

MANAGING MAJOR RISKS OF THE FUTURE

As the events of recent years attest, the world has become a more dangerous place. The risk landscape has taken on new contours with the emergence of devastating terrorist attacks on civilian targets, new contagious diseases infecting both humans and animals, hugely destructive natural disasters (notably earthquakes and flooding), and severe disruptions to critical infrastructure such as energy supplies, transport and information systems. But what has also changed are the context in which these new threats are surfacing and societies' capacity to manage them. Globalisation is contributing to these changes in important ways by raising the level of complexity of the challenges and by increasing economic, social and environmental interdependence. This in turn is making co-operation among national governments, as well as between the public and private sectors, all the more crucial.

Emerging risks

In 2003, the OECD's International Futures Programme (IFP) published a report on *Emerging Risks in the 21st Century: An agenda for action*, which focused attention on the vulnerability of many of the vital systems underpinning OECD economies – health, transport, water, electricity, information – and set out a number of recommendations for governments and the private sector on improving the management of emerging systemic risks in the future. Three strands of that work are now being followed up.

Reappraising risk management

The first consists of supporting OECD governments in reappraising their risk management policies. The focus is on the consistency of policies, on their ability to deal with the challenges – present and future – created by emerging systemic risks, and on the opportunities for improvement. To this end, a group of member countries has come together to review selected risk-related policies and, on the basis of concrete case studies, to develop an international risk management “toolbox” and explore the possibilities for applying best practices. It is expected that the case studies will concentrate on a range of threats and vulnerabilities that could prove critical to the functioning of member countries' economies. Thus they are likely to address such themes as ongoing vulnerability assessments for critical infrastructures, security and reliability of power supply systems, prevention of disasters triggered by natural hazards such as floods, and public/private management of large-scale accidents.

Sharing lessons from major disasters

The second strand concerns the need to share lessons to be learned from major disasters. Following a proposal submitted at the March 2003 meeting of the Executive Committee in Special Session, the OECD initiated an analysis of the economic and social impact of recent large-scale disasters and identified lessons for the future. The focus is primarily on restoring trust and securing recovery in the aftermath of disaster. In preparing the analysis, the OECD secretariat has drawn heavily on in-house expertise, pulling together a team of specialists from eight OECD directorates and agencies.

Several policy messages stand out from this work:

- Governments are often not well prepared to handle the economic and social impact of disaster. In addition to the loss of life and human suffering, the damage inflicted on the economy can be huge. It is estimated for example that the economic cost of the terrorist attacks of 11 September 2001 amounted to some USD 120 billion, and that of the 1995 Kobe earthquake was around USD 130 billion.
- The public's trust, as well as consumer and investor confidence, are essential ingredients of recovery. They must be strengthened through credible communication and effective government action.
- Such action often needs to be taken in partnership with the private sector, which has an important role not only in disaster prevention but also in response and recovery. Sharing the burden of mega-risks clearly requires improved public-private interaction (see section on *Catastrophic risks*, page 50).
- Finally, major disasters can have global implications that can easily overwhelm the response capacities of any single country, and therefore call for close international co-operation.

The report was published in Spring 2004 under the title *Large-Scale Disasters: Lessons Learned*.

Impact of increased security activity

The third strand of work under development aims at gaining a better understanding of the broader implications of increased security activity. Organised crime, terrorism, disruption of global supply chains, computer viruses – all have played a role in raising people's awareness of the risks they face in today's world. The result has been the emergence of a USD 100 billion market for security goods and services fed by growing demand from governments, businesses and private households. With globalisation and technological progress continuing at a rapid pace, the security economy is expected to expand further in the years ahead. New identification and surveillance technologies such as biometrics and radio frequency ID are coming on stream, and satellite-based monitoring is set to play an ever greater role. These developments promise to have far-reaching economic and social impact over the longer term. The challenge for policymakers is how to meet the apparent need for greater security without unduly impeding economic efficiency, privacy and other democratic rights.

The OECD is about to publish a first report on these issues entitled *The Emerging Security Economy*. It argues that improving security comes at a cost that falls into two types: the investment needed to put in place the requisite security arrangements; and the second-order impact that the security arrangements may have on the operations of the sector in question or of the entire economy. Tighter security, for example, may mean longer delivery times, disruption of global supply chains and of finely-tuned just-in-time delivery systems.

These frictional costs tend to make trade more expensive and reduce trade flows. Similarly, tougher controls on movements of people across national frontiers can impose delays and efficiency losses. New technologies can help to reduce these trade-offs, but they in turn have potential implications for data protection and privacy concerns. More work is required to gain a better understanding of the complexities of the emerging security economy, of how and when governments should intervene, and which policies deserve priority.