) vulnerability as the adverse events linked to threats/hazards to which a system is exposed to are known. Robustness can be seen as an antonym to (static) vulnerability. General resilience includes coping with the unknown. In particular, the approach presented here allows us to precisely relate different types of risk, vulnerability, robustness and resilience, and considers all concepts together as part of adaptive risk management.

Keywords: risk; vulnerability; resilience; decision theory

1. Introduction

Risk, vulnerability, and resilience have become very popular concepts in environmental, health, and sustainability sciences, and as well in many other disciplines dealing with endangerments, threats, or other agents, which may cause adverse

*Corresponding author. Email: roland.scholz@env.ethz.ch

ISSN 1366-9877 print/ISSN 1466-4461 online

http://dx.doi.org/10.1080/13669877.2011.634522
http://www.tandfonline.com

affects in certain systems (Adger 2006; Folke 2006; Renn 2008). Many efforts have been made to harmonize different definitions of risk and to relate the concept of risk to vulnerability and resilience. The International Programme on Chemical Safety (IPCS) *Risk Assessment Terminology*, for instance, defines risk as the 'probability of an adverse effect in an organism, system, or (sub-)population caused under specified circumstances' (IPCS and WHO 2004, 13).

In general, *risk* is seen as a static concept and evaluates – based on processes of judgment or assessment (Scholz and Siegrist 2010) – the potential losses or adverse effects of uncertain events, which can result from an action or exposure to a hazard. In this paper we speak of outcomes, events, or impacts when referring to manifestations of the consequences of a decision or action, without introducing any evaluation. Hazard, danger, and threat are terms used synonymously to denote exposure to negative outcomes or to agents that may cause severe adverse future effects or losses. However, real-world risks are not static, but change depending on the actions taken by the system that is exposed to risk or changes and dynamics of the context. Thus, concepts such as systemic risk evolved. 'Systemic risks are at the crossroads between natural events (partially altered and amplified by human action . . .), economic, social and technological developments, and policy driven actions, all at the domestic and the international level' (Renn 2008, 15). This definition of risk endorses the dynamic perspective. We reveal below how static conceptions of risk and vulnerability are related to one another.

The concept of vulnerability became an important concept in the Third Assessment Report of the IPCC where *vulnerability* is defined as

> the degree to which a system is susceptible to, or unable to cope with, adverse effects . . . including . . . variability and extremes. Vulnerability is a function of the character, magnitude, and rate of . . . [external] variation to which a system is exposed, its sensitivity, and its adaptive capacity. (McCarthy et al., 2001, 6)

Here, the term *adaptive capacity*, the extent to which a natural or social system is susceptible to sustaining damage from climate change to the ability to implement prospective or reactive adaptive actions to cope with certain adverse events and their consequences. Given this prominent definition, vulnerability goes beyond a static 'manifestation of the inherent states of the system that can be subjected to a natural hazard or be exploited to adversely affect that system . . .' (Aven 2011, 519) as has been suggested by some risk researchers such as Haimes (2009).

The concept of *resilience* has recently emerged as a rising star to conceptualize human–environment systems in sustainability science (Folke 2006). However, a clear formal conception is lacking; as a result, the sound operationalization of resilience falls short, and advancement in this respect remains a core challenge of resilience research (Carpenter et al. 2001; Carpenter, Westley, and Turner 2005; Walker et al. 2002).

As the reader may already infer from the above, a key problem of the concepts of vulnerability and resilience is that they are often solely verbally defined. They often lack a crisp, formal conception and do not specify in which way a system is exposed to which threat, and how the likelihood for being hit by adverse events depends on the agents' behavior in the past, present, and future. In this article we present a decision-theoretic perspective that allows for a general formal definition of these concepts and the various uncertainties pertaining to the actions and behavior of systems, as well as the occurrence of outcomes, events, impacts, and their evaluation. A critical point is in what way risk, vulnerability and resilience are linked to certain types of action. The presented approach in particular allows scholars to precisely relate different types of risk, vulnerability, and resilience and considers all concepts together as part of adaptive risk management. Here, we define *adaptive risk management* as the sequence of actions which may be taken by a decision-maker or system (such as a company, government, etc.), after cognizing the exposure to risk or by being confronted with adverse impacts that result from a decision or action in a *risk situation* (a definition of risk situation is provided in Section 2.2).

The article is structured as follows. Section 2 reviews the cutting-edge research on risk, vulnerability, resilience and robustness, and illustrates how these concepts are related. Based on this, Section 3 links vulnerability and risk in a decision-theoretic framework, highlighting four different types of adaptations. Subsequently, Section 4 concludes with our findings, some reflections on the relationship between vulnerability, resilience and robustness and the challenge of operationalizing these concepts for quantitative assessments.

2. The essentials of risk and vulnerability

This section reviews the current state of the art in the discussion on risk, vulnerability, resilience, and robustness to show the close interconnectedness of these concepts.

2.1. Aspects and variants of risk

When we talk about risk, two aspects are essential to consider. The first aspect is how much the decision-maker knows about the future outcomes and their value. We only speak about risk if outcomes that may result in a certain situation or action are evaluated as losses, adverse effects, threats, hazards, danger, negative events (compared to a baseline), or outcomes. The second aspect is the conceptualization of the possibility or likelihood of a future event. We only speak about a risk situation if there is at least one possible future event where both the decision theorist and the decision-maker do not know with certainty whether it will manifest or not. This leads to the concept of risk in the meaning of the evaluation of the loss potential of an uncertain event resulting from an action. In this view, risk is genuinely prospective, as it refers to uncertain future events. In addition, risk can be considered as a primitive in the sense that it is an elementary concept that everybody shares, given the intuitive understanding that uncertain losses are involved (Brachinger and Weber 1997; Scholz and Tietje 2002).

As stated above, risk always includes an evaluation of losses. Thus, from a decision-theoretic perspective, risk judgments are based on preference or utility functions, which distinguish between gains and losses. However, we have to consider prospect theory (Tversky and Kahneman 1992), which reveals that what are considered to be losses or gains are relative and depend on the views or perspectives that a decision-maker takes with respect to a decision situation and its outcomes. Thus, when dealing with risk or vulnerability, we have to acknowledge that – in principle – the preference or utility function may change over time.

In many risk situations there is also a chance of gaining something, and the gains may be incorporated when evaluating risk. Conceptions in which risk is exclusively defined via the evaluation of adverse outcomes are denoted as pure risk.

If we include both the losses and the gains in a risk judgment or assessment, we speak about speculative risk (Brachinger and Weber 1997; Fishburn 1982).

