

## **Respiratory Protective Equipment and the Management of Risk: Where Safety and Security Diverge**

Stevyn D. Gibson

Department of Defence Management and Security Analysis  
Royal Military College of Science, United Kingdom Defence Academy, Cranfield University  
Shrivenham, SN6 8LA United Kingdom  
s.gibson@rmcs.cranfield.ac.uk

### **ABSTRACT**

**T**he management of risk is witnessing the emergence of a new risk category – security. Like safety, security draws significantly upon the collective theory, philosophy and methodology of risk. Unlike safety, much of the risk managed by security practitioners emanates from deliberate, malicious human intervention rather than accident or negligence. The nature of security risk is uncertain and ambiguous rather than merely complex. Whereas safety risk is largely bounded by routine interaction with contemporary society, security risk remains unbounded. Security is unsuited to the scrutiny of pure science alone; rather it necessitates a reflection that incorporates the ‘dual nature of risk’ concept as both an objective reality as well as a social construct. In this new context, security, as a manifestation of contemporary society, is looking for new understanding and new approaches from and by all members of the “security commons”. Security risk management is a coping strategy rather than a solutions strategy. respiratory protective equipment is no exception.

**Keywords:** Risk management, safety, security, postmodernism, terrorism, RPE

### **INTRODUCTION**

**T**he world of risk is extremely diverse; environmental risks (man-made or natural), financial risk, political risk and commercial risk might form a taxonomy. Strategic, operational, tactical and technical might be another. The varieties and classifications are endless to such a degree that all we can be sure of is that there is a galaxy of risk out there. Risk, whatever its form, is at least uniformly defined as the product of the likelihood, ‘p’, of some future event and the impact of that event, ‘I’. In plain English, risk is the likelihood or probability of suffering future harm, loss or danger. Risk is more often associated with a negative or downside rather than a positive or opportunity. This common perception reflects society, particularly Western society, in the postmodern world<sup>1</sup>. It is always worth reminding students of risk and practitioners of risk management that much of the progress of the modern world (post-Enlightenment through industrialization) was achieved by the undertaking of significant risk in order to create and derive benefit and exploit opportunity. However, increasing complexity, litigation, political correctness, the influence of the media and human rights, the latter seemingly in ascendance over human responsibilities, are collectively militating against risk-taking for mankind’s benefit. Risk cannot be nullified either by

---

<sup>1</sup> The ‘postmodern world’ and ‘postmodernism’ are terms used in the literature that essentially refer to the world we live in today. As such the term ‘postmodern’ can mean different things to different people. Here it is simply meant to reflect contemporary society as distinct from industrial or ‘modern’ society, which went before.

reducing its likelihood (p) or by mitigating its consequences (l). That is not to say that we should not attempt to drive risks towards zero when harm or danger may be present. It is to say that perfect solutions are few and far between and that progress and success should be measured by how far we can drive negative risk towards zero rather than its absolute measure.

This paper has been deliberately written as a discussion paper rather than a scientific paper per se. It introduces an evolving context for the management of risk, where science and technology can now only hope to form part of the management process for complex, uncertain and ambiguous risks. It introduces the increasingly difficult trade-off and risk-benefit balancing acts that security risk managers struggle with in this context. Their ability to measure and manage through quantification, experiment or modelling (to mention a few techniques), become increasingly illusory and subjective in a field where the human condition, philosophically, psychologically and ideologically, is as important for determining impact as the nature of the impact itself. It takes respiratory protective equipment (RPE) as a case in point to demonstrate the tension between the innovation, development and application of many technologies that arise for societies in terms of the management of security risk. By implication, it asks the question – how safe is safe enough? It equally implies, in the absence of a science to measure the totality of these evolving risks, that new responses might be determined by consensual negotiation beyond baseline standards. What security managers are keen to avoid is being able to answer that question with certainty only when it is too late!

## POSTMODERNISM AS CONTEMPORARY SOCIETY

During the course of the last 15 years, which saw the collapse of the Soviet Union, the removal of the Cold War's bi-polarizing world influence, and the more recent terrorist attack of 9/11, as much an attack on the perceived ends of globalisation as on America, the world has transitioned from the modern to the postmodern (Rathmell, 2002). Postmodernism is characterised not only by the collapse of communism, the release of tribalism, ethnic conflict and the emergence of global, disruptive terrorism but also by the explosion of information, the all-pervading Internet, the ease of travel, the collapse of borders and the first worrying signs of the demise of the concept of the nation state and its attendant mainstays of democracy, trust and freedom (Barber, 1995; Huntington, 2002). In short, life for many, certainly in the developed world, has become complex, fast, interdependent and uncertain; more than it has ever been. Atlee refers to this combined effect as 'complexxity' with intentional 'xx' for emphasis (2003). Postmodernism has introduced risk to society to such a degree that its management has become almost mandatory for individuals, organizations and societies alike to undertake.

