OECD (Ed.); International Transport Forum (Ed.)

Working Paper

Security, risk perception and cost-benefit analysis: Summary and conclusions

OECD/ITF Joint Transport Research Centre Discussion Paper, No. 2009-6

Provided in Cooperation with:
International Transport Forum (ITF), OECD

Suggested Citation: OECD (Ed.); International Transport Forum (Ed.) (2009) : Security, risk perception and cost-benefit analysis: Summary and conclusions, OECD/ITF Joint Transport Research Centre Discussion Paper, No. 2009-6, Organisation for Economic Co-operation and Development (OECD), Joint Transport Research Centre (JTRC), Paris, https://doi.org/10.1787/225674203172

JOINT TRANSPORT RESEARCH CENTRE

Round Table, 11-12 December 2008, Paris

Discussion Paper No. 2009-6
March 2009

Security, Risk Perception and Cost-Benefit Analysis

SUMMARY AND CONCLUSIONS

International Transport Forum

The International Transport Forum is an inter-governmental body within the OECD family. The Forum is a global platform for transport policy makers and stakeholders. Its objective is to serve political leaders and a larger public in developing a better understanding of the role of transport in economic growth and the role of transport policy in addressing the social and environmental dimensions of sustainable development. The Forum organises a Conference for Ministers and leading figures from civil society each May in Leipzig, Germany.

The members of the Forum are: Albania, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Bosnia-Herzegovina, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, FYROM, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mexico, Moldova, Montenegro, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russia, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom and the United States. The Forum's Secretariat is located in Paris.

Joint Transport Research Centre

The OECD and the International Transport Forum established a Joint Transport Research Centre (JTRC) in 2004. The Centre conducts co-operative research programmes addressing all modes of transport to support policy making in Member countries and contribute to the Ministerial sessions of the International Transport Forum.

JTRC Discussion Papers

The JTRC Discussion Paper Series makes economic research commissioned or carried out at the Joint Transport Research Centre available to researchers and practitioners. The aim is to contribute to the understanding of the transport sector and to provide inputs to transport policy design. The Discussion Papers are not edited by the JTRC and they reflect the author's opinions alone.
The Discussion Papers can be downloaded from:
http://www.internationaltransportforum.org/jtrc/DiscussionPapers/jtrcpapers.html
The International Transport Forum's website is at:
http://www.internationaltransportforum.org/
For further information on the Discussion Papers and other JTRC activities, please email:
itf.contact@oecd.org

Security, Risk Perception and Cost-Benefit Analysis

TABLE OF CONTENTS

FOREWORD

This document summarizes discussions at the Round Table on *Security, Risk Perception and Cost-Benefit Analysis*, held in Paris on 11-12 December 2008. The objective of the Round Table was to take stock of expertise on the assessment of risk and insecurity in transport and to consider how this expertise can be used to support project and policy appraisal. The discussions were chaired by Andrew Evans (Imperial College London, UK) and based on four introductory reports, also available as JTRC Discussion Papers, which can be downloaded from the links below:

Rapporteurs:

Dr. Khalid BICHOU (Imperial College London)
http://www.internationaltransportforum.org/jtrc/DiscussionPapers/DP200820.pdf

Prof. Peter GORDON/James. E. MOORE/Harry W. RICHARDSON (University of Southern California, USA)
http://www.internationaltransportforum.org/jtrc/DiscussionPapers/DP200822.pdf

Prof. André de PALMA (École Nationale Supérieure, Cachan, France)
http://www.internationaltransportforum.org/jtrc/DiscussionPapers/DP200821.pdf

Dr. Robert POOLE (Reason Foundation, USA)
http://www.internationaltransportforum.org/jtrc/DiscussionPapers/DP200823.pdf

1. INTRODUCTION

Security concerns are high on the political agenda in many countries because of the widespread perception that security is increasingly threatened by intentional malicious acts including terrorist attacks. While terrorism has a long history and measures to maintain and improve security are in place, major events – including but not limited to the 9/11 attacks – have triggered stronger action to improve security. In this context, much attention goes to maintaining secure transport for two reasons. First, many transport facilities and vehicles are appealing targets for terrorist attacks because of the concentration of potential victims. Second, transport can act as a conveyor for terrorist attacks, e.g. by moving weapons into ports or by turning airplanes into weapons. In both cases, the difficulties in protecting the many potential targets while maintaining smooth transport operations strengthens the appeal of transport targets.

The costs of potential damage from terrorism are substantial but so are the costs of improved security. Careful policy appraisal can help make good use of scarce resources. This paper, which is drawn from debates during the round table on "Security, risk perception and cost-benefit analysis", held in Paris in December 2008, investigates how economic analysis can contribute to the design of policies to maintain or enhance security in transport. A standard economic approach to policy design is to evaluate the costs and benefits of various policy options ("projects"). In order to make sense, a project's benefits should exceed its costs, and when choosing between alternative approaches, ranking alternatives according to their net benefits helps inform policy decisions. However, cost-benefit analysis has difficulty dealing with security issues, mainly because the benefits are uncertain or at least extremely hard to quantify. As is discussed in Section 2, the basic problem is that it is hard to determine the probability of terrorist attacks in an objective manner. Subjective probabilities are available, but here the question is how they can be best determined. Section 3 provides an overview of some methods to establish reasonable probability assessments for use in policy appraisal. Obviously, the design and implementation of security policies moves forward whether a full-fledged cost-benefit analysis is available or not. Can economic analysis be of use? Section 4 addresses this question. At least two types of useful input can be thought of. First, economic analysis can help establish whether policies attain their objective at least possible cost. Second, careful economic modeling can chart the direct and indirect impacts of attack scenarios, and this information is of obvious relevance to the definition of policy priorities. Gordon *et al.* (2008) emphasize that, if the goal is to rank targets in terms of impacts, there is a need for analyzing specific scenarios rather than defining generic targets.

On the basis of the discussion of how economic analysis can help design responses, Section 5 examines what broad response strategies are available, and how useful they are or could be. Sections 6 and 7 deal with aviation security and maritime security, mostly from a cost-effectiveness point of view. This approach assesses if policies are well-designed in the sense of reaching their stated goal, however defined, at the lowest possible cost to society. While judging the effectiveness of a policy is very difficult if it is unclear how it would affect the probability of an attack, it is sometimes possible to judge if the mechanisms employed to

produce a given "security product" are the best available ones. Where such analysis has been carried out, the results tend to be critical of current practice. Poole (2008), for example, argues that aviation security as currently produced in the US, could be provided at lower cost or – alternatively – better procedures could be provided with the same budget. For maritime transport, there is considerable consensus that current initiatives are at best weakly effective. In both sectors, policies appear to be inspired more by the need to show initiative than anything else. Section 8 concludes.

2. THE NATURE OF TERRORIST THREATS

The practice and analysis of security problems in transport is often inspired by work on transport safety. However, safety and security are fundamentally different issues, because safety is associated with risk while security is associated with uncertainty. In the case of risk, e.g. accident risk, the events are unintentional and their likelihood can be reasonably estimated from empirical observations. But the probability with which intentional events that cause security concerns will occur is much harder to quantify, for two reasons. First, terrorist attacks are relatively infrequent. This is especially true of attacks that belong to the class of extreme events, with low probabilities, major consequences, and possibly spillovers into connected systems[1]. For such infrequent events, past events carry little information on future probabilities.

Second, attaching probabilities to intentional acts is particularly problematic because of the possibility of strategic behavior: terrorists adapt their strategy to changes in the security environment in which they operate. Since little is known about how they will respond (because the set of available strategies is very large), it is not clear how security policies or other relevant changes affect attack probabilities. In sum, terrorist attacks are not characterised by risk but by uncertainty, meaning that no credible objective probability can be assigned to their occurrence.

Given this difficulty, the question is how reasonable probability assessments to support security management can be obtained. Attempts to establish subjective probabilities use a variety of methods, including reliance on intelligence and expert opinion (see Section 3). The challenge is to arrive at the best possible subjective probabilities, i.e. those that make the best use of available information ("best-information subjective probabilities"; BSP). The BSP are not common knowledge, because of the usual costs of disseminating information, but also because best use of intelligence may require secrecy. For this reason, the BSP may well differ from citizens' subjective probabilities (CSP). There is evidence that, in general, individuals' perception of risk is characterized by risk aversion, misperception of probabilities, and loss aversion. When objective probabilities are unknown, it is unclear whether citizens tend to over- or underestimate the probability of a terrorist attack. However, if the commonly observed characteristics of risk perception apply to the case of security, it is plausible that

[1] The average scale of terrorist attacks is small, but fundamentalist terrorism seeks mass casualties (Sandler and Enders, 2005), a phenomenon that arguably increases transport facilities' appeal as a target.

the probability of infrequent large scale attacks is overestimated compared to the BSP. One question, to which we return below, is should policy be based on CSP or BSP.

3. DETERMINING BEST-INFORMATION SUBJECTIVE PROBABILITIES

There exist various sources of information on probabilities of terrorist attacks, including intelligence services, insurance markets, expert opinion, and public opinion. The issue is how to make best use of these sources for the design of security policy.

Intelligence services gather and interpret information on terrorist activity, so are particularly well placed to form opinions on the likelihood and nature of future attacks. It is, however, less obvious that this information can be used in overall policy design, because of secrecy restrictions, and because the information may be too short-term and microscopic to support strategic policy design. Secrecy requirements pose a principal-agent problem: the principal wants security, and needs to monitor agents' operations to attain that objective, but monitoring is difficult under the secrecy requirement. More broadly, strict secrecy policies create a problem of accountability and potentially of legitimacy. Authorities could argue that policies are justified by the information available to them but which cannot be made public. It is therefore important to limit secrecy requirements to the absolute minimum and to establish alternative sources of information, allowing democratic checks on whether policy choices seem justified on the basis of a reasonable public assessment of security risks.

The insurance industry potentially is one alternative source of information. Private underwriters have been attaching probabilities to a wide range of attack scenarios since the 1970s, for the purpose of issuing terrorism risk coverage. The underwriters combine historical records with intelligence and industry experience to assign probabilities. The number of underwriters is small (though reportedly growing), and information on their assessments of probabilities is commercially sensitive and not in the public domain. Furthermore, evidence presented at the round table showed limited correlation between two underwriters' assessments of probabilities. Interpreting the probabilities is difficult without information on the premiums charged. It appears that the market for this kind of risk is thin. Information on ex post checks of the stated probabilities is not available either. These shortcomings limit the extent to which this market is a source for determining BSP, a shortcoming exacerbated by the potential problem that, because of a lack of transparency and of competition, prices reflect willingness-to-pay, and not just expected costs. Increased transparency and a broader market are required before the industry's probability assessments can be turned into useful public knowledge.

Insurance companies also rely on catastrophe modelling. The approach here is to gather and review intelligence, and to model it systematically, amongst other ways by eliciting judgments on relative risks from experts. Subjective and objective information is combined and made explicit in the form of a sequence of conditional probabilities. There are three large companies that provide this kind of modelling. Insurance companies tend to use all three sources to decide on premiums. Public bodies, such as the Department of Homeland Security, do not rely on these services for decision making, although the information is

accessible to them in principle. One potential explanation is that public bodies have access to information they think to be better. Another possibility is that assessments provided by private insurers usually are industry or transport mode-specific, so do not provide ideal guidance for deciding on the general (public) provision of security.

In general, public and private provision of security and security insurance are complementary. Some security risks are too large or too strongly correlated to be covered by the private sector (as diversification is difficult), so justifying public intervention, and some are hard to monetize,. Public provision of security may induce positive spillovers by reducing the amount of coverage that needs to be provided privately. Oversimplifying somewhat, one might argue that public policy should focus on improving overall security, while private initiatives are better suited to managing risk at the level of specific targets. However, target-specific risk management is fraught with problems. First, there is the possibility that better management at one target just shifts risk to other targets, with little or no improvement of overall societal security (see Section 5). Second, individual operators' measures to improve security do not necessarily lead to lower insurance premiums, because insurers fear "contamination" of more secure companies by less secure companies. The World Customs Organisation Authorised Economic Operators program and the US C-TPAT program in maritime transport can be mentioned as examples: operators in compliance with the requirements of these programs are not offered cheaper insurance. These problems again highlight the need for coordinated public involvement in terrorism insurance.

Lastly, prediction markets could conceivably generate good information on subjective probabilities. Prediction markets involve participants betting on outcomes. This offers the advantage of including a real financial incentive. Such markets can reveal "the wisdom of the crowds" (Surowiecki, 2004), and under certain conditions the aggregation of assessments made by independently deciding individuals outperforms the assessments of the separate individuals and possibly of individual experts. The main conditions are that there is diversity of opinion in the crowd (generated by different availability of information or different interpretation of the same information) and that individuals independently make up their mind. Experts may miss relevant issues that affect probability under scrutiny, especially when working in strongly centralized environments.

Whether to base economic analysis of security-management (in as far as such analysis is feasible, see Section 4.) on CSP or on BSP is a matter of judgment. One view, in line with welfare economics, is that consumers' evaluation of policy effects, based on CSP, is what matters. The other view is that in these matters government knows best (in technical terms, security is a merit good), so that BSP is relevant. A practical approach is to evaluate measures for both types of probability assessment, and present results for both cases to policy-makers.

Summarizing, while there are several valuable sources of information for establishing subjective probabilities, all have their shortcomings, and systematic approaches to aggregating and disseminating information are lacking. This compromises the general public's capacity to assess security threats and the responses to them. If as may well be the case, threats are overestimated, this may imply acceptance of rather costly policies, even if they are not very effective.

4. ECONOMIC ANALYSIS TO SUPPORT SECURITY POLICY DESIGN?

Economic analysis aims to contribute to good policy-making through systematic analysis of the costs and the effects of various policy approaches. Ideally, effects are measured in terms of benefits, so that costs and benefits can be compared and net benefits calculated. Clearly, the presence of uncertainty poses difficulties for quantifying the benefits of deterrence strategies, as it makes the impact of deterrence on probabilities extremely hard to determine[2]. Not only does uncertainty pose problems for determining the benefits of a program, it also compromises the capacity of analysis to determine how effective a program is in attaining its stated goals. That is, judging the effectiveness of security policy is hard when the counterfactual (i.e. what would happen in absence of the policy) cannot be determined.

Against this background, an extreme view is that the risk management paradigm and economic analysis in general are not suitable for the support of security policy, as it is not feasible to determine reasonable attack probabilities, the modelling of impacts is too sketchy to be useful, and it is not possible to say how effective measures are in reducing threats. Under these conditions, pursuing a quantitative assessment may lead to the adoption of measures that infringe on civil liberties or are otherwise poorly legitimated, while their benefits are questionable[3].

While the concern underlying this extreme view is widespread, few subscribe to the view that quantitative analysis is useless. If ways can be found to communicate the uncertainties underlying quantitative assessments, then such analysis can help policy-makers decide on their course of action. The tools used also provide a framework for thinking about the issues, i.e. the process is of value, not just the output, amongst other reasons because the tools are consistent. Ultimately, of course, no analysis as such commits anyone to a particular way forward.

Uncertainty imposes modesty on how much guidance economic analysis can provide, but useful contributions are possible if the presence of uncertainty is explicitly accounted for. Given the lack of precise information on probabilities, decision-making analysis ought to work with ranges of probabilities under which some or other course of action is chosen. The robustness of programs, i.e. their effectiveness under different assumptions on future events, is also a useful indicator of their performance. Alternatively, if there is no information on probabilities, one can determine what change in probabilities would be required to justify the costs associated with some program. This at least forces decision-makers to be explicit on why the program is expected to produce projected changes in threat levels.

---

2 Given the imperfect assessment tools, one might also say that the impact of security measures on trade and other components of welfare is uncertain, so that deciding on security policies involves trading off different uncertainties.

3 Note that it was argued in Section 3 that similar problems may arise in the absence of economic analysis.

A somewhat less ambitious approach is to carry out economic impact analysis, that is attempt to trace the economic effects of a given attack scenario, where the scenario and the probability with which it occurs are exogenous. Gordon *et al.* (2008) discuss the principles underlying the modeling of the economic impacts of attack scenarios, and provide some examples. They emphasize that, if the goal is to rank targets in terms of impacts, there is a need for analyzing specific scenarios rather than defining generic targets: analysis needs to focus on a specific port, airport, or other potential target, not on an abstract target. Furthermore, the assessment needs to be spatially disaggregated, looking at business interruption effects at sub-national and sub-metropolitan levels, as the main policy interest is at those levels. The tools discussed in Gordon *et al.* (2008) focus on short run impacts and do not allow for price adjustments. Economic impact analysis is not cost-benefit analysis: it helps in determining priority rankings for target hardening (an important component of current security policies, see next section), but does not offer a framework for comparing costs and benefits.

While most experts subscribe to the view that models are useful in supporting policy, some warn against the use of overly complex and data-rich tools. Given the uncertainties associated with security, simple models are likely to be more structurally stable than complex tools, implying that they are better suited for a forward-looking analysis. The lack of precise answers coming from such simple but stable models reflects the uncertainties underlying the analysis. Any precise statement on what to do, whatever its source, is suspect given the structural uncertainty that characterizes security problems. Given the nature of terrorist threats, there is no way to define how to respond optimally under all circumstances. Responses will need to adapt on a continuing basis. Presumably, then, the role of economic analysis is to make current security policy less bad, and to avoid the biggest mistakes. From this point of view, the next sections discuss broad policy responses as well as aviation and maritime security measures.

5. BROAD TYPES OF RESPONSES TO TERRORIST THREATS: SENSITIVITY, TARGET HARDENING, ADAPTATION

Terrorism can be seen as a violent response to prevailing patterns of economic, social and cultural interactions (institutions), by groups that see themselves – for good or for bad reasons – as disadvantaged by those patterns. While one dislikes the type of response, it is worth asking what can be done to change the perception of disenfranchisement. De Palma (2008) calls for such "sensitivity" in our attempts to manage the future, and suggests that institutional change is a key component of a credible strategy for managing terrorist threats in the long run. In a similar vein, Sandler *et al.* (2008) argue that improved international cooperation and reorientation of international policy-making produces net benefits[4]. Clearly, standard economic tools, such as cost-benefit analysis, are of very limited

[4] ASPI, 2008, criticizes Sandler *et al.* (2008) for considering too limited a set of policy options, ignoring psychological costs of terrorism and potential co-benefits of counter-terrorism spending, and notes there is little explicit evidence for the connection between US foreign policy and transnational terrorism.

use when thinking about institutional change. They are too imprecise to put reasonable numbers on the costs and benefits of such broad strategies, and are indeed not designed for the purpose. Democratic societies use different mechanisms to arrive at decisions on such broad policy directions.

Independent of the extent to which institutional change is pursued, societies will respond to prevailing security threats in some way or other. Target-hardening is a response that aims to make it harder for terrorists to strike against selected targets. A fundamental problem with this strategy concerns the selection or prioritization of targets, given the multitude of potential targets and terrorists' flexibility in responding to any set of measures. Target-hardening ideally should be flexible and dynamic rather than attempt to build walls around selected targets, but current practice deviates strongly from this ideal.

Even under ideal conditions, many think that target-hardening is fundamentally not very effective and therefore a losing strategy, except possibly in terms of political window-dressing. Sandler *et al.* (2008) find the net benefits of most target-hardening measures to be negative, with costs exceeding benefits by a factor of 10 or so. The main reason for this limited effectiveness is that terrorists can easily adapt to policies given the multitude of potential targets. The extreme position is that target-hardening shifts probabilities among targets but does not reduce the aggregate probability of an attack at all. Not all experts subscribe to this view, however, on the argument that terrorist organizations do perform a risk-management calculus, so can be influenced by deterrence strategies. Intriligator (2008) supports the conclusion that target hardening has not produced net benefits in as far as it pertains to the security risks posed by past attacks but goes on to argue that the possibility of an attack involving weapons of mass destruction, e.g. nuclear weapons, should not be ignored. Given the potentially very high costs of such an attack, improved security and target hardening may be worthwhile, even if analysis of past events shows that economic impacts were limited and target-hardening not very effective.

To the extent target-hardening is adopted as a strategy, care should be taken to make it a flexible strategy. One way to increase flexibility in security policy is for regulation to focus on outcomes, not on the process. This contrasts with much regulatory practice, which tends to be strongly or entirely prescriptive. For example, in aviation security, Transport Canada decides on the measures to be taken and the implementing agency CATSA, which has the security-expertise, has no flexibility to modify or augment the measures it employs. This separation of responsibilities is important for the governance of security policy but could perhaps be made more flexible by a shift to outcome oriented monitoring of performance. The difficulty with outcome-oriented regulation, however, is that the ultimate product (security) is elusive, so that intermediate goals need to be determined (e.g. percentage of passengers screened) which again risks introducing rigidities in operating practice. The use of "red teams" (personnel that simulate terrorist behaviour to test the workings of defence mechanisms) can be used to measure effectiveness and could perhaps be relied on as the main outcome-oriented control.

Given that reducing incentives to stage terrorist attacks takes a long time and is not likely to be entirely successful, and given that target hardening is far from perfect even in its optimal form, it follows that terrorist threats and the occurrence of terrorist attacks are inevitably associated with current institutions. More prosaically, terrorism is a cost of doing business. A useful third component of a comprehensive response strategy then is to find ways to reduce the impacts of terrorist attacks through adaptation (impact reduction, disaster recovery, responses to emergencies, etc.). This component was not discussed extensively at

the round table, but it is obviously important, and useful insights on system resilience are available from literature on natural disasters (see Rose, 2007, for a conceptual discussion).

In short, responses to terrorist threats involve three types of measure: reduce the incentives to pursue terrorist strategies, protect targets and reduce the impacts in case attacks take place. The following two sections discuss aspects of target-hardening in the context of aviation and maritime transport.

6. RISK-BASED SECURITY MEASURES IN AVIATION?

Poole (2008) argues that a cost-effective air passenger screening policy must be risk-based, and that current policy is only risk-based in name. He proposes a three-tiered system that focuses on detecting dangerous passengers rather than dangerous objects, as is currently done. Up to 50% of travellers would be able to volunteer for registered traveller programs that would involve voluntarily submitting to security profiling. Many frequent travellers would sign up to such systems in order to reduce queuing time at airports. Screening for low-risk passengers would be limited, although random checks would be retained to avoid easy gaming of the system. With this approach, more resources become available for dealing with higher risk categories of passengers, and especially the 1% or less categorised as high-risk travellers. This would permit attaining the same level of security at lower cost, or better security without increasing expenditure.

Distinguishing passengers on the basis of the risk they pose involves profiling. The profiling is intelligence based, so is less prone to perceptions of discrimination than statistical profiling. Good profiling obviously requires good intelligence (how to decide which travellers do *not* pose a terrorist risk?), and agencies that make efficient use of the available information (whereas the US Transport Security Agency currently does not use available FBI materials to perform criminal background checks).

While few experts deny the economic sense of the proposal, some difficulties remain. First, political acceptance of the system may be low, for example because of equity concerns. Second, switching to a risk-based screening system requires changing regulations, a lengthy process that could take up to 10 years according to some. Furthermore, it is not clear that a passenger-oriented approach instead of an object-oriented approach is sufficiently legitimate to be implemented, even if it is more efficient than an object-based approach.

Current aviation security procedures mostly focus on reducing the risk of terrorists boarding planes. It is conceivable that placing separate security checks nearer gates, instead of using a single point of control for all passengers, serves this goal better. However, such a system would reduce security within the airport, which itself may be a target for a terrorist attack.

It was noted that aviation security policies mainly seem to respond to a need “to do something”. Some recent changes in security measures have been labelled “security

theatre", because the measures are quite visible but their effectiveness is questionable. Such an approach seems more in line with policy-making on the basis of CSP, in the sense of attempting to reduce public concerns about security, rather than effectively reducing the probability of attacks. To the extent that reduced concerns improve welfare, such policies entail benefits, but the desirability of such a policy approach can be questioned (see Section 3).

7. SECURITY-MANAGEMENT IN MARITIME TRANSPORT

The maritime transport sector is complex, not very transparent, and by its nature strongly international. For these reasons it is difficult to arrive at a systematic and coordinated approach to the regulation of security (as well as of other issues). An effective framework for security management should be multi-layered, as it needs to address the security of cargo traffic, of vehicles and facilities, and of supply chains. Such a framework does not exist, however: the term "supply chain spaghetti" is sometimes used to refer to the multitude of regulatory initiatives that overlap and possibly contradict each other.

US initiatives on maritime security drive much of the debate on the costs and benefits of maritime security policy. The Secure Freight Initiative receives most attention, with its goal of 100% scanning of US-borne containers by 2012. It is sometimes argued that many emerging security initiatives at ports outside the USA are driven by the fear that doing nothing will make it hard or impossible to export to the USA, not by security concerns as such. This incentive may compromise the effectiveness of the measures that are taken.

At present, 0.1 to 1% of all containers imported into Europe are inspected. For containers exported to the US, the inspection rate is about 2%. 100% inspection is not the best target for a cost-effective security policy. It is not optimal[5] and is probably not feasible. Current inspection rates suggest that supply chain security is more a topic of debate than an observable practice. The approach of scanning containers in itself is subject to criticism, because detection rates are low. Furthermore, bulk and tramp transport is not controlled, while it arguably is as susceptible to carrying bombs and other hazardous material as container traffic.

Bichou (2008) argues that the maritime transport industry as a whole might benefit from improved security management through improvements in operating efficiency triggered by it (implying that some actors in the industry currently are not minimizing costs). Such benefits may emerge, but they are not proven. The hypothesis that regulatory compliance can increase productivity lacks empirical support in most cases where it has been studied. In addition, it is clear that not all parties will gain. Smaller ports and operators in particular are likely to suffer from stricter security requirements, given that regulatory compliance involves substantial fixed costs. This raises concerns regarding the impact of security measures on competition.

[5] It is not clear what level of screening would be best to equilibrate benefits from deterrence and security costs.

With respect to maritime transport, there is a widespread sentiment that the security measures that are implemented or are being debated achieve very little or nothing, except possibly that they raise awareness of security concerns among seafarers. There is also little confidence that measures are progressively being improved ("closing more doors"). There is a tendency for security measures to be driven by access to funding or by the need to maintain access to some markets, rather than by a real desire to improve security in an effective manner.

8. CONCLUSION

The objective of the round table was to take stock of the expertise on the assessment of risk and insecurity in transport, to discuss how the expertise can support project and policy appraisal, and which gaps in knowledge remain. First, it is important to note that terrorist threat issues are fundamentally different from safety issues. Security is characterized by uncertainty, meaning that no objective probabilities can be determined for the occurrence of attacks. Uncertainty makes economic analysis difficult. The tools developed for costing risks, e.g. on the basis of historical accident records, cannot be applied to events that are uncertain. Moreover terrorists adjust their strategies according to the security measures taken, something that does not happen in relation to accidents. This limits the extent to which experience with safety policies can help make better security policy.

Subjective probabilities on terrorist attacks can be gleaned from intelligence, the insurance industry, and prediction markets. None of these sources is without shortcomings, but all are useful and can contribute to a systematic and transparent approach to establishing the probabilities underlying security policy design. Such an approach is currently lacking in national security policy development, and given a likely tendency for individuals to overestimate terrorism risk, this situation is conducive to high and poorly targeted spending on security. Many security measures in aviation and in maritime transport are broadly assessed not to be effective, so they do not provide value for money.

Economic analysis could help improve the effectiveness of security policies. For example, economic impact analysis is useful for determining the likely economic costs from various attack scenarios. More broadly, systematic economic analysis provides insight in how deterrence strategies hold up under alternative assumptions on how likely attacks are to occur. Economics also clarifies how stated security goals can be attained at the lowest possible cost. For example, switching from process-oriented to output-oriented regulation likely improves the effectiveness of passenger screening in aviation. Risk-profiling in aviation screening, in order to concentrate resources where they are most needed whilst maintaining random checks on pre-screened passengers, is probably the key measure for achieving better levels of security from the resources spent. The use of profiling has been handicapped by concerns that it can be used to discriminate between citizens on inappropriate grounds and could raise privacy issues. However, an opt-in approach can be used where passengers wishing to benefit from faster passage chose voluntary profiling.

In sum, the economic analysis reviewed at the round table is critical of current security policies, which are seen to be largely ineffective in improving security, and too expensive in terms of attaining intermediate goals (such as screening rates) that are easy to measure but give little indication of the true degree to which security is improved. Security policies are, on the whole, wasteful. For this criticism to be taken seriously, clear alternatives need to be put forward. The alternatives put forward, such as profiling, sometimes lack political support. Rather than abandoning such improvements it would seem appropriate to devote greater efforts towards developing safeguards against misuse and informing politicians and the public on the safeguards and the merits of the improved measures available. Otherwise policy will continue to be wasteful, a price that many policy-makers appear willing to impose on society in return for creating the perception that "something is being done". , Greater transparency on the expected costs of terrorist threats might also help reduce waste by moderating the demand for action. Most importantly better levels of security could be achieved with the resources currently devoted to it.

REFERENCES

ASPI (Australian Strategic Policy Institute), 2008, Risky Business – Measuring the costs and benefits of counter-terrorism spending, Special Report, Issue 18. http://www.aspi.org.au/publications/publication_details.aspx?ContentID=190&pubtype=10

Bichou, Khalid, 2008, Maritime security and risk-based models: review and critical analysis, JTRC Discussion paper 2008-20. http://www.internationaltransportforum.org/jtrc/DiscussionPapers/DP200820.pdf

de Palma, André, 2008, Rationalité, aversion au risque et enjeu sociétal majeur, JTRC Discussion paper 2008-21, http://www.internationaltransportforum.org/jtrc/DiscussionPapers/DP200821.pdf

Gordon, Peter, James E. Moore II, and Harry Richardson, 2008, Economic impact analysis of terrorism events: recent methodological advances and findings, JTRC Discussion paper 2008-22,. http://www.internationaltransportforum.org/jtrc/DiscussionPapers/DP200822.pdf

Intriligator, Michael D., 2008, On "Transnational Terrorism" - Perspective Paper on the Todd Sandler, Daniel G. Arce, and Walter Enders Paper for the 2008 Copenhagen Consensus. (http://www.copenhagenconsensus.com/Default.aspx?ID=1152)

Poole, Robert W., 2008, Toward risk-based aviation security, JTRC Discussion Paper 2008-23. http://www.internationaltransportforum.org/jtrc/DiscussionPapers/DP200823.pdf

Rose, Adam, 2007, Economic resilience to natural and man-made disasters: multidisciplinary origins and contextual dimensions, Environmental Hazards, 7, 4, 383-398.

Sandler, Todd, Daniel G. Arce and Walter Enders (2008) Terrorism – Copenhagen Consensus 2008 Challenge Paper, Copenhagen Consensus Center (http://www.copenhagenconsensus.com/Default.aspx?ID=1152).

Surowiecki, James, 2004. The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations, Random House.

ROUND TABLE 145: SECURITY, RISK PERCEPTION AND COST-BENEFIT ANALYSIS

Paris, 11-12 December 2008

LIST OF PARTICIPANTS

Chair:

Prof. Andrew EVANS
Imperial College, University of London
LONDON
United Kingdom

Rapporteurs:

Dr. Khalid BICHOU
Imperial College, University of London
LONDON
United Kingdom

Prof. Peter GORDON/
James E. MOORE II/
Harry RICHARDSON
University of Southern California
LOS ANGELES
USA

Prof. André DE PALMA
Ecole Normale Supérieure de Cachan
CACHAN
France

Dr. Robert POOLE
Reason Foundation
LOS ANGELES
USA

Participants:

Dr. Torkel BJORNSKAU
Institute of Transport Economics
OSLO
Norway

Mr. Andrew COOK
Department for Transport
LONDON
United Kingdom

Dr. Andrew GRAINGER
Trade Facilitation Consulting Limited
KINGSTON UPON THAMES
United Kingdom

Dr. Juha HINTSA
Cross-Border Research Association
LAUSANNE
Switzerland

Dr. Brian JACKSON
RAND Corporation
ARLINGTON
USA

Mr. Carl KOOPMANS
Ministry of Transport, Public Works and Water Management
THE HAGUE
The Netherlands

Prof. Dr.-Ing. Juergen KRIEGER
Federal Highway Research Institute
BERGISCH GLADBACH
Germany

Dr. David LEVINSON
University of Minnesota
MINNEAPOLIS
USA

Mr. Alex MACFARLANE
Department for Transport
LONDON
United Kingdom

Dr. Susan MARTONOSI
Harvey Mudd College
Claremont, CA
USA

Prof. Daniel MIRZA
Université François-Rabelais
TOURS
France

Dr. Andrew MORRAL
RAND Corporation
ARLINGTON
USA

Mr. Serge PAHAUT
Université Libre de Bruxelles
BRUSSELS
Belgium

Prof. Barry E. PRENTICE
University of Manitoba
Winnipeg
Canada

Dr. Mark B. SALTER
University of Ottawa
OTTAWA
Canada

Dr. Risto TALAS
Cass Business School
GB-LONDON
United Kingdom

Dr. Nicolas TREICH
Toulouse School of Economics (TSE)
TOULOUSE
France

Monsieur Rene VAN BEVER
Service public fédéral Mobilité et Transports
BRUSSELS
Belgium

Professor David WIDDOWSON
University of Canberra
CANBERRA
Australia