When we look at the different definitions of risk provided in literature, a critical point is whether risk is tied to a decision or action. The German sociologist Luhmann (1990) suggested to differentiate risk from danger. In a risk situation, an individual must – in principle – have the opportunity to make a decision. A salient example would be a mother who rides a bike too quickly with her baby as a passenger. She is taking a risk, whereas her child is in danger. Thus, a natural hazard changes to a risk if a person or system makes a decision or takes an action that affects the occurrence of adverse impacts. In this paper, we follow this differentiation as we redefine different conceptions of risk and vulnerability from a decision-theoretic perspective.

2.2. Risk situation and risk function

The risk situation is the risk or decision analyst's model of the situation that a decision-maker may face or be encountered with. In the most elementary risk situation (see Figure 2), a decision-maker is supposed to have the choice between two alternatives, and an uncertain loss E^- is linked at least to one of them. Today, decision analysts do not only utilize probabilities, which are usually denoted with p (and whose calculus meets the Kolomogorov axioms) to model risk situations. Thus, we represent the uncertainties using $\tilde{p}$. The positive and negative outcomes ($E^+$and E^-) can be represented by value functions (e.g. amounts of money, usually denoted by v) or utility functions (of an absolute scale, usually represented by u).

We argue that – from a decision or risk analyst's perspective – probability and utility are the concepts commonly used to describe risk situations. Thus in general, the modeling of a risk situation is based on the use of probabilities $p_{i,j}$ for different events or outcomes $E_{i,j}$, which may result from a decision or action A_i. When constructing risk situations, the events have values $v(E_{i,j})$ or are valued by a utility function, $u(E_{i,j})$ and at least one of the uncertain events has a negative value (see Figure 2).

The *risk function* is the decision or risk analyst's model of how the risk is perceived, judged, or assessed by a decision-maker. In order to conceptualize risk judgments, the cognition of uncertainty and the existence of a preference function are required. However, the decision-maker must by no means make explicit reference to probability and utility, but only cognize uncertainty and potential losses (see Figure 1).

The risk function is a model of how the decision analyst conceives the risk assessment and risk judgment, whereas the risk situation is a model of the decision analyst's view on the situation for which a risk judgment or assessment is provided. As presented in Figure 3, the risk function transfers or maps the risk situation into a risk judgment or assessment. We denote the space of all possible risk assessments or risk judgments as the space of risk cognitions. Thus, the arguments of the risk function are taken from the pre-image set (A, p, E) and the image set of a risk function is the space of risk cognitions. The image set can be scalar (e.g. when only risk is represented by a rational number between 0 and 1), vector (e.g. if different statistical parameters of the distribution of outcomes represent risk, such as the mean and the semivariance of losses), or of a non-numerical type (e.g. if certain traits of the risk situation, e.g. the voluntariness, dread, etc. represent the risks). We should note that this representation allows for including the costs of getting access to a

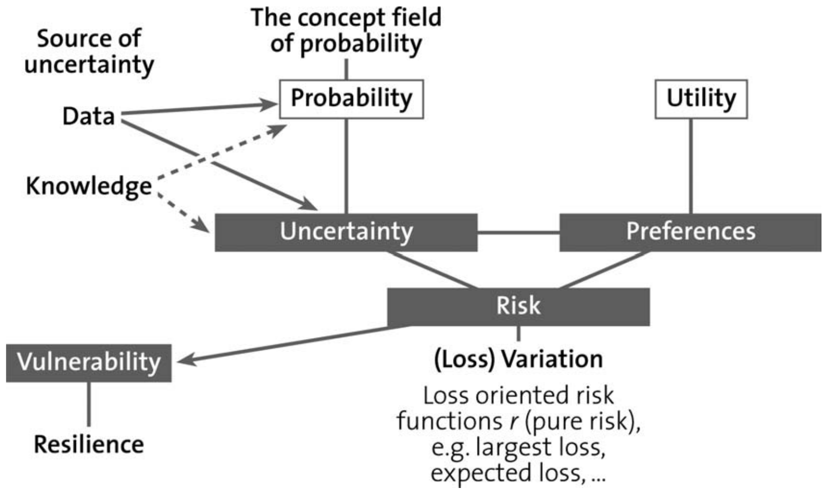

Figure 1. A roadmap of concepts: risk as a function of uncertainty and preferences; probability and utility as operationalization of uncertainty and preferences; vulnerability as an extension of risk that is complementary to resilience.

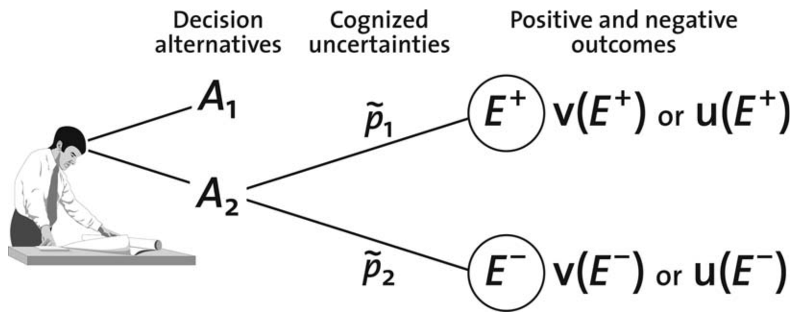

Figure 2. Definition of an elementary *risk situation* from a decision theoretic perspective. A player has the choice between two alternatives in which an uncertain loss E^- may appear (Scholz and Tietje 2002).

decision alternative (which is important for the aspect of discounting risk). This is done by incorporating A as an argument of the risk function.

The decision-maker is not (necessarily) supposed to explicitly cognize the probabilities and value function or the costs of getting access to a decision alternative. Instead, we assume that – for defining a risk function – the decision-maker has access to different alternatives and is recognizing that different alternatives may result with some likelihood/uncertainty, and that negative events or outcomes may also result.

We should know that there are different concepts of probability, such as the subjective, objective, logical, and many other variants of probability (Fine 1973; Hacking 1975; Scholz 1991), both on the side of the decision analyst, who conceptualizes the risk situation, and on the side of the decision-maker or risk assessor, when providing a risk judgment or risk assessment. Thus, we speak about a concept field of probability (see Figure 1), which includes at least the idea that probability is in

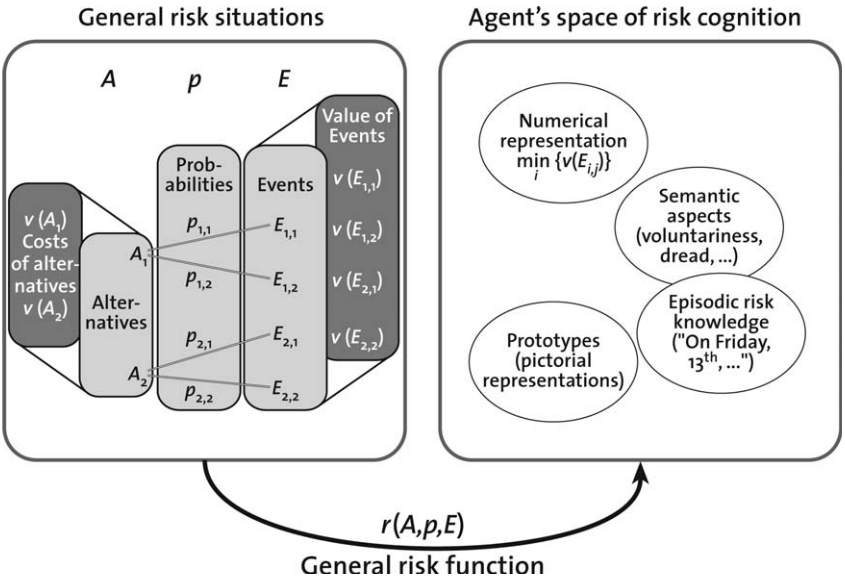

Figure 3. Graphical representation of general (discrete) risk situations and the general risk functions which map from the space of risk situations to the agent's risk cognition (Scholz and Tietje 2002, 181).

the *data* (i.e. notions of objective probability) or that probability is in the knowledge (i.e. notions of subjective probability). Yet in principal, if we speak about concepts of probability, these concepts have to follow the Kolomogorov axioms (which are the basis of probability calculus). Naturally, there are other concepts, such as fuzzy sets, belief functions (Shafer 1976), Baconian probabilities (Cohen 1980), or 'imprecise probabilities' (Walley 1991), which do not each follow the probability calculus, but aspire to conceptualize uncertainty (Scholz 1987).

2.3. Vulnerability, robustness, and resilience

Vulnerability is also a basic concept whose notion is understood by everyone. It goes back to the Latin term *vulnus* (wound) or *vulnerare* (to wound). Systems that are vulnerable are open to attack, damage, or adverse impacts. The concept of vulnerability is used in many disciplines, ranging from medicine (via public health and psychology), to economics and finance, and from environmental sciences to technical systems such as information technology systems (Adger 2006). If we want to define vulnerability, it is important to note that 'vulnerability is not static, but rather is constantly changing' (Miller et al. 2010). Vulnerability includes the option to lessen exposure or sensitivity. As Jerome Ellison puts it: 'the man who can read commercial documents ... is far less *vulnerable* to fraud' (Merriam-Webster 2002a). As we will show, one has to differentiate between vulnerability at a certain point of time and vulnerability over a certain span or period of time. Today, in particular, the concept of vulnerability has become a key concept in climate research, where specific species, water systems, coastal systems, countries, or ecosystems are usually seen as vulnerable (Adger 2006). These strands have in common the fact that vulnerability is conceived as a function of the exposure, sensitivity, and adaptive capacity of a system (McCarthy et al., 2001; see Polsky, Neff, and Yarnal 2007).

It is interesting to see that in many of these fields, vulnerability is seen as complementary to resilience (Chapin et al. 2010; Gallopin 2006; Miller et al. 2010), as both resilience and vulnerability deal with system responses to disturbances. Others consider vulnerability to be an antonym of *robustness* (Aven 2011, 521). Originally used in relation to the robustness of populations and ecosystems, resilience has been recently extended to a wider perspective on the interplay of disturbance and reorganization in human–environment systems (Brand and Jax 2007; Folke 2006). In general, resilience is defined as a system's capability to adsorb shocks or to avoid crossing a threshold and to reorganize after an adverse affect or exposure to danger (Resilience Alliance 2009). Contrary to resilience, robustness does not include the ability to reorganize (Aven 2011), and instead is seen as a (static) system property. When expressing it in other terms, which relate resilience directly to vulnerability, 'resilience is a system's capability to prevent catastrophes as sudden radical changes or the breakdown of a certain state' (Scholz and Tietje 2002, 317–8) when showing proper adaptive actions.

We will refer to this topic in Section 3 when distinguishing between static and dynamic concepts of risk and vulnerability. In Section 4, we further highlight the distinction between specified (or targeted) and general resilience (Walker and Salt 2006). Specified resilience signifies the resilience of a given system to a specific disturbance regime, (e.g. Bennett, Cumming, and Peterson 2005), and aims to operationalize resilience of what to what by means of resilience surrogates (Carpenter et al. 2001; Carpenter, Westley, and Turner 2005; Walker et al. 2002). In contrast, general resilience corresponds to 'the general capacities of a social–ecological system that allow it to absorb unforeseen disturbances' (Walker and Salt 2006, 120). In this vein, Walker et al. (2002) propose to focus on 'maintaining the capacity of the system to cope with whatever the future brings, without the system changing in undesirable ways.'

We will show that a proper formal definition of vulnerability may better relate vulnerability to resilience and may contribute to the formalization of resilience as well.

2.4. *Semiformal definitions of risk and vulnerability*

As we have already seen above, a formal, mathematical representation helps to precisely describe the relations between (i) a system or a decision-maker, (ii) the actions (or decisions) which are taken by a decision-maker, (iii) the events and their perceived or anticipated impacts (including their valuation), (iv) the uncertainty of these events, and (v) how these elements of a risk situation are integrated into what is understood by risk judgment or risk assessment. In the following, we show how a formal definition allows for exact specification of the relation between risk and vulnerability. We start with two semiformal representations of risk. In the environmental toxicology community, risk is defined as a function of exposure (Equation (1))

$$\text{risk} = f(\text{exposure},\ \text{sensitivity}). \tag{1}$$

Another common reductionist description conceives risk as the probability of loss (Equation (2)), or as is frequently done in insurance, defines risk by the probability (or frequency) of losses (e.g. deaths) multiplied by the amount of loss (Equation (3)):

$$\text{risk} = p(\text{loss}) = p(\text{loss from future action}), \tag{2}$$

$$\text{risk} = p(\text{loss}) \times v(\text{loss}). \tag{3}$$

The latter (Equations (2) and (3)) are close to the definition of hazard as 'an adverse chance (as of being lost, injured, or defeated)' (Merriam-Webster 2002b). 'Indeed, *risk* must be measured in terms of the likelihood and severity of adverse risk' (Haimes 2006, 295). In general, *risk* can be defined and measured as a function of the probability and the severity of losses or adverse effects:

$$\text{risk} = f(\text{uncertainty of loss, value of loss}). \tag{4}$$

A semiformal definition of vulnerability plays an important role in the IPCC definition, which is presented in Section 1:

$$\text{vulnerability} = f(\text{exposure, sensitivity, adaptive capacity}). \tag{5}$$

As we can see when comparing Equations (1) and (5), the adaptive capacity is the extension of the toxicological risk concept leading to vulnerability in the IPCC definition. In the following we conceive this component of vulnerability as a system's or decision-maker's capability to take actions in order to change, reduce, or mitigate a given risk.

3. Decision-theoretic definitions of risk and vulnerability

We start by presenting formal definitions of a decision-theoretical risk definition and show that these definitions may become identical if they include certain assumptions about how the actors behave and in what way adverse environmental impacts resulting from events may be evaluated by risk judgments or risk assessments. We then show how vulnerability can be seen as adaptive risk management, in the sense that certain means can be taken in a given time range in order to reduce the risk.

Most representations are used to delineate (countable) discrete actions and events. But the elementary definitions can easily be transferred to sets of continuous actions (for instance, time spent standing at a dangerous location as a variable representing action) or events (for instance, pain as an impact variable, which can be measured on a continuous scale).

3.1. Formal definitions of risk from a decision-theoretic perspective

We start from the decision-theoretic risk concept, which has prevailed in risk research across many disciplines. In this section we largely follow the work of Scholz and Tietje (2002). As illustrated in Section 2.2, we distinguish between a risk situation and a risk function. A risk situation is a decision situation in which an actor has the choice between different alternatives, where the choice of at least one alternative is linked to an uncertain loss. The risk function is the evaluation of the different alternatives related to the riskiness of a situation, as perceived by a decision-maker.

The risk function is the decision analyst's model of how a decision-maker or risk assessor evaluates the riskiness of the alternatives. We present a formal description of these two concepts.

In a decision-theoretic model of a (specific) risk situation R_s (see Figure 1), an actor or decision-maker has the option to choose from a set of different alternatives A (Equation (6))

$$A = \{A_1, \ldots, A_i, \ldots, A_n\}. \tag{6}$$

Given the choice of an alternative A_i, a set of different outcomes or events may result:

$$E_i = (E_{i,1}, \ldots, E_{i,j}, \ldots, E_{i,N_i}). \tag{7}$$

E simply defines the set of all possible (known) future events which means

$$E = \bigcup_i \{E_i\}. \tag{8}$$

As the definition of a risk situation relies on conceptualizing the 'likelihood' according to probabilities, given the choice of an alternative A_i, the event $E_{i,j}$ occurs with the probability $p_{i,j} = p(E_{i,j})$. Thus

$$p = (p_{i,1}, \ldots, p_{i,1}, \ldots, p_{i,N_i}), \tag{9}$$

denotes the probability function of the occurrence for outcomes E_i that may result if the alternative A_i is chosen. The set p includes all probability vectors for all sets of events that may result for all (action) alternatives A_i

$$p = \bigcup_i \{p_i\}. \tag{10}$$

Thus, a specific risk situation R_S is defined by the three three sets, i.e. the set of alternatives A that can be chosen, the set future events E and their probabilities p:

$$R_S = (A, p, E). \tag{11}$$

Formally, the risk function r (of a decision-maker, system or risk assessor) can be conceived as the mapping from the set of all possible risk situations (called $\hat{R}_S$) to the space of risk cognitions $\hat{R}_C$. Formally this reads:

$$r : \hat{R}_S = \bigcup \{R_S\} \rightarrow \hat{R}_C = \bigcup \{R_C\}. \tag{12}$$

$\hat{R}_S$ is the set of all risk situations that a decision assessor or decision-maker may face or is supposed to face in the eyes of a decision analyst. $\hat{R}_C$ denotes the set of risk cognitions (i.e. risk perceptions or risk assessments), which are all (conscious or unconscious) evaluations that a decision-maker is facing. Fundamentally different types of risk functions can exist. As mentioned above, a decision-maker can represent the riskiness of the outcomes of a decision either numerically (e.g. by '$r = 0.74$'), verbally (e.g. by 'the risk is very high'), episodically (e.g. 'this choice reminds me of the decision which I had to make when …'), physiologically–emotionally (e.g. a measure of the arousal or psychogalvanic resistance of the skin) or of another type (see Figure 3, right side). The risk functions also include formal, method-based risk assessments.

Vlek and Stallen (1980) point out that the (numerical) risk function of a decision-maker might focus on (avoiding) the largest possible loss, the distribution of losses (for instance, when measured by the semivariance of losses, the bigger losses get a quadratically higher evaluation in the risk function), or even on the expectancy value. Here we want to stress that the expectancy value of the outcomes related to an alternative is not semantically representing the expected utility, but rather the riskiness judged by the average loss or gain that results when choosing a certain alternative.

Technically the latter reads that maximum loss (i.e. the outcome with the lowest value; Equation (13)), the semivariance of losses (Equation (14)) or the expected value (Equation (15)) may become risk functions:

$$r_1(A_i) = \min_j \{v(E_{i,j})\}, \tag{13}$$

$$r_2(A_i) = \sum_{j \text{ with } v(E_j)<0} (p_{i,j} \times v(E_{i,j}) - 0)^2, \tag{14}$$

$$r_3(A_i) = \sum_{i=1} p_{i,j} \times v(E_{i,j}). \tag{15}$$

Naturally, there may be many other risk functions r_k for a certain decision-maker. For the functions r_2 and r_3 the decision-maker must be able to recognize and link the probabilities and values (utilities) of outcomes. This may not always be the case, as the risk functions may just be the uneasiness felt when facing the largest loss. If this is the case, Equation (13) would change to Equation (16), where f_u is the function representing the felt uneasiness:

$$r_4(A_i) = \max_j \{f_u(v(E_{i,j}))\}. \tag{16}$$

3.2. *Defining the exposure-based (toxicological) risk concept*

The exposure-based risk concept is frequently used in toxicology and environmental risk assessment (Paustenbach 1989, 2002). This variant of risk (see (1)) emerges from the idea that a system S is exposed to a certain dose caused by a threat, hazard, which then has a certain impact on that system. We call the loss-related characteristics of the dose–response relationship sensitivity.

Simplified, we can consider the dose to be the exposure and the response to be the impact. The dose D may represent the total uptake or concentration of a toxicant. A stochastic response, sensitivity, or impact I may represent the outcomes. An outcome may be the likelihood of getting a certain disease or a different degree of system dysfunction (illness). Figure 4 shows different dose–response functions, which map different sensitivities. Thus, the dose–response function $\mathrm{r}_{\mathrm{exposure}}$ becomes a risk function. In a formalized form, we can write

$$r_{\text{exposure}} : D \rightarrow I. \tag{17}$$

Here

$$D = \bigcup_i \{D_i\}, \tag{18}$$

represents all possible exposures or doses D_i and

$$I = \bigcup_j \{I_j\}, \tag{19}$$

all possible impacts.

Clearly, the assumption of a deterministic dose–response relationship represents an oversimplification. Thus, it is more realistic to assume that – given a certain dose D_i – the different responses occur with a certain probability. Formally, we can represent this by means of impact-related probabilistic response functions. In the case of a continuous scaling of the responses, we can represent the probability distribution of the impact using the density function

$$f_{D_i}(I). \tag{20}$$

If we assume a discrete set of impacts (e.g. by distinguishing between the impacts 'dead' and 'alive' or different states of being alive), we can represent the probabilities of a set of impacts related to a dose D_i as

$$P(D_i) = p_i = (p(D_{i,1}), \ldots, p(D_{i,j}), \ldots, p(D_{i,N_i})). \tag{21}$$

Figure 4 represents three exemplary (continuous) dose–response functions, which we call r_1^x, r_2^x, and r_3^x. We can think about a certain concentration of a toxic substance in a critical compartment of a living system or the probability of risk dysfunction. Naturally, the assumption of a deterministic dose–response function is unrealistic. Thus, we assume that for a certain dose, $D_i = x_i$, certain responses (i.e. impacts, outcomes, or adverse effects) may appear probabilistically. These are represented by the probability distributions $f_{x_i}^1(I)$, $f_{x_i}^2(I)$, and $f_{x_i}^3(I)$.

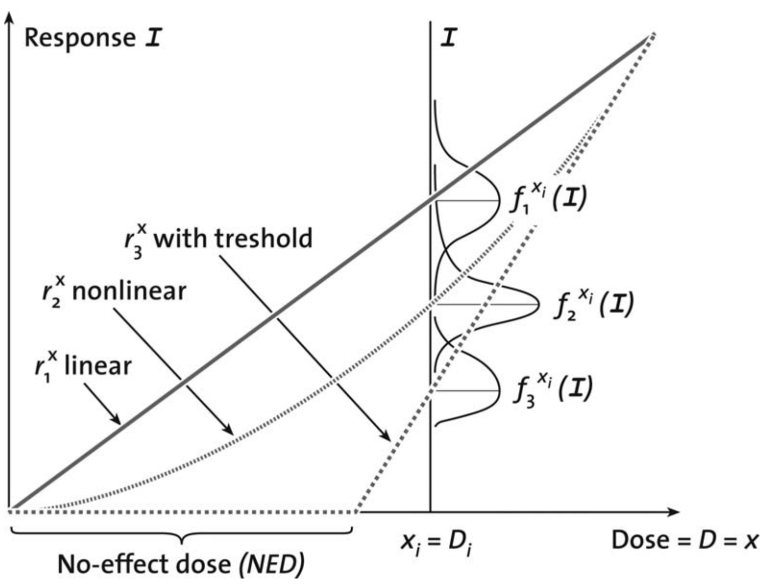

Figure 4. Linear, nonlinear risk (i.e. dose–response) functions r_1^x, r_2^x, and r_3^x with and without threshold and exemplary probabilistic dose–response functions $f_1^{x_i}$, $f_2^{x_i}$, and $f_3^{x_i}$ illustrated for a certain dose $x_i = D_i$.

3.3. Relating the decision-theoretic and the toxicological concepts of risk

The formal definition of risk reveals that the decision-theoretic concept of risk equals the toxicological definition of risk, if the doses D_i are supposed to be dependent on the behavior of a person and seen as a function or consequence (c) of actions taken, or even simplified and interpreted as actions A_i:

$$D_i = c(A_i) = A_i. \tag{22}$$

Furthermore, the set of impacts I_i can be seen as a set of events E_i:

$$E_i = I_i. \tag{23}$$

This can be reasoned by interpreting the dose of a toxicant as an impact of the conscious or unconscious behavior (decision) of a subject (decision-maker). Also, the costs of getting access to an alternative (which means here: receiving a certain dose) can also be included. At least in the context of an industrial society, it often holds true that being exposed to contaminants in lower doses (e.g. by living in city areas with low air contamination) is linked to certain costs. We should note that if exposure is completely independent of behavior, we should not talk about risk.

3.4. Definitions of vulnerability

3.4.1. Static vulnerability equals risk

In the *toxicological risk* concept, the *exposure* to a threat mostly means being exposed to a *dose* of toxicants. The vulnerability concept, however, relies on a broader concept of exposure, which includes, for instance, natural hazards, or environmental changes such as global warming. In the technical domain, exposure may be related to terrorist attacks or the unreliable supply of technical parts. In financial markets, exposure may refer to uncontrolled market dynamics, resulting in tipping points. In all these cases, we postulate an active component of the system or decision-maker before he receives an exposure, D_i. We assume (see Equation (24)), that the exposure is an impact or consequence (i.e. a function c) of an (action) alternative A_i

$$XP_i = D_i = c(A_i). \tag{24}$$

In its most simplified form, one can even identify a specific exposure XP_i with a specific action A_i, which means $XP_i = A_i$.

We speak about static vulnerability if the time dimension is not specified. In this case, the outcomes are considered to take place simultaneously (or 'directly after' the decision or action). When we consider the exposure at a given point of time t as a variable, we turn to vulnerability as a dynamic concept. The conditions of the environment may change over time or because of the impacts of an action taken. Thus, in general, we have to consider vulnerability as function of time: $vu(t)$.

Similar to what we have done with the toxicological risk definition, we conceptualize sensitivity within the definition of vulnerability (see Equation (5)) as specific responses $I_{i,j} = E_{i,j}$ or action A_i in a stochastic manner, and assume that certain impacts $I_{i,j} = E_{i,j}$ may result with probability $p_{i,j} = p(E_{i,j})$ in the discrete case (or $f_x(I)$ where x is the exposure and I the impacts which represent the events).

Thus, if we only consider one point of time t_0, the static vulnerability function can be transferred in a risk function:

$$vu(t_0) = vu(A, p, E) = r(A, p, E). \tag{25}$$

3.4.2. *Vulnerability as a dynamic concept*

Vulnerability can be conceived of as a dynamic concept $vu(t)$, if we study the vulnerability of a system over a time period $[t_0, t_1]$. In principle, there are two sources of change. We can look at changes of or within the decision-maker (or system) over time. And we can look at changes of the environment, which can be either impacts of the actions of the decision-maker or which can happen independently of the decision-maker. Thus, when linking the time axis to the left side of Figure 3, Figure 5 distinguishes between four major changes in the vulnerability $vu(t)$ of a system within the time interval $[t_0, t_1]$. First, the vulnerability may change as new events emerge over time that have not occurred before, or certain (adverse) events may disappear (changing events). Second, the probabilities of the occurrence of certain events may change (changing probabilities). Third, the function that valuates the events may change over time as certain events/outcomes become more or less important (changing value or utility functions). And fourth, due to the adaptive capacity, a decision-maker may develop certain new actions that were not available before, or the capability to show certain actions may disappear (creating new action alternatives).

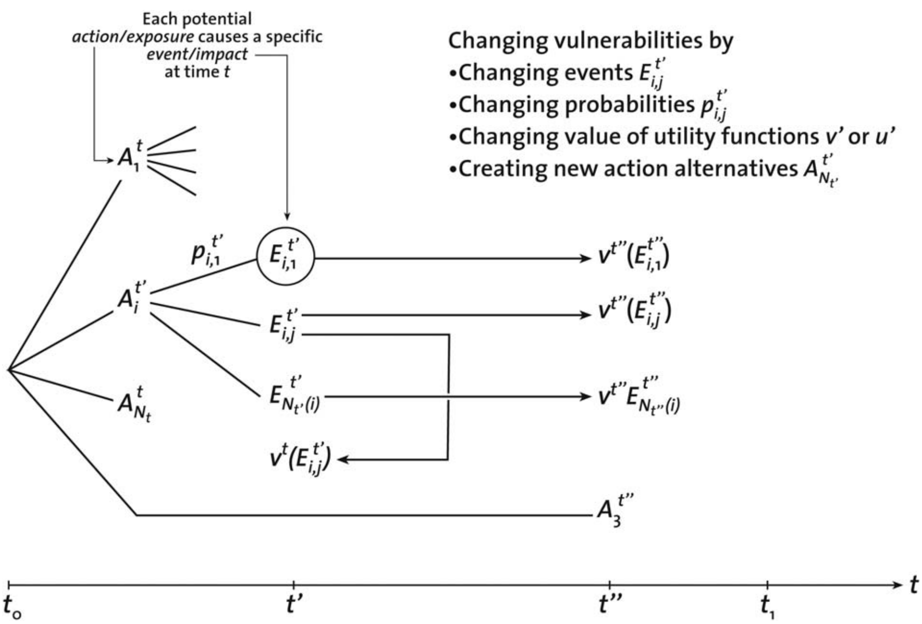

Figure 5. Changing events, probabilities, value or utility functions, and new actions over time t in the definition of vulnerability within a period $[t_0, t_1]$, which are partly due to adaptive capacity.

3.4.3. Formal description of the types of changes of adaptation and vulnerability

Let us assume that there is a set of actions $\{A_1^{t\prime}, \ldots, A_i^{t\prime}, \ldots, A_{N_i}^{t\prime}\}$ which is at the disposal of a decision-maker at time $t_0 \le t' \le t_1$ and that each action may cause different events $E_{1,1}^{i}, \ldots, E_{i,j}^{t\prime}, \ldots, E_{N(i)_{t\prime}}^{t\prime}$. Each event $E_{i,j}^{t\prime}$ may appear with a probability $p_{i,j}^{t\prime}$.

The first type of vulnerability change formally means (see Figure 5) that the events/outcomes that may result from one and the same action A_i^t may change over time, i.e.

$$E_{i,j}^{t\prime} \neq E_{i,j}^{t\prime\prime} \quad \text{for some} \quad i \neq j \quad \text{and} \quad t' \neq t''. \tag{26}$$

The issue that the number of events may change is formally represented by a certain number of events $N(i)_t$ and we assume that $N_{t\prime}(i) \neq N_{t\prime\prime}(i)$ for some actions A_i^t with $t \le t' \neq t\prime\prime$.

Second, the probabilities of an event linked to an action may change over time, which similarly reads

$$p_{i,j}^{t} \neq p_{i,j}^{t\prime} \quad \text{for some} \quad i \neq j \quad \text{and} \quad t' \neq t''. \tag{27}$$

Third, the value or utility function may change over time, which reads

$$v^{t\prime}(E_{i,j}^{t\prime}) \neq v^{t\prime\prime}(E_{i,j}^{t\prime\prime}) \quad \text{for some} \quad i,\ t' \neq t'' \quad \text{with} \quad E_{i,j}^{t\prime} = E_{i,j}^{t\prime\prime}. \tag{28}$$

Fourth, the decision-makers or the systems may enrich their behavioral program and may introduce new action alternatives or may lose the capability to perform some alternatives. Thus the number of alternatives may change over time (expressed by a changing index N_t in $A_{N_t}^t$).

As mentioned above, the change in events and probabilities can be seen as partly independent and as partly dependent on the decision-maker's activity. If they are dependent, they may be seen as components of the adaptive capacity, such as a change of the value/utility functions and the introduction of new alternatives.

4. Summary, discussion, and conclusions

4.1. Vulnerability and adaptive risk management

This paper relates the main definitions of variants of risk and vulnerability and illuminates the key components from a decision-theoretic perspective. We elaborated that all concepts, such as risk, vulnerability, robustness, and resilience, can be looked at from a static and a dynamic perspective.

We revealed that vulnerability could be conceived as a certain form of dynamic risk management, in which the environment is changing and the decision-maker is able to partially affect the (probabilities and events of the) environment, change the evaluation of the events, or invent new decision alternatives and actions. This meets the definition and notion of vulnerability if a management perspective is taken. We call this specific form of dynamic risk management adaptive risk management. In adaptive risk management, actions and decisions are taken from the perspective that unwanted or critical negative events in a changing environment should be prevented over time. This is the core meaning of coping with or reducing vulnerability.

4.2. The challenge to define uncertainties and probabilities

Uncertainty is a main component of both the risk and the vulnerability concept. In a colloquial sense, uncertainty may exist with respect to the value of the events and may relate to the likelihood of the occurrence of (particular/certain) outcomes. We argue that the notion of the term uncertainty asks for specification, in particular when dealing with risk and vulnerability.

We revealed that, from a decision-theoretic perspective, different types and languages of uncertainty might be involved in the risk situation or the risk function. It is meaningful to assume that the risk analysts have a clear model (i.e. know) what events may occur, and that the analysts have a model of the likelihood of the events if they speak about risk or risk management. The risk function, on the contrary, is a model of how an assessor calculates or measures risk, or how a decision-maker perceives or judges risk. At least for the (lay) decision-maker, it is implausible to assume that that the specific values (or utilities) of the outcomes are known and that he/she cognizes a probability distribution (which meets the probability calculus) when perceiving risk or providing a risk judgment. The same may hold true for expert risk assessments, which are often not based on explicit probabilities and value functions (Otway and Vonwinterfeldt 1992). Thus, the 'knowledge given' may differ between a risk situation and a risk function. Simply, we suggest that for risk situations, knowledge about the occurrence should – in general – be represented by probabilities (or similar quantitative concepts) and the knowledge about the value of the events in a quantitative manner (e.g. by value or utility function). However, when looking at risk functions, 'knowledge given' may just mean that the decision-maker has a clear image of positively and negatively evaluated events (e.g. by partially ordered preference functions, Lehmann 1996) and that the likelihood of the different events may be at least qualitatively assessed (e.g. the probability is very high).

4.3. Danger, risk, and vulnerability

We show from a decision-theoretic perspective that the terms hazard, risk, and vulnerability apply to different situations. We think that it is meaningful to talk about *danger* (threat, peril) if a decision-maker faces a threat whose exposure is supposed to be independent of the action taken by the decision-maker. On the contrary, when we talk about risk or vulnerability, we include the (conscious or unconscious, intended, or unintended) decisions, choice of strategies, actions, or alternatives that induce different types of exposure, events, outcomes, effects, impacts, or (environmental) responses. When we measure danger or hazard, we should restrict ourselves to the assessment of the 'threats to humans and what they value' (Hohenemser, Kates, and Slovic 1983, 379). Risk assessments or judgments, however, include the conditional likelihood or probability, given a certain decision or action, the valuation of the losses and – if a speculative risk perspective is taken – the evaluation of gains that may result from an alternative.

When representing the risk situation and risk functions in mathematical terms, we could show that, under a few assumptions (i.e. assuming that different exposures include a behavioral or action component and assuming a probabilistic dose–response function), the exposure × sensitivity-based toxicological risk concept can be transferred to the decision × uncertain loss-based decision-theoretic risk concept. This directly provides the link to vulnerability.

Contrary to risk, which is conceived mostly as a static concept, vulnerability is primarily a dynamic concept. The formal analysis revealed that, if we look at vulnerability of a system only at a certain point of time (i.e. static), it is identical to the decision-theoretic concept of risk. If we look at vulnerability over a certain period of time, the adaptive capacity of a system may allow to affect that: (i) certain events which may result from an action/decision may disappear, change, or that new events appear and (ii) that the probability that an event appears may change over time and be partly affected by previous actions. But (iii), the decision-maker can also change the evaluation of certain adverse events, which are due to a decision-maker's or system's vulnerability. The change in valuation can have different causes, e.g. certain events are judged differently, or because the environment has changed and a certain loss becomes relative, as it can be compensated for by other issues. Finally (iv) a decision-maker or system can expand the scope of its actions or decisions. The actions involved in (iii) and (iv) together represent the adaptive capacity, which is the decision-maker's capacity to change the risk to which the system will be exposed over time. The term adaptive risk management makes risk a dynamic concept, as indicated by the term adaptive risk management.

4.4. Vulnerability and resilience

This article has proved the old insight that mathematics provides nothing new, but simply allows us to describe things more precisely. We have shown that vulnerability and resilience are not complementary, but instead are highly similar, and in many respects, identical concepts. In general, resilience can be seen as the system's capability to prevent catastrophes or breakdowns (Scholz and Tietje 2002). The concept of 'specified resilience' asks to identify 'a particular threshold effect, where the system will not recover its earlier pattern of behavior if this threshold is passed' (Walker 2009). Based on this, it is very easy to construct a model of adaptive risk management in which future events are (supposed) to be eliminated if their value is below the threshold (see Figure 5). Thus, we think that specified resilience can be formalized similarly to the method that we propose in this article for the concept of vulnerability. However, the concept of 'general resilience' does not specify any kind of specific shock or catastrophe that will affect a system. General resilience instead acknowledges the unknown that we face with regard to future states, and which stress impacts we may be exposed to. We argue that, for instance, sustainability requires the design of resilient human–environment systems that are capable to cope with any disturbances that may appear in the future (cf. Chapin et al. 2006).

According to the conceptual framework represented in this paper, specified resilience can be conceived as adaptive risk management or coping with vulnerability, whereas general resilience goes beyond this frame. Thus, we argue that resilience research may highly benefit from the merits of four decades of risk research. This will, however, require that risk increasingly be conceived of as a dynamic concept, as we suggest in this article.

4.5. The relation of the concepts in a nutshell

We talk about danger (peril, threat) if the exposed human or system is not supposed to make a decision or take an action related to the source of danger. In the decision-theoretic framework presented here, risk includes a related behavioral, action alternative component. The framework provides a language to represent and to relate different variants of risk, such as toxicological, pure vs. speculative risk, or risk perception and risk assessment.

Risk, vulnerability, robustness, and resilience are strongly related concepts. Risk, vulnerability, and robustness can be conceptualized in a static and dynamic manner. From a decision-theoretic view, (static) vulnerability is the same as the risk concept. In contrast, we can define adaptive risk management (i.e. dynamic risk) in such a way that it equals vulnerability.

(Dynamic) Vulnerability may become specified resilience. In vulnerability, as in robustness, the potential threats are known. Robustness can best be seen as an antonym of vulnerability, and in the case of a scalar measurement, one concept similarly represents the negative of the other. In general (non-specified) resilience, however, the future adverse events are not known. Here the challenge is not to cope with uncertainty, but with the unknown, which opens a new, previously unrecognized floor for decision research.

References

Adger, W.N. 2006. Vulnerability. *Global Environmental Change* 16, no. 3: 268–81.

Aven, T. 2011. On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. *Risk Analysis* 31, no. 4: 515–22.

Bennett, E.M., G.S. Cumming, and G.D. Peterson. 2005. A systems model approach to determining resilience surrogates for case studies. *Ecosystems* 8, no. 8: 945–57.

Brachinger, H.W., and M. Weber. 1997. Risk as a primitive: A survey of measures of perceived risk. *Operations Research-Spectrum* 19, no. 4: 235–94.

Brand, F.S., and K. Jax. 2007. Focusing the meaning(s) of resilience: Resilience as a descriptive concept and a boundary object. *Ecology and Society* 12, no. 1.

Carpenter, S., B. Walker, J.M. Anderies, and N. Abel. 2001. From metaphor to measurement: Resilience of what to what? *Ecosystems* 4, no. 8: 765–81.

Carpenter, S.R., F. Westley, and M.G. Turner. 2005. Surrogates for resilience of social-ecological systems. *Ecosystems* 8, no. 8: 941–4.

Chapin, F.S., S.R. Carpenter, G.P. Kofinas, C. Folke, N. Abel, W.C. Clark, P. Olsson, et al. 2010. Ecosystem stewardship: Sustainability strategies for a rapidly changing planet. *Trends in Ecology & Evolution* 25, no. 4: 241–9.

Chapin, F.S., A.L. Lovecraft, E.S. Zavaleta, J. Nelson, M.D. Robards, G.P. Kofinas, S.F. Trainor, G.D. Peterson, H.P. Huntington, and R.L. Naylor. 2006. Policy strategies to address sustainability of Alaskan boreal forests in response to a directionally changing climate. *Proceedings of the National Academy of Sciences of the United States of America* 103, no. 45: 16637–43.

Cohen, L.J. 1980. Some historical remarks on the Baconian conception of probability. *Journal of the History of Ideas* 41: 219–31.

Fine, T.L. 1973. *Theories of probability: An examination of foundations*. New York, NY: Academic Press.

Fishburn, P.C. 1982. Foundations of risk measurement. II. Effects of gains on risk. *Journal of Mathematical Psychology* 25, no. 3: 226–42.

Folke, C. 2006. Resilience: The emergence of a perspective for social-ecological systems analyses. *Global Environmental Change – Human and Policy Dimensions* 16, no. 3: 253–67.

Gallopin, G.C. 2006. Linkages between vulnerability, resilience, and adaptive capacity. *Global Environmental Change – Human and Policy Dimensions* 16, no. 3: 293–303.

Hacking, I. 1975. *The emergence of probability*. Cambridge, MA: Cambridge University Press.

Haimes, Y.Y. 2006. On the definition of vulnerabilities in measuring risks to infrastructures. *Risk Analysis* 26, no. 2: 293–6.

Haimes, Y.Y. 2009. On the definition of resilience in systems. *Risk Analysis* 29, no. 4: 498–501.

Hohenemser, C., R.W. Kates, and P. Slovic. 1983. The nature of technological hazard. *Science* 220, no. 4595: 378–84.
IPCS, and WHO. 2004. *Risk assessment terminology*. Geneva: WHO.
Lehmann, D. 1996. Generalized qualitative probability: Savage revisited. In *Twelfth conference on uncertainty in artificial intelligence*, ed. E. Horvitz and F. Jensen, 381–8. Portland, OR: Morgan Kaufmann.
Luhmann, N. 1990. *Risiko und Gefahr* [Risk and danger]. St. Gallen: Hochschule St. Gallen.
McCarthy, J., O. Canziani, O.N. Leary, D. Dokken, and K. White. 2001. *Climate change 2001: Impacts, adaptation and vulnerability. contribution of working group II to the third assessment report of the IPPC* Book section: Summary for policy makers. Cambridge: Intergovernmental Panel on Climate Change.
Merriam-Webster. 2002a. 'vulnerable'. *Webster's third new international dictionary, unabridged*. http://unabridged.merriam-webster.com (accessed November 22, 2010).
Merriam-Webster. 2002b. 'hazard'. *Webster's third new international dictionary, unabridged*. http://unabridged.merriam-webster.com (accessed November 22, 2010).
Miller, F., H. Osbahr, E. Boyd, F. Thomalla, S. Bharwani, G. Ziervogel, B. Walker, et al. 2010. Resilience and vulnerability: Complementary or conflicting concepts. *Ecology and Society* 15, no. 3: 11.
Otway, H., and D. Vonwinterfeldt. 1992. Expert judgment in risk analysis and management – process, context, and pitfalls. *Risk Analysis* 12, no. 1: 83–93.
Paustenbach, D.J., ed. 1989. *The risk assessment of environmental and human health hazards: A textbook of case studies*. New York, NY: Wiley.
Paustenbach, D.J., ed. 2002. *Human and ecological risk assessment. Theory and practice (Foreword)*. New York, NY: Wiley.
Polsky, C., R. Neff, and B. Yarnal. 2007. Building comparable global change vulnerability assessments: The vulnerability scoping diagram. *Global Environmental Change* 17, no. 3–4: 472–85.
Renn, O. 2008. *Risk governance: Coping with uncertainty in a complex world*. London: Earthscan.
Resilience Alliance. 2009. Assessing and managing resilience in social-ecological systems: A practitioner's workbook. http://www.resalliance.org/index.php/resilience_assessment.
Scholz, R.W. 1987. *Cognitive strategies in stochastic thinking*. Dordrecht: Reidel.
Scholz, R.W. 1991. Psychological research in probabilistic understanding. In *Chance encounters: Probability in education*, ed. R. Kapadia and M. Borovcnik, 213–54. Dordrecht: Reidel.
Scholz, R.W., and M. Siegrist. 2010. Low risk and high public concern? The cases of persistent organic pollutants (POPs), heavy metals, and nanotech particle. *Human and Ecological Risk Assessment* 16, no. 1: 1–14.
Scholz, R.W., and O. Tietje. 2002. *Embedded case study methods: Integrating quantitative and qualitative knowledge*. Thousand Oaks, CA: Sage.
Shafer, G.A. 1976. *A mathematical theory of evidence*. Princeton, NJ: Princeton University Press.
Tversky, A., and D. Kahneman. 1992. Advances in prospect-theory – cumulative representation of uncertainty. *Journal of Risk and Uncertainty* 5, no. 4: 297–323.
Vlek, C., and P.J. Stallen. 1980. Rational personal aspects of risk. *Acta Psychologica* 45: 273–300.
Walker, B. 2009. Specified and general resilience. http://wiki.resalliance.org/index.php/1.5_Specified_and_General_Resilience (accessed October 5, 2009).
Walker, B., S. Carpenter, J. Anderies, N. Abel, G. Cumming, M. Janssen, L. Lebel, J. Norberg, G.D. Peterson, and R. Pritchard. 2002. Resilience management in social-ecological systems: A working hypothesis for a participatory approach. *Conservation Ecology* 6, no. 1: 17.
Walker, B., and D. Salt. 2006. *Resilience thinking: Sustaining ecosystems and people in a changing world*. Washington, DC: Island Press.
Walley, P. 1991. *Statistical reasoning with imprecise probabilities*. London: Chapman and Hall.