OECD

International Transport Forum

TRANSPORT RESEARCH CENTRE

TERRORISM AND INTERNATIONAL TRANSPORT: TOWARDS RISK-BASED SECURITY POLICY

ROUND TABLE

144

OECD

International Transport Forum

TERRORISM AND INTERNATIONAL TRANSPORT: TOWARDS RISK-BASED SECURITY POLICY

ROUND TABLE

144

TRANSPORT RESEARCH CENTRE

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

This work is published on the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

Also available in French under the title:
OCDE/FIT Table Ronde n° 144
TERRORISME ET TRANSPORT INTERNATIONAL
POUR UNE POLITIQUE DE SÉCURITÉ FONDÉE SUR LE RISQUE

Corrigenda to OECD publications may be found on line at: *www.oecd.org/publishing/corrigenda*.

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 International Transport Forum was created under a Declaration issued by the Council of Ministers of the ECMT (European Conference of Ministers of Transport) at its Ministerial Session in May 2006 under the legal authority of the Protocol of the ECMT, signed in Brussels on 17 October 1953, and legal instruments of the OECD. The Forum's Secretariat is located in Paris.

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 OECD and the International Transport Forum established a Joint Transport Research Centre 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.

Further information about the International Transport Forum is available on Internet at the following address:
www.internationaltransportforum.org

TABLE OF CONTENTS

SUMMARY OF DISCUSSIONS

SUMMARY CONTENTS

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 are 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 characterised 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 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), thus justifying public intervention, and some are hard to monetise. 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 programme and the US C-TPAT program in maritime transport can be mentioned as examples: operators in compliance with the requirements of these programmes 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 centralised 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 policymakers.

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 programme, it also compromises the capacity of analysis to determine how effective a programme 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 policymakers 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 programmes, 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 programme. This at least forces decision-makers to be explicit on why the programme is expected to produce projected changes in threat levels.

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 characterises 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 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 organisations 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 programmes 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.

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 characterised 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. based on 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 policymakers 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.

NOTES

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.

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.

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.

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

REFERENCES

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

Bichou, Khalid (2008), Security and Risk-Based Models in Shipping and Ports: Review and critical analysis, JTRC Discussion Paper 2008-20. www.internationaltransportforum.org/jtrc/DiscussionPapers/DP200820.pdf

de Palma, André (2008), Rationalité, aversion au risque et enjeu sociétal majeur, JTRC Discussion Paper 2008-21, 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. 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. (www.copenhagenconsensus.com/Default.aspx?ID=1152)

Poole, Robert W. (2008), Toward a Risk-Based Aviation Security Policy, JTRC Discussion Paper 2008-23. 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 (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.

RATIONAL BEHAVIOUR, RISK AVERSION: HIGH STAKES FOR SOCIETY[1]

André de PALMA

Ecole Nationale Superieure
Institut Universitaire de France
Cachan
France

SUMMARY

Cachan, February 2009 (Revised)

1. INTRODUCTION[2]

… I blame them for having made … a choice …
The true course is not to wager at all …

…but you must wager…You are embarked.
Which will you choose then?

Pascal, *Thoughts*
(Lafuma 418, Brunschvicg 233)

Certain areas related to the topics under discussion here lie outside my field; for instance the evaluation of risk assessment and security deficiencies in the transport sector. What has convinced me of the importance of this subject are a few very general conclusions, indeed I would say, impressions, that I have drawn from the truly remarkable development of our powers to analyse the risk decision-making process over some years now.

In this paper, the term "unknown events" is often used with reference to the management of risks arising from intentionally malicious acts[3]. The costs of security in this sense of the term are an element of every transport budget today. In addition to the costs of prevention, surveillance and forecasting, the costs of the potential damages arising from such acts will also have to be taken into consideration from this point onwards.

The events of 11 September 2001, which accelerated this trend, should suffice to convince us that, from now on, the consequences of such damages will be on a scale comparable to the costs of war. Some authors have taken issue with the idea that there would be some scale chasm between these two types of phenomena. Actually, the figures for wars connected with terrorism today are reported to be somewhere well in excess of millions of billions of dollars. This is what is to be gathered from General Haig's response (2003) that terrorism is now a branch of warfare. In a sense that we have yet to define, these are strategic decisions. The criteria which, in the eyes of the US Government, linked this attack to the wars that followed have actually more to do with retaliation than with simply estimating the consequence of the costs and benefits of a prevention policy, where these can be calculated.

Hence, the additional expenditures incurred in many areas since the events of 11 September 2001 are not purely consequences that are more or less costly or more or less acceptable. That is because they are linked to the part played by these events in exposing vulnerabilities that were, and still are, largely underestimated, as well as to a desire to retaliate. The fact is that the logic of deterrence - a field in which the military man is more at ease than the economist – can simply not be reduced to the calculation of prevention and surveillance costs.

Viewed in this light, it is easy to see why economists do not feel very able to contribute to the definition of deterrence policies. Nevertheless, what economists can do is to approach the problem from the other end. Instead of calculations as to the logic of the decision, they can endeavour to propose an estimate of the various costs. This was what started off discussions on the costs of the US War in Iraq in budgetary terms: with their estimate of USD 3 000 billion, Stiglitz and Bilmes (2008) prompted a substantial revision of previously accepted estimates of these costs[4].

This brings us up against the limitations of cost-benefits analysis, as Stiglitz concluded in a bid to counter claims that he had neglected[5] the latter approach: costs were very substantially higher than had been stated by US political leaders. More importantly, with reference to benefits, Stiglitz said plainly that there were none that he could see. As we are reminded by the work of the founders of prospective analysis in economics – of whom I will say more below – the strategic approach does more than simply extend extrapolation calculations: it complements them.

2. COST-BENEFIT AND PROSPECTIVE ANALYSIS

The aim of cost-benefit analysis is to evaluate the outcomes of a given project. Choices may be *absolute* (a proposed project will either be selected or not) or *relative*: there are two competing projects and decision-makers must determine which alternative they consider most appropriate.

The work of planning and prospective analysis – some fine exercises of which were seen in the last century – requires that the implied relationships be handled by a less binary process. This means that there will be several series of decisions to take: which projects for which programme, when and how their execution can be slotted into a job schedule, which methods of finance seem appropriate, which supporting measures will be required, to mention but a few. This is very far from a straightforward all-or-nothing answer.