Postmodernism travels under many pseudonyms from Ulrich Beck's "risk society" to Slovic's "post normal science" to Fukuyama's "posthuman future". They all imply a change in the conduct and order of society and specifically note the technological spin-offs from science that are affecting that change (Beck, 2001; Fukuyama, 2002; Slovic, 2000). The best analogy is a deck of cards being thrown into the air, which remains hanging in suspension. There is much guesswork going on as to how they might ultimately land - but landed they have not.

So much for the context in which risk, (particularly security risk) managers find themselves in today. The tools at their disposal range along a spectrum of response from purely scientific, where data and knowledge is abundant as in nuclear power, to a "quick and dirty" response, where knowledge is weak but protection is urgent as in nuclear materials proliferation or the spread of the SARS virus. In the latter group the 80/20 Pareto principle will suffice until science and knowledge can catch up.

## RECOGNITION OF DIVISION

Following 9/11, the journal of Risk Analysis, the world's leading risk management journal, devoted several issues throughout 2002 to the discussion of traditional quantitative scientific risk analysis tools being applied to the new and disruptive risk of global terrorism. Collectively they made two conclusions that seem pertinent to the management of risk for RPE. First, they began to recognise a distinction between issues of safety and security. Second, they recognised that the application of risk-analysis methodology, tools and theory was inadequate to deal with this new species of risk.

Slovic, quoting Erikson, who throughout the 1990s referred to a "new species of trouble" as "unbounded" and "unending" where early accidents in the chemical and nuclear industry were concerned, characterised post 9/11-terrorism as a new species of trouble straining the capacity of quantitative risk analysis (2002). "Our models of the hazard generating process ...are too crude to permit precise predictions of where, when and how [a] new attack might unfold," he states, adding the question: "What is the role of risk analysis when the stakes are high and the uncertainties are enormous?" He suggests that: "risk analysis should be supplemented by 'vulnerability analysis'", which characterises the forms of physical, social, political, economic, cultural and psychological harms to which individuals and modern societies are susceptible.<sup>2</sup> He further identifies the need to recognise and incorporate the phenomenon of 'the social amplification of risk' first recognized by Kasperson *et al.* (1988). This conceptual framework explains why some events have enormous effects extending beyond their immediate direct impact. In the 1995 Tokyo subway attack twelve people died but several hundred people presented themselves for treatment for chemical poisoning, many of whom had absolutely no symptoms whatsoever rather displaying the phenomenon of 'mass-sociogenic' illness, which they had manufactured in their own minds (Hyams *et al.*, 2002).

Kunreuther refers to 9/11 as having "raised a set of issues regarding how we deal with events where there is considerable ambiguity and uncertainty about the likelihood of their occurrence and their potential consequences" (2002). Like Slovic, he refers to the imperative in dealing with the social amplification of risk created by issues of risk perception, risk communication and trust.

The 'triplet definition' of risk, defined by Kaplan and Garrick in 1981, roots quantitative risk assessment in answering three questions: what can go wrong, what is the likelihood of that happening and what are the consequences if it does happen (1981)? Garrick further argues that this triplet definition remains viable for terrorist events just as it remains viable for all low probability and high consequence events (2002). However, he adds: "The difference comes from the fact that a facility accident is an inadvertent event whereas a terrorist act is an intentional act." He advocates a change from purely quantitative methods of risk assessment to methods that ask the question 'how can **we make** it go wrong' utilising scenario building techniques and vulnerability analysis, which reflect not only the likelihood of occurrence but also the **reality** of that likelihood [emphasis added].

Finally, Deisler concludes that formal risk analysis has a role in managing the consequences of terrorist attack, but: "What it cannot do is assist in the development of that ultimate tool of risk management – the reduction to insignificance of the source of the threats" (2002). He argues that risk management needs to be broadened out to incorporate political, diplomatic and socio-cultural dimensions of risk in order to improve decision-making processes as well as broadening the scope of risk analysis.

---

<sup>2</sup> Risk assessment matrices like CARVERS (criticality, accessibility, recuperability, vulnerability, effect, recognizability and shock) are being used to create 'soft' subjective measures of risk through benchmarking, where quantification is considered difficult to impossible.

## COMPLEXITY, UNCERTAINTY AND AMBIGUITY

It is worth pursuing the changing nature of risk set in the context of the changing nature of global society. This has been brought about by the various but colluding facets of postmodernism described above. It has also arisen through recognition by the cognoscenti in the risk analysis community that their object of analysis – risk – has expanded, compounded and become uncertain and ambiguous beyond the merely complex that current methodology and practice does address.

Many distinguished academics of risk theory refer to the 'dual nature' of risk that revolves around the discrepancy between the perception of a risk and its reality (Adams, 1995). It is a debate between pure, objective scientists utilizing quantitative, laboratory controlled experimentation where every alteration of variables is rigorously controlled versus social scientists utilizing rich, qualitative case studies, where interference with real-life process is frowned upon. Like the nature versus nurture discussion the answer lies somewhere between the two if not intuitively a combination of the two. But society likes and approves of evidence whatever its origin. Evidence, particularly when conducted through independent research, engenders trust. Regrettably, science, whether purist or social in origin, consistently fails to live up to the perfection that is expected of it and the management of risk to which science has applied itself can no more nullify risk than anyone else. It can however go some way to reducing it where appropriate. Following the debate on terrorist risk, Renn and Klinke elucidate a catch-all taxonomy that characterises risk as predominantly one of three categories: complex, uncertain and ambiguous (2002).

Complexity is the easiest to manage; science can be employed to deliver much of the remedy in this department. The bogeymen of the 1970s and 1980s – nuclear power and the chemical industries respectively – have been tamed by complex, scientific risk management procedures.

Ambiguous risk is more difficult to deal with and is best exemplified by debate over the risks of such technologies as genetically modified organisms (GMOs), cloning and gene therapy or activities such as smoking. In these cases the argument over the scientific data is not in question rather the interpretation of the same data by varying scientists diverges and is the cause of ambiguity when interpreted by the objects of that risk, particularly the public. In some cases the bias of the scientist is transparently obvious and questionable as they are hired in the name of independence by opposing sides in the debate. This disagreement creates further confusion for the public perception of these risks, which in turn is reinforced by poor dissemination of information, the information gap being filled by the media and an attendant reduction in trust between the scientific community and the public at large. Slovic has further shown that a defence based on the assumption that scientists know best and the public is ignorant is no longer credible (2000). He has repeatedly demonstrated in psychometric experiments that there is little or no significant difference between public perception of risk and 'expert' perception of that same risk. People continue to smoke knowing that it is killing them in one of several ways.

Uncertainty is the most difficult risk class to manage. Here not only is the science that underlies the quantification or qualification of risk unclear and difficult to measure but also its interpretation, as a result, is open to question. The assessment of the risks of terrorism, nanotechnology or pandemic viruses currently place themselves firmly in the uncertain category. The knowledge base is weak and the data available or collected is poor or difficult to obtain in the first place. Finally, Renn points out that risk does not sit neatly into one of these categories but displays symptoms of all three – complexity, uncertainty and ambiguity (2002).

The conclusion that theoreticians of risk come to is that risk management strategies divide into three generic approaches roughly but not exclusively corresponding to complex, uncertain and ambiguous (Stirling, 1999). Complex risk can simply be treated by scientific and technological intervention. Here measures might include numerical thresholds such as safe working loads, exposure

limits and standards. Where uncertainty is present, risk managers tend to adopt the 'precautionary principle' or 'resilience' measures. Here techniques might include 'containment' efforts, constant monitoring or diversification until greater knowledge is brought to bear upon the issue. Where ambiguity is present, there is a growing use of deliberative discourse techniques to achieve consensus. These might include group Delphi techniques, negotiated rule making and citizen juries. It is interesting to note that Denmark convenes a Citizen Council of 15 members once or twice a year to deliberate and contribute to the formation of national policy where the issues are concerned with the impact of major technological development (Atlee, 2003).

## **RISK MANAGEMENT: SAFETY AND SECURITY**

**H**aving defined risk as the product of an event's future likelihood and impact it is worth defining both the process of its management and two particular fields of risk management - safety and security. Risk management is a process not an objective. There is no final solution just evolution and continual change. The risk manager can never say that he/she has finished; that would be to mis-read the world in which he/she lives. The process is circular from risk identification through assessment, treatment and control – little different from the management process itself. Having derived a risk control method the process is iterated.

Safety as a risk management discipline emerged from the social deprivation of industrial Britain and matured through the nuclear, chemical and manufacturing advances of 20<sup>th</sup> century America. Much of the quantitative risk analysis techniques that all risk managers employ today is derived from the pioneering statistical-based scientific work of the American nuclear industry of the 1970s. By contrast security is a recently emerging risk management field. In some parts of the developed world, notably continental Europe there is no vocabulary to even distinguish the two risk categories. The French, German, Spanish, Italian and Russian words for security are the same as the word for safety (sécurité, Sicherheit, seguridad, sicurezza and byezopasnost respectively). However, intuitively and instinctively a distinction has formed. In Anglo-Saxon regions of the world from the United States through Great Britain to Australasia very real and practical differentiation has been made, the main drivers being the impact of terrorism and to some degree legislation and regulation. Both disciplines derive their theory, principles and processes from the world of risk but the risks they have to deal with are very different.

Security like safety is both a process and a product. The process utilizes the philosophy and methodology of risk theory to create a product or ontological state in which one can enjoy a level of safety or security. Both are defined as a relationship between an asset, a protection and a threat. Without all these three present and interacting there is neither a process nor a product of security or safety. The great distinguishing feature of the two is that whereas safety risks emerge unintentionally and accidentally, even when engendered by human intervention, security risks are caused by deliberate and malicious human intention (Gibson, 2003).

Here the two worlds of safety and security part company. Safety is concerned with managing the risks created by largely benign, well-meaning interventions. The manifestation of these interventions themselves being products and processes designed to enhance life rather than deliberately disrupt and destroy it. Security by contrast is forced to deal with the downside of human intervention, quite often deriving from the very progressive technologies delivered with the intention of enhancing life.<sup>3</sup> The machinations of a devious, cunning and resourceful mind are not readily testable in a laboratory environment even if its products were readily submitted for testing. The variables that contribute to a

---

<sup>3</sup> It is not the subject of this paper but it is worth remembering a middle ground, where the 'enhancing' quotient of enhancing technologies depends upon the context from which you make that judgment. GM foods would fall into that category at present.

security risk are difficult enough to identify left alone assess. The security risk manager is usually dealing in unknowns, half-truths and best guesses. There is considerable effort underway to bring the scientific method, enjoyed by safety risk managers, to bear upon security risks but the likelihood and impact aspects of security risks are far more difficult (p) and unbounded (I) to assess than safety risks. On another philosophical level, the root causes of security risks, whether criminological or terrorist in origin are being studied in order to tackle the issue at source as another dimension to managing those risks. But by far the greatest work is being done on the impact side of the security risk equation. While likelihood, p, of a terrorist event can be more fully understood it is the most difficult aspect to manage. Consequently, the impact side, I, is more readily mitigated by security risk management processes and products such as business continuity management or consequence management programmes.

The security approach to risk management has a further disadvantage when compared to safety. It has yet to achieve the maturity enjoyed by safety and the manifestations of that maturity represented by widespread legislation, regulation and scientific application. In some respects it is catching up fast and in other respects it should deviate along a different route. The fork in the road, once again, centres on the issue of intent - accidental or deliberate. In the latter the moving parts that constitute the risk are constantly changing, devious and malicious. They do not subject themselves to the norms of civilized society: the law, regulation, audit or corporate governance. Consequently, the response, if it is to manage a security risk, must at least acknowledge that fact and when looking for solutions be cognizant of what it is up against.

The security world is desperate for the means by which it can reduce the risk equation, both theoretical and practical. The "security commons": public sector, private sector, academic, non-governmental organisations (NGOs) and citizens each have a role to play in identifying solutions (Steele-Vivas, 2000). That is not to say that reducing the risk equation by any means is acceptable - far from it. Perfection has often been sacrificed in design standards. It is saying that regulation and acknowledgement of the changing nature of risk and the emergence of security risk in a class of uncertainty beyond safety risk is vital to managing this new breed of risk. Having recognized this distinction, then the norms of civilized society (e.g., legal, social, cultural, practical, regulatory, and so on) must adapt to the new circumstances in which risk managers must operate. The security world will catch up with the safety world and match it where it can but it will never coalesce or be the same because the root causes are fundamentally and significantly different.

## RESPIRATORY PROTECTIVE EQUIPMENT

RPE is a good example of the modern world transiting to the postmodern, of post-normal science having to deal with the dual nature of risk and of the competing and sometimes conflicting needs of safety versus security. One of the main aims of both security and safety practitioners is to save life. It's a self-evident and noble aim. Both want to save more life tomorrow than we can today. Better processes, new and appropriate technology and a systematic approach can achieve this. But the process towards this improvement will be relative rather than absolute. Where new technology and processes are concerned, the desire to drive down risk and increase security should not be held up by 'bureaucratic' scientists, corralled by a fear of litigation or stuck in the purely quantitative, controlled-variable, laboratory-style approach of the modern world and normal science. Rather it should be enabled by innovative science cognizant of the postmodern world where risk cannot be reduced to zero, extrapolated scientific experiment no longer truly represents the uncertainty of the real world and solutions qua 'coping strategies' should be regarded as important as methodology. This has been eloquently interpreted by Slovic, Fischhoff and Lichtenstein in their interpretation of the question; how safe is safe enough (Slovic *et al.*, 1980)?

The European certification procedures for RPE are a case in point. This paper supports the notion that the claims of RPE should be verified to ensure, in the words of a well-known British product, that "it does exactly what it says on the tin"<sup>4</sup> and that customers (users) can have confidence that specific RPE will do what it claims. However, within and amongst scientists and practitioners of the RPE standards and certification world there seems to be at worst some flaws and at best some points of debate, which themselves reflect much of the wider discussion on the very nature of science, risk and determining what is right for postmodern or contemporary civil society.<sup>5</sup>

Two particular points stand out. First, there is now a body of evidence to suggest that the laboratory testing of RPE, even with its built in safety factors, contrasts significantly with the work-place testing of RPE.<sup>6</sup> Second the approach to create international standards of RPE under the auspices of the International Standards Organisation (ISO), supported by the International Society for Respiratory Protection (ISRP), seems to differ fundamentally from that of the European approach under the auspices of the Comité Européen de Normalisation (CEN).<sup>7</sup> Notwithstanding their relative ages, the former and younger body seems predominantly keen to establish standards that equate to what the human needs to do to perform. The latter and older body seeks principally to establish equipment performance against standard norms.<sup>8</sup> Has the former placed itself more in tune with contemporary societal risks and risk management as coping strategy?

Encroaching on this world, which has been established largely to protect the human being in his/her working environment, is this new manifestation of risk - security risk – although impacting upon the worker in a working environment in a purely superficial and circumstantial way (where else do most people spend their day in the Western world?!), its source invariably emanates from outside that environment and has very little relation to it at all. Following 9/11, the US market is looking for solutions to this new type of risk perceived, however tenuously, as including chemical, biological, radiological and nuclear (cbrn) as well as high-explosive material.<sup>9</sup> To this effect the National Institute for Occupational Safety and Health (NIOSH) standard Part II is drafting product specification with this type of risk in mind in conjunction with the Technical Support Working Group (TSWG – part of the US Department of Defence) who are instrumental in and determined to find solutions (coping strategies) for this new class of risk.<sup>10</sup>

---

<sup>4</sup> The UK advert for Ronseal paint uses this catch phrase.

<sup>5</sup> The manifestation of this debate was witnessed personally by the author at the First International Conference for PPE quality compliance in Moscow, September 2003.

<sup>6</sup> Lecture by Mr Robin Howie of Robin Howie Consultants to the First International Conference "Procedures of Assurance of Personal Protective Equipment (PPE) Quality Compliance in the EU and Russia." 4-5 September 2003. Moscow.

<sup>7</sup> Lecture by Mr. Goran Berdtsson, President of the International Society for Respiratory Protection (ISRP) to the First International Conference "Procedures of Assurance of Personal Protective Equipment (PPE) Quality Compliance in the EU and Russia." 4-5 September 2003. Moscow.

<sup>8</sup> I am grateful to the referees who point out the distinctions between standards bodies and certification (notified approved inspection) bodies. These distinctions will be well known to readers of this journal. The author simply takes them all in the round as influencers of RPE.

<sup>9</sup> Conversation with the Managing Director, Hazard Management Solutions Limited, which runs a database of global terrorist incidents, which clearly demonstrates to date that the incidence of terrorism utilising high explosive far outweighs those utilising cbrn, whichever measure of impact you can to analyse by.

<sup>10</sup> Having said this, it does seem that both NIOSH and TSWG prefer to recognise a risk management approach when they see one rather than specifying one.

---

## CONCLUSIONS

As new standards for RPE are being considered, there is an opportunity for the three main bodies influencing RPE (CEN, ISRP and NIOSH) to reflect these new risks; the distinction between safety and security risks, new theories about risk management and the wider context of postmodernism, which society itself is grappling to come to terms with, as they draft the new requirements. While there may be internal debate as to what properly and universally constitutes a valid certification process for RPE they should certainly begin to recognise the dual nature of risk that permeates much of risk management in the postmodern world and consider the distinction between safety and security risks. The security risk manager is keen for solutions, qua coping strategies, **now**, which, at least in this author's opinion, will necessarily sacrifice perfection for the time being until science and knowledge can catch up. Security risk managers are not merely managing complex risk but also ambiguous and uncertain risk in an overall effort to drive that risk back towards an acceptable level not an absolute level. They would prefer to choose from imperfect options in the meantime than no options at all.

## ACKNOWLEDGEMENTS

The author is most grateful to the anonymous referees who provided invaluable advice and in particular (independently) supported the idea that it would make a useful debating piece, which was the intention. The opinions and errors are the author's alone.

## REFERENCES

- Adams J. (1995) Risk. London: Routledge.
- Atlee T. (2003) The Tao of Democracy: Using Co-Intelligence to Create a World that Works for All. Cranston RI: The Writers Collective.
- Barber B. (1995) Jihad vs. McWorld: Terrorism's Challenge to Democracy. London: Transworld.
- Beck U. (2001) World Risk Society. Cambridge: Polity Press.
- Deisler PF, Jr. (2002) A Perspective: Risk Analysis as a Tool for Reducing the Risks of Terrorism. Risk Analysis. 22 (3): 405-413.
- Fukuyama F. (2002) Our Posthuman Future: Consequences of the Biotechnology Revolution. London: Profile Books.
- Garrick JB. (2002) Perspectives on the Use of Risk Assessment to Address Terrorism. Risk Analysis. 22 (3): 421-423.
- Gibson SD. (2003) The Case for 'Risk Awareness'. Security Journal. 16 (3): 55-64.
- Huntington SP. (2002) The Clash of Civilizations and the Re-making of World Order. London: Simon & Schuster.
- Hyams KC, Frances MM, Wessely S. (2002). Responding to Chemical, Biological or Nuclear Terrorism: The Indirect and Long-Term Health Effects May Present the Greatest Challenge. Journal of Health Politics, Policy and Law. 27 (2): 273-291.

Kaplan S and Garrick BJ. (1981) On the Quantitative Definition of Risk. *Risk Analysis*. 1(1): 11–27.

Kasperson R, Renn O, Slovic P, Brown H, Emel J, Goble R, Kasperson J, and Ratick S. (1988) The Social Amplification of Risk: A Conceptual Framework. *Risk Analysis*. 8: 177–187.

Kunreuther H. (2002) Risk Analysis and Risk Management in an Uncertain World. *Risk Analysis*. 22 (4): 655-664.

Rathmell A. (2002) Towards postmodern intelligence. *Intelligence and National Security*. 17 (3): 87-104.

Renn O. & Klinke A. (2002) A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies. *Risk Analysis*. 22, (6): 1071-1094.

Slovic P. (2000) *The Perception of Risk*. London: Earthscan.

Slovic P. (2002) Terrorism as Hazard: A New Species of Trouble. *Risk Analysis*. 22 (3): 425-426.

Slovic P, Fischhoff B & Lichtenstein S. (1980) Facts and Fears: Understanding Perceived Risk. In: Schwing, R.C., and Albers, Jr, W.A., eds. *Societal Risk Assessment: How Safe is Safe Enough?* New York: Plenum Press, 181-216.

Steele-Vivas R. (1996) Creating a Smart Nation: Strategy, Policy, Intelligence and Information. *Government Information Quarterly* 13 (2): 159-173.

Stirling A. (1999) On Science and Precaution in the Management of Technological Risks. Final report for EC Forward Studies Unit. Report EUR 19056 EN. Brussels: European Commission. In: Renn, O. & Klinke, A. (2002). op cit.