By now, we are well used to reading that putting each programme in place requires the co-ordination of a series of sub-programmes and the need for cross-transactions with other programmes. The 20th century talked a great deal about priority ranking in this respect, a technique that ensures that nothing is missed out.

Over the past few decades we have learned to associate various sets of risks with these programmes: risks associated with fluctuations in demand, sudden changes in the costs of production factors, setbacks in completion time and the risk of seeing programmes appear which could fully or partly replace those on which firm decisions have already been taken, etc.

These risks are themselves associated with others: the vagaries of the economic cycle, more or less sudden shifts in the price of raw materials, hitches in the course of the project. The list is endless, we know, but in times of escalating hostilities, any omission will only too readily be seen –with the virtue of hindsight– as criminal negligence or sheer stupidity, even when the omission, whatever it was, had genuinely been said insignificant at the time.

Here, we have learned to identify some risks that are foreseeable and quantifiable and some that are foreseeable but difficult to evaluate. Lastly, as evaluation methods progress, it often seems with hindsight that other risks should have been included in an evaluation, but were simply omitted.

For instance, it has been axiomatic for centuries now that the construction costs of large-scale infrastructure projects are frequently revised upwards in the course of the project. One particular difficulty – and every error here is costly – is to ensure proper synchronisation of the work of several teams operating together: a construction site, by definition, is not like a routine production-line operation. Therefore, it is rather difficult to see how prospective cost-benefit analysis studies can quietly ignore these risks. Moreover, once built, the infrastructure will inevitably face greater intermodal competition.

Clearly, these observations are well within the grasp of any first-year student who has just signed up for an industrial economics course. They have also entered into the folklore of observers of collective decision-making[6]. So as not to make these – suddenly more human – decision-makers look more fallible than they actually are, it is only reasonable to make allowances, too, for the host of different agents involved in this kind of large-scale investment project.

Something else that we have known for centuries is that business banks are not necessarily averse to cost increases in construction programmes under way. After all, their primary function in this context is lending, not repaying. Any inconsistencies that become obvious after the event stem largely from forgetting, when we look back, that the mutual interests of the principals only ever partially coincided.

In these times of widespread crisis, the issue will not be if or how the entrepreneurs in question could or should have done more to meet specifications, often drafted after the fact, once the fatal failure has been noticed. Rather, it will be whether we can afford the time to take on board these consequences, which at one time were genuinely negligible, but later turned out to be a factor in the accelerated changes that our world is now going through.

To put it simply, assuming that whatever issue challenges us is one that is identifiable and measurable, then the new economics of risk management may well not be of any great help. For example, there is no need for experimental economics procedures to set up navy patrols around the Horn of Africa. Giving the green light to the competent admiralties should suffice.

That said, an economist's role is to acknowledge an interesting problem in that very area where his skills are seldom acknowledged, it seems, and so he would be delighted to be allowed to formalise the symmetries between the tactics available to victims, pirates and States in terms of models borrowed from game theory. However, the economist also has some more general comments to add.

The difference between deterrence and prevention, the reason that the military man will often instinctively silence the economist, does not actually come under the scope of cost-benefit analysis. This is because the military man has the resources available to calculate an escalation to extremes. Typically, this is not really reducible to the criteria an economist would use, since the military man's rationale is to break the other *whatever the cost*.

These tactics are indeed not unfamiliar to the economist. It is the underlying rationale, more than calculation of the relevant criteria, which may give his partners pause for thought. For instance, a firm may undercut prices in order to outdo its competitors. Certainly, an economist can help to make sure that such a strategy is as low-risk as possible. He can also describe it, since he has the experience to understand it. The aim is to describe and prevent behaviour aggressive enough for their prospective analysis to include the risk of certain mutual destruction. That is the problem we have to weigh up. Let us now state it in somewhat more provocative terms: it is the right time, and may even seem reasonable, to say that urgent consideration must be given to one straightforward question: do we really have to go grudgingly, as it were, into the globalised economy, into one crisis after another peopled by elusive enemies? The economist has a few reminders to give in this regard.

We have just seen that there is little sense in expecting any second-rate review aimed at bringing those responsible for this or that programme before the Court of History. There would be little point, for instance, in accusing mortgage-lending banks of being insensitive to the rapidly dissuasive difficulties experienced by borrowers in meeting repayment terms. Nonetheless, it is true that the escalating defaults on mortgage payments and the growing inevitability of sales at a loss destabilised the banking market in the end. However, this crisis does not spell the end of the world. Rather, it shows the limits of the role to which economists have too often been confined as the accountants of an ill-justified and ill-run system.

On the other hand, we shall see how increasingly urgent it is to have a process that strengthens our sensitivity to the losses incurred, but also to the sacrifices made and the many reactions of the working populations mobilised in the modern economy in the wake of the shortly-expected completion of market openness policy: the foreseeable closure of those markets. Important as it was to tempt to master the management of the internal risks of a given programme or of an economy bounded by identifiable reference points, it seems every bit as misguided to want to transplant the methods of this policy to areas which, by definition, we cannot reasonably hope to control. This widespread mistake is one that we risk walking right into today because we do not know what the impact of our activities will be in the outposts of the empire, the four corners of our world. The reason is not that we are any more deserving of scorn or censure than our predecessors, it is just that the world is on the brink of rather rapid and probably rather violent change now that with the mobilisation of Indonesia, Mexico and Brazil after India and China, we have come full circle and done the rounds of all of the major labour-force and consumer catchment areas available.

It is because globalisation will soon be complete that our insensitivity to unfair terms of trade and to the predictable, but unforeseeable, reactions of those concerned is untenable. Evading the issue is a tactic that is becoming a little more antiquated each day.

However, in this new world that we are being ushered into by rapid globalisation and its corollaries – about which I will say a few words – I must say from the outset how forcibly I am reminded of Popper’s reference to what the barbarian King Pyrrhus of Epirus said about strategy while at war with the Romans: “*Another such victory and we … are lost*.”

For just a moment, we will try to see globalisation from the perspective of the 1970s. What I wish to do here is to perpetuate the spirit of open, realistic optimism that prevailed when the OECD’s *Interfutures* exercise was conducted 33 years ago now. What were in substance the reasons adduced for this programme?

As you will remember, the proponents of this analysis and assessment project – holding that the *internal proletariat* was to be successfully integrated in modern societies, thanks to a constantly growing middle class – proposed to raise the issue of the *external proletariat*: “*more than 120 countries with rapidly growing populations, already accounting for three-quarters of humanity, to which the industrialised nations have a collective responsibility* (Albert, 2000).” But trends in both capital and migration flows over recent years demonstrate that the prevalence of an attitude of insensitivity to the changes that are happening now has sharply increased among both public opinion and decision-makers.

The insensitivity, not to say incredible hardheartedness of the past two decades has such an impact on us that we have to belabour the point, in order to make this change in ideas and attitudes more apparent. Who is so bold as to say that, over the past twenty years in a certain number of countries in Africa, there has been a decline in the number of children in school, and not just relative to the school-age population, but in absolute terms? For a generation, the dominant "Trade not Aid" motto, which promotes trade with entrepreneurs in poor countries rather than increasing up support for needy populations, has marked a retrograde trend. It seeks to extend prematurely, to countries on the farthest fringes of our economy, processes which, incidentally, our experts did not invent, but which grew out of the countries of Asia and South America: developing the local middle classes, boosting agricultural exports, freezing agrarian reforms and criticism of land redistribution. These policies have a quantified target: the sadly famous 0.7 per cent, which our governments should be earmarking for aid to the poor countries of the Third World, said by some, when it was introduced, to be a reduction compared with budgets and policies in colonial times. This is a controversy beyond the scope of this paper.

3. THREE MODELS FOR MANAGING THE FUTURE

I will now turn for a moment to contrasting descriptions that address the future. Along the way, I invite you to reconsider *extrapolation* and *strategy* procedures, two familiar approaches, which many people seem to think exhaust all the possibilities. This is true, in a way, since if they are taken as opposite extremes, however artificial this often is in practice, they do appear to cover all of the approaches between them. This is a dangerous mistake to make for one simple reason: both procedures often – so often that one may ask why – omit an approach that is nevertheless common to both of them: sensitivity. Let me explain.

First, there is extrapolation, in a way the more *naturalistic* of the two, as we shall see. For some people, extrapolation is the driving force of forecasting. A forecaster's job is often to extrapolate trends from the known past to a future that is assumed to be uncertain. On the timescale marked out for measurements taken for this purpose, the present is ideally represented as no more than a point, which must not distort the calculations too much.

However, the present does exist; we live in it. That is why good observers, such as Jacques Lesourne, have been keen to repeat that prospective analysis, an exercise which by its very construction is oriented towards long-term, can reduce the pressure exerted on the present by the short term. Extrapolation has been criticised for ignoring freedom, disregarding the undeniable span of the present, the uncertainties related to our imperfect knowledge, etc. These criticisms are interesting, but before addressing them, I would like to give a brief description of the other family of approaches to the future.

From more "*interventionist*" circles, we have actually inherited a second method of matching what we see with what we forecast. *Strategy*, indeed, can be described as reversing the order of the ends and the means of extrapolation procedures. What it sees and faces are the objectives that can be ascribed to the future, not the data inherited from the past. What it seeks to be able to forecast are patterns of available investment that will have to be called on in the near future if a given long-term end-point is to be attainable. The challenge that strategists agree to take up is to choose among possible futures, deploying the appropriate resources to best advantage. Hence, strategists take the opposite tack to forecasters. They endeavour to find out more about the resources of an uncertain present that can be deployed to attain a future that they profess to choose.

As we have said, treating these two theories as opposites is largely artificial: good strategists must know their way around extrapolation, while forecasters have to take strategic interactions between agents into account. Consequently, those who advocate either method to the exclusion of the other need to be taught that they are complementary. That is why I wish to say a few words about one strength they have in common. Faced with the conventional opposition of the two, my comments are intended to bring certain echoes of the word *sensitivity* to life again. The aim of this exercise is to help the actors pay a little closer attention to *context*: the set of circumstances, by definition complex and underestimated, in which any change carries major consequences.

The keyword here is sensitivity to distant, complex, barely perceptible evolutions: how does one ensure that the signals sent by a world that is in the process of delivering its own future are not unduly neglected when we are busy primarily with the forecasting or monitoring tasks that our local job requires? To state the question in more direct terms: which elasticities are weak today for decision-makers and their advisers but will be critical tomorrow, and relative to which processes? What things are we not paying attention to today, more or less intentionally, that we will inevitably have to think about tomorrow?

To take a basic example, we have long counted on the low elasticity of transport demand relative to energy prices, to the point of taking this low elasticity as some sort of universal constant. If we are to survey this problem, a good questionnaire should be able to capture these potentials even before they occur. The variables to be measured and the indicators selected must be carefully calibrated so that they do not conceal what is not obvious (Prelec, 2004). While not attempting to try to teach professionals how to draft questionnaires, how many thousands of very expensive ad hoc surveys have been content with reproducing what was alleged to be true?

It must be said that the extrapolation work requires a certain strength of character. It is about putting a name to developments; that is to say, about designating areas where a relevant variable, albeit a third derivative, changes sign. Incidentally, if futurists wish to extrapolate well, they must not be slow to recognise change. For instance, how many authors religiously trotted out the theory that, since transport demand was relatively inelastic to transport costs, one could ignore ranges of values and population sub-groups in which highly predictable changes in attitude were already becoming apparent? Futures analysts seem to let themselves become inured to the surprising, if negligible, speed of such changes.

Strategists are more known for their insensitivity. All they can see is the objective, people say. They are capable of steamrolling everything in their path on their march towards destiny. That is certainly not wise, but excess is the hallmark of the strategist.

If there is one thing that risk analysis in major technical projects has been able to teach us over the past few decades, it is that a total lack of sensitivity makes for good actors, in the sense understood in Diderot's *Paradoxe sur le comédien*: "*it is extreme sensibility that makes mediocre actors; it is mediocre sensibility that makes the multitude of bad actors; and it is the absolute lack of sensibility that prepares actors who shall be sublime*." The detachment of the mad scientist contrasts with the chatty tone of the newspaper columnist.

Since extrapolation seemed to ignore the freedom to change, it is quite reasonable to want to include this freedom in forecasting: one day US consumers buy fewer four-wheel drives, for example. However, it may prove decisive, as we can perhaps see more clearly today, even if we are going through a politically and intellectually retrograde period, to look for this more essential function, which I call sensitivity, preparing freedom. We will come back to this point later.

4. THE CASE FOR INSTITUTIONS

An ill-defined policy is still a policy. A preference to have no policy is permissible, but in that case, one also has to wager on the chances of success of the "no-policy" option.

As Pascal, a mathematician who was also interested in the decision-making process, explained *"…but you must wager. You are embarked":* there is nothing clumsily interventionist about trying to understand the dynamics of an action.

The fact is that economics is not to be confined simply to drafting recommendations for an inescapable but obscure institutional outer world. Where need be, it can also study the environment that produces these institutions, as the vector through which their recommendations are requested, read, tested, accepted or called into question.

As well as that, over and above the mechanisms of contractual transactions, economists are able to evaluate the impact of the statutes of institutions to which the actors belong on price-setting mechanisms: transactions are negotiated within an institutional framework that is given and liable to change.

What is an institution? Hauriou, the founder of modern institutional studies, will serve as our guide: "*A little sociology leads away from the law, much sociology leads back to it.*" An institution is a source of law and, at the same time, it is an actor capable of initiatives; it can more easily be described by saying what it is not. An institution is a source of standards, but is not the same as the law and not the same as a contract. A contract has value only because of the interests of the parties to it. The law assigns duties to subjects regardless of their interests. An institution carries out the duty that its mandate assigns to it.

When we speak of statutes, different information asymmetries, powers to negotiate or exercise a veto, what we are talking about are the established, stabilised components of social interactions. Should we try to ignore them? No. Classic theory allowed us to raise profound but simple questions, such as: "What is the nature of the firm?" – the question raised by Coase (1937) more than half a century ago. If the price mechanism were the only way to ensure co-ordination among agents, why would entities such as firms exist at all? This work, which has long been regarded as a "*tour de force*" of neoclassical theory, was in fact an effort to take the real world into account.

The market itself is an institution, loaded with deeply ingrained historical and local characteristics. Every country lives off a capital of established customs which account in part for the diversity of policy choices that it can make.

One of Coase's fundamental ideas is worth noting: institution is not here in order to breathe a little more soul into an inhuman market. It does more than ensure a little justice and fairness. Primarily, it plays an intrinsically economic role by helping to manage the problem of transaction costs. Contracts are not free bilateral interactions sheltered from any social influence. A world with no memory would be very costly in terms of transaction prices. After all, as the Olson (1965) Paradox demonstrates, the production of a public good is not necessarily always promoting the self-interest of the rational individual. We know that this paradox did not hinder critical thought, as it allowed Olson to illustrate the variable weights of individual and sometimes diverging interests according to group size, for instance, leading to his famous conclusion that small groups could be more effective than large groups in mobilizing individuals. Rousseau, in his *Discourse on the Origin of Inequality* (1775), paints this logically consistent model: "*If a deer was to be taken, everyone saw that, in order to succeed, he must abide faithfully by his post: but if a hare happened to come within the reach of any one of them, it is not to be doubted that he pursued it without scruple, and, having seized his prey, cared very little, if by so doing he caused his companions to miss theirs*."

The new institutional economics of Coase and North revisits this issue in depth since, in their work, not only do institutions influence actors, they are themselves created by the actors' efforts to reduce transaction costs. When a market that has become very fluid spawns relations that are improvised, aggressive and verging on violent, some of the actors will apply the institutional brakes necessary to curb the costs of such improvisation. Institutions, North says, are humanly devised constraints that structure political, economic and social action. In a situation of bounded rationality, he says, it is often rational to fall back on established procedure, available knowledge and a given apparatus; accounting for contingencies like these gives economics access to the world of ordinary humans.

Therefore, although transactions sometimes generate poverty or revolt, there are no grounds for lazily concluding that this is inevitable. Observation of the actors' behaviour shows that Coase's entrepreneur keeps processes that he could outsource inside the firm, because he sees certain inherent advantages in the firm/institution and in the relationships of synchronisation and subordination that it allows.

5. DECISION THEORY AND ITS HISTORY

"Entre ma passion pour l'histoire et celle pour la modélisation mathématique,
je n'avais pas à trancher.
La science économique pouvait les satisfaire toutes les deux."

("I did not need to decide between my passion for history and
my passion for mathematical modelling.
Economics could satisfy them both.")

Lesourne, 2000, pp. 189-190

Being sensitive to what one risks losing, or what one is already losing, precisely because that loss was for too long considered negligible, and being capable of doing the calculations over again, is an imperative for us today and one that economists are professionally familiar with. In order to understand what is new about this imperative for a certain number of actors battling in business or politics, I propose to give you a brief review of some recent achievements in risk theory.

Calculating damages from events subject to any given probability distribution raises problems and the formulation of those problems has seen changes over the last few decades. At this point, I propose to make a few short comments on some aspects of these developments in thinking. Decisions on resource allocation under a risky environment often obey today the theoretical model known, in modern terms, as the "*expected utility*" model. This section briefly reviews the history of our ideas on this subject, which we will see, I hope, are not out of place in this discussion.

The theoretical model for expected *utility*, outlined by the Bernoulli family in the early years of the 18th century and formalised a century ago by Von Neumann and Morgenstern, corrected classic rationalism and the optimal application of probabilities to decision-making which had prompted the correspondence between Pascal and Fermat in the mid-17th century. The latter had confined themselves to rationalising decisions solely in terms of the expected value of the benefits associated with a set of events, each of which had a given probability.

To go back to our overview and simplify matters, let us first consider the ideal case of a world without unknown events. If the future development in the economy is certain, it is unique and the actors have no great difficulty in knowing what it is since it can be deduced unmistakably from the present state of affairs. The revenues generated by investments are known and there is therefore no risk, no risk premium, no speculation and no insurance. However, we know that not even Robinson Crusoe lived in that kind of economy. Firms, contracts, institutions and the market can only interact in a world where there is, at the very least, chance and a way of taking it into account: through risk calculations. If allowance is made for chance, then possible events and their consequences are not ruled out, even if we follow policies aimed at excluding them or dealing with them.

Let us now review a few critical steps towards these developments in allowing for the evaluation of possibilities. For the authors who were the founders of probability calculation, Huygens and Bernoulli with Pascal and Fermat, future events are unknown but not their probabilities[7].

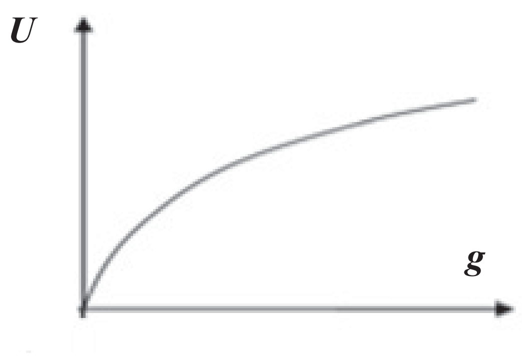
Does that cover everything? Do we now just have to add some detailed results into this general theory? No. A counter-example formulated by one of the active figures in the construction of probability calculations very quickly showed that rationality in these calculations could not always be recommended. The Saint Petersburg Paradox, constructed to demonstrate that although an infinite gain over the long run should, under expected value theory, prompt someone to gamble an infinite sum, observation shows – understandably – that a rational gambler will avoid the extremes to which the rational decision leads and, in fact, will quite reasonably bet a relatively small amount. When presenting this paradox, "Bernoulli's nephew", Nicolas, noted at the beginning of the 18th century that if the expected value of the gain was the only criterion used, as it was for the probability theorists of the 17th century, one would inevitably be recommending choices that no reasonable person would make in practice.

Bernoulli's conclusions were of even more value than his paradox. He concluded that a new concept, that of *expected utility,* should be introduced. He opened up a new field when he proposed that no estimation of risk could neglect the reverse problem: what is the gain required to guarantee a given person a utility about which practically nothing certain can be said since it is so subject to change with circumstances. He continued "*Thus, although a poor man generally obtains more utility than does a rich man from an equal gain, it is nevertheless conceivable, for example, that a rich prisoner who possesses two thousand ducats but needs two thousand ducats more to repurchase his freedom, will place a higher value on a gain of two thousand ducats than does another man who has less money than he*."

Expected utility models will therefore take account of the decision-maker's attitude by applying a utility function *U,* the sole basis of which are the decision-maker's wealth or gains. While Bernoulli's assertions have, of course, come in for criticism, the fact remains that he opened up a new world to us. In a sense, his intuitions are more valid still today than when he first formulated them: for researchers at the end of the 20th century, a concave utility function would come to mean risk aversion; the steeper the curve the greater the aversion. Let me draw your attention to the extremely universal nature of this reasoning. This analysis of perceptions, i.e. the diminishing valuation of successive marginal utilities, enabled the construction of one of the first mathematical functions of valuation behaviour and the introduction of experimental procedures in numerous disciplines.

At this point, I would mention, if I may, the economic theory of diminishing returns on increasing investments or the physiological theory of perception as a function of increments in value of data perceptible to the senses. These highly diverse fields required relentless clarification in order to avoid the emergence of a risky "theory for everything". We have now arrived at a threshold that enabled 19th century men of science to cross over into the New World of social science. Analysis of the types of attitude that actors have towards risk from the classic curve is not at all anachronistic. For a person who is less tolerant of risk than another, the utility function will be a concave transformation of the utility function of the latter. In the case of people with zero risk aversion, the utility curve will be linear while for others who are risk-seekers, the lack of aversion to risk will show as a convex utility function.

Figure 1. **Utility *U* as a concave function of gains *g***



Source: Bernoulli, 1738.

Expected utility theory, without the shadow of a doubt, has been the dominant paradigm of decision theory since the middle of the last century. It can been said, simplifying a great deal, that until the 1980s it provided an often controversial but always accepted reference framework for prediction in the field of economics and finance, direction in the management sciences and description in the field of psychology.

Yet, from the very beginning, some very relevant – and scathing – comments had been made based, for instance, on another counter-example which proved very fruitful: the Allais Paradox. Presented to the American Economic Society in 1953, this paradox was to set a decisive limit on von Neumann's expected utility theory (Allais, 1989). I will not go into detail, here, on the discussions that have marked the past half-century, but will briefly present some simple properties of other models inspired by prospect theory, as proposed by Kahneman and Tversky (1979)[8], tackling the now acknowledged impasses of expected utility theory.

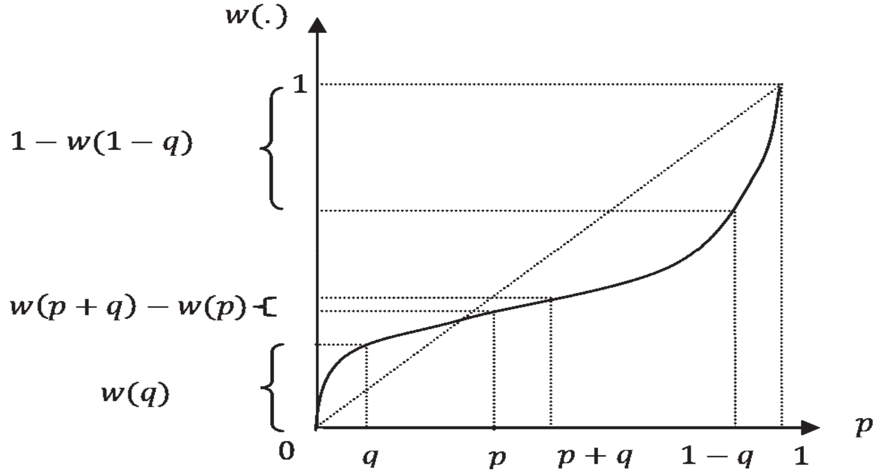
This family of models is more descriptive than normative in purpose: they are an attempt to understand what decision-makers do, how they make intuitive judgements and what their choices reveal, not to propose any general or absolute optimisation criteria to them. Expected utility theory tried to reconstruct the decision-making process from the standpoint of logic, while prospect theory focused on describing the mental process of decision-making. In this latter case, emotion and, more broadly, action, are an integral part of the decision-making process. It was a genuine attempt to construct a broader-based decision theory which would set the already recognised advances by rational decision theories in their proper context, without actually contradicting them.

Let us say from the outset that the aim, according to the authors themselves, was not to give a better description of the behaviour of insurers and bankers. The models constructed by Kahneman and Tversky (1979) try at most to provide an account of certain relatively simple and isolated characteristics of decisions. This severely curtails the descriptive scope that one might wish to ascribe to them in relation to the real world. Last, but not least – and this commensurately reduces the predictive power of the theory – in the real world, as Kahneman was keen to demonstrate, it often happens that *people take risks because they do not know that they are taking them*. Hence, one should certainly not look to prospect theory to provide direct answers to the practical questions that decision-makers ask themselves in the real world.

Numerous empirical studies conducted in recent decades have demonstrated that there are deviations from the behaviour predicted by expected utility theory. Risk aversion as exhibited by decision-makers proves to be more complex in practice; furthermore, it is related to a new aversion, the *aversion to loss*, and takes account of the consequences of a sequence of gains and losses.

A short introduction to probability distortion after Kahneman and Tversky may prove useful. Events that have a very low probability of occurrence, close to zero, are subjectively perceived as having a higher probability (overestimation transformation), while those with a high probability of occurrence, close to one, are subjectively perceived as having a lower probability (underestimation transformation). Hence, in order to describe the behaviour of a decision-maker in the case of a lottery (*x, p*), objective probability *p* is replaced by a probability distortion, applying a probability transformation *w*(.), strictly increasing over the interval [0,1] where *w*(0)=0 and *w*(1)=1. Instead of evaluating the lottery (*x, p*) by *p U*(*x*) it is valued as *w*(*p*) *U*(*x*)*, where U*(.) represents the person's utility function.

Figure 2. **Probability weighting function: subjective probabilities *w* as a function of objective probabilities *p***

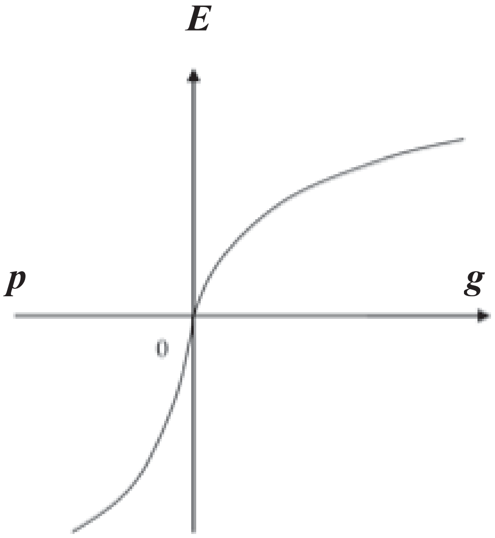


Source: Tversky and Kahneman, 1992.

Tversky and Kahneman (1992) later extended prospect theory and found that the way in which people tended to distort the probability of an event depends on how they rank that prospect on a scale of order of preference from most to least favourable. The person then works out the *cumulative* probability of obtaining *at least* a given sum. Hence, as illustrated in the figure above, if the probability of obtaining at least 1 is actually *q*=15%, a person will estimate this probability as *w*(q)=35%, for example. Moreover, if the probability of obtaining at least 2 is actually *p*+*q*=50%, people will estimate this probability as *w*(*p*+*q*)=45%. The probability of obtaining between 1 and 2 will therefore be distorted from *p*=35% to *w*(*p*+*q*)-*w*(*q*)=10%.

The curve shown above plots the transformations for risk attitudes is a case of bounded rationality, as it has been known since the seminal papers by Simon (1982). In order to plot this curve, a more complex utility function is introduced that takes other distortions related to subjective evaluation into account. First, we note an asymmetry between the perception of gains and losses: it is immediately apparent that the utility function is concave for gains and convex for losses. There is also some diminishing sensitivity: the impact of some gain variation diminishes with the distance from the reference point. Lastly, the marginal disutility of losses is greater than the marginal utility of variations of the same magnitude in gains.

Figure 3. **Transformation of gains and losses**



Subjective evaluation *E* as a function of the objective income;
the regions of gains *g* and losses *p* are distinct.
The reference point here is (*0, 0*).

Source: Tversky and Kahneman, 1992.

6. THE EXPERIMENTAL APPROACH TO RISK PERCEPTION: A BRIEF OVERVIEW

At this point, I propose to make a few remarks about some aspects of the relationships between security management, risk analysis and cost-benefit analysis. Experimental psychology and economics have highlighted systematic deviations in the behaviour of people confronted with risk where numerous conventional approaches propose prediction based on expected utility theory.

These systematic deviations reflect a tendency to distort probabilities and their consequences depending on whether events are rare or frequent, since we have demonstrated that there is an asymmetric distortion between gains and losses. In real life, individual perceptions influence not only individual decisions but also the decisions of governments subject to the influence of public opinion or elections.

There are several aspects to probability distortion.

Individuals have a tendency to *overestimate* departures from deterministic situations (probabilities are distorted in this case). Low probabilities (rare events) are systematically overestimated. There is a fundamental difference between an event that is impossible (probability strictly nil, generally undistorted) and an event that is possible but highly improbable (which will be overestimated). Mathematically, this property is reflected by a discontinuity in the distortion function near the point of origin.

Certain probability distortions of this type have been studied by de Palma and Picard (2008) with the aid of a database of over 4 000 people (using an "experimental economics" procedure run through an Internet site, http://www.RiskToleranceOnLine.com.)

The types of question asked in order to highlight these probability distortions are as follows:

Which of the following two possibilities do you prefer?

- Option A, lottery (EUR 1 000, where $p = 0.05$ and EUR 100 where $1\text{-}p = 0.95$.
- Option B, a sure gain of EUR 140.

Calculations show that the Option A lottery offers a chance of winning EUR 145, an amount which is higher than the sure gain offered in Option B (EUR 140). The risk premium is therefore EUR 145 -EUR 140 = EUR 5. Generally, it is not enough to explain the choice of Option A by a person whose risk aversion has previously been estimated based on lotteries where the chance of winning was of the order of 50%. This person shows an *optimism bias*, in that he pictures himself on the "winning side of the divide" and overestimates the probability of winning the "jackpot" of EUR 1 000.

Conversely, there are low-risk situations where losses can be high. Often, we find that there is a *pessimism bias* which makes people overestimate low probabilities of poor performance and avoid the relevant options more than they should under expected utility theory. For instance, many travellers reacted to the events of September 2001 by avoiding air transport and using the car for long-distance travel instead. As transport by car is much more dangerous than air transport in terms of accidents per kilometre travelled, this was a case of pessimism bias: the consequences were an increase in the number of deaths.

The rejection of options which carry a risk of adverse consequences is amplified by two other phenomena. Firstly, people do not like to be disappointed, i.e. to suffer consequences that leave them less well off compared with a given point of reference. This anchor point can be conditioned by on one's past experience or future expectations. Mathematically, this is reflected in a discontinuity in the derivative of the utility function in or around the reference point. In this case, the slope to the right of the reference point is less steep than the slope to the left: people are more sensitive to a change in outcome when they incur a loss (defined in relation to the reference point) than to a change in gain of the same magnitude.

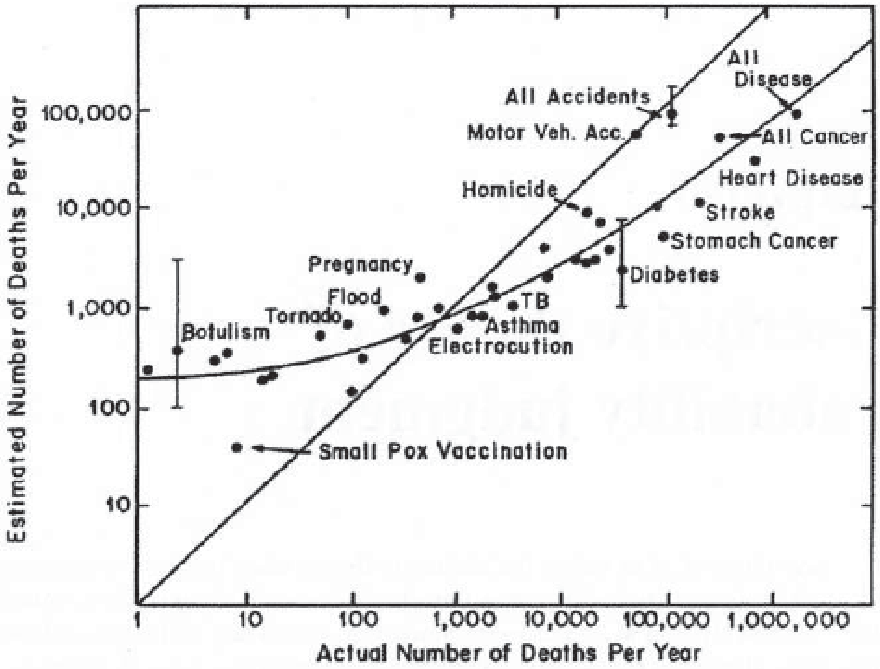
From the analysis of the data gathered via http://www.RiskToleranceOnLine.com three different patterns of attitude to risk have been found, expressed here in terms of total lottery wins.

1. Risk aversion: respondents do not like risk and are ready to settle for a smaller amount than they had hoped in order to avoid putting it at risk. The reduction they accept is the risk premium.
2. Aversion to loss: with a point of reference of EUR 100, the risk premium for a lottery where there is a possibility of loss (for example, one that offers the same probability of winning EUR 90 or EUR 110) will be higher than for a wins-only lottery (for example, one that offers the same probability of winning EUR 100 or EUR 120). The same person would be ready to pay a risk premium of EUR 5 in the first instance (deterministic win of EUR 95) but only EUR 3 in the second case (deterministic gain of EUR 107).
3. Lastly, people have a tendency to distort low probabilities of very high gains (optimism bias) and high losses (pessimism bias).

Where major risks to society are concerned, a further distortion pertains. It is related to the scale of an incident and to the fact that society seems less able to tolerate major disasters than repeated incidents, even when the total number of victims is the same in both cases. This is an *aggregation bias*. The figure attached shows experimental data/perception pairs for a certain number of familiar causes of death.

In other words, it seems that society as a whole would more easily tolerate a series of accidents each causing minor damage than a single accident that causes major damage, even when losses are the same: for instance, judging by the various indicators that inform policy discussions or the column inches in newspapers, 5 000 road accidents each causing one death has less of an "impact" on us than five air transport accidents each causing 1 000 deaths. This comparison does not mean that we should resign ourselves to abandoning risk management policies. On the contrary, it is something that more responsible risk management should think about.

Figure 4. **Distortion of death numbers:**
in abscissa, actual number of deaths per year for some sets of causes;
in ordinate, estimated number of deaths



Source: Lichtenstein *et al.*, 1978.

Quite obviously, these perceptions differ from a normative (expected utility theory) and descriptive (behavioural finance theories, see Thaler, 1993) perspectives. Cost-benefit analysis proposes a method for allocating public resources to choices that offer the best combination of efficiency and equity. Resource allocation is also subject to acceptability criteria for investment decisions[9]. We have seen that the public's perceptions are subject to perception bias and other anomalies which mean that it is far removed from the rational man whom classic economic theory viewed as taking decisions without bias and free of influence.

7. CONCLUSIONS: ANY TERRORIST WORTHY OF THE NAME HAS SOMETHING TO LOSE

I will close with these few pointers. While the logic of Aristotle described man as conceived by philosophy, now in a dramatic turnaround, we are attempting to gain a better understanding of real men and women. Psychology and economics have done better than follow this general trend in the scientific approach. Risk calculation is no longer a disembodied normative ideal. Today, it assesses the real-life contexts in which evaluation and decisions take place.

As regards economic transactions, it is institutions (whether Coase's firm, the marketplace of a provincial village or the IMF) that enable us to manage certain objectives that would not result spontaneously from social interactions.

Over the next few years, institutional creativity will be sorely needed. The stability provided will have to offset certain distortions in judgment and preferences, which psychologists and economists have learned to try to recognise today, now that we have moved on from simply establishing normative doctrines of rational action. Institutions allow us not to exploit the fact that the psychological attitudes of our partners can be taken into account[10]. They guarantee the viability of situations which, without them, could be disastrous.

In periods of great instability, it can be crucial to remain capable of seeing that negligence, hostility and incompetence are labels that we choose to cling to when we stop negotiating on the basis of partners' preferences and begin to fight with them: people who are negligent, incompetent or hostile are people we no longer negotiate with. Under these conditions, the input from economists cannot be to provide weapons for archaic rituals of execution and expulsion. Before helping to stamp out or control terrorists, before working out a theory that explains the flaws that allow us to predict, repress or explain them, economic science can help us, more simply, to continue to pay attention to the instability that threatens our own analyses and to the distortions that affect our perception of what is at stake and of the probabilities in instable transactions. Hence, economics stands poised to demonstrate that it is now a human science in its own right.

There is much evidence that any group of human beings is capable of dealing with probabilities. The pre-history of games, just like that of rituals, attests to this interest[11]. That is why risk – like language, tools, or kinship – can be said to be a constant of human society. This comment has relevance for more than simply theory. It has a bearing on decision-making in an unstable environment.

When groups of humans who are strangers meet, the radical instability of relationships that are neither codified nor institutionalised lead to rapid shifts in stakes that can swing from trade to war and back. A noteworthy analysis by Lévi-Strauss has provided a model for this instability[12]. It is this instability that institutions can channel. The risk of outbreaks of non-negotiable violence – certain of modalities of which have been given the name terrorism – is not external to the society we live in and therefore calls for social, political and economic solutions, not for the technical calculation of prevention or repression.

A memorable anecdote from Roman antiquity relates that pirates sailing in the vicinity of Scipio's home asked if they could pay homage to the great man (Valerius Maximus, 30). Informed readers think that it was actually the victor of Carthage they wished to honour; after all, as pirates worthy of the name, they had reaped the benefits of the annihilation of the only great maritime power in the western Mediterranean. Historians shown how barbarians and pirates are invariably an integral part of the economy of the Empire that they appear to be threatening from the outside[13]. That is the difficult but necessary analysis that we should preferably be capable of conducting, given the extreme events that the current changes in our world are bringing about. Economics could perhaps have some suggestions on the technical problems that this change is bringing. It can most certainly set us thinking.

NOTES

1. My thanks to Serge Pahaut for our many fruitful discussions together over the past few years. Nathalie Picard and Jean Picard submitted useful suggestions for improving the quality and readability of this paper. Lastly, Kurt van Dender also helped me to improve its presentation.

2. The lessons of history and anthropology warn us that we had best not draw the rash conclusion that any two things are linked unless they show a link everywhere they occur. As a concept, security actually has its roots deep in the prehistory of law. Whatever the interpretation proposed, in many civilisations it harks back to some solemnised form of public *ritualised* practice. Here, one should at least note that the different mutations that this family of practices has gone through extend to much more than the socially guaranteed recognition of individual entitlement as it relates to the power to buy and sell freely. In other words, while the object at stake often attracts enemies, it does not necessarily have an owner.

3. For reference, the amounts are of the order of the annual GDP of the US, which is currently around USD 15 000 billion.

4. See the discussions on this idea in Viscusi (2003).

5. Moreover, this is a theme that has been catalogued by folklorists: the devil offers to build a bridge when its construction falls behind schedule (Folktale AT 1191, Aarne and Thompson, 1964).

6. Expected value is obviously not necessarily part of the set of observable events. Hence, in the case of an unloaded, six-sided dice, the expected value is 21/6, or 3.5, a figure which does not appear on any side of the dice.

7. The value of this theory is that it revisits several fundamental issues: for their study on aversion to ambiguity (which inclines people to gamble more willingly when the probabilities are known), Tversky and Fox (1965), following the Ellsberg Paradox (1961), mention the *Treatise on probability* by Keynes (1921) which was published in the same year as Knight's doctoral dissertation (1921), in which the latter paved the way for Coase and married the theory of the firm with risk theory.

8. This applies particularly to public goods (transport infrastructure, environment infrastructure, etc.; see de Palma *et al.*, 2005, 2007, 2008).

9. We know that the Vienna School and von Mises (1940) tried to draw on the logical process of human action, praxeology, to avoid over-psychologising. A properly conducted psychological experiment cannot fail to reveal why it was rational for someone to do one thing or another under this or that set of circumstances.

10. We could mention the outstanding work done by Ascher (1991), which shows how points awarded for different outcomes of a game of chance played by the Iroquois Cayuga are proportional to the probability distributions of these outcomes.

11. Although this study of models was taken up again in his essay on the Nambikwara Indians and in some passages of *Tristes tropiques*, its first appearance was during the First World War (Lévi-Strauss, 1943). Many political studies try to describe terrorism in terms of unstable interactions, instead of pretending to reduce it to some explainable causes such as poverty, culture, etc. Let us mention here the recent work by Sageman (2004).

12. This is a classical subject from Roman and Chinese studies, to mention only two empires, but one could also mention the colossal study on international relations by Duroselle (1992).

BIBLIOGRAPHY

Aarne, A. and S. Thompson (1964), *The types of the folktale*, FF communications 184, Helsinki.

Allais, M. (1989), "Les lignes directrices de mon œuvre", Nobel Prize conference before the Royal Swedish Academy of Sciences (9.12.1988), *Annales d'économie et de statistique*, No. 14.

Albert, M. (2000), Interfuturs vingt ans après, in: *Décision, prospective, auto-organisation*. Mélanges en l'honneur de J. Lesourne, Paris, Dunod, pp. 306-317.

Ascher, M. (1994), *Ethnomathematics*, Chapman and Hall.

Auerswald, P., L. Branscomb, T.M. La Porte and E.O. Michel-Kerjan (2006), *Seeds of Disaster, Roots of response (How Private Action Can Reduce Public Vulnerability)*, Cambridge University Press.

Bernoulli, D. (1738), *Specimen theoriae novae de mensura sortis*. Eng. tr. "Exposition of a New Theory on the Measurement of Risk", *Econometrica,* 22, 23-36, 1954.

Coase, R.H. (1937), "The Nature of the Firm", *Economica*, 4, pp. 386-405.

de Palma, A. and E. Quinet (2005), *La tarification des transports*, *Enjeux et défis*. Paris, Economica.

de Palma, A., R. Lindsey and S. Proost (2007), *Investment and the Use of Tax and Toll Revenues in the Transport Sector*, Elsevier Science.

de Palma, A. and J.-L. Prigent (2008a), Hedging Global Environment Risks: an Option-based Portfolio. Insurance, *Automatica*, 1519-1531.

de Palma, A. and N. Picard (2008b), "Cardinal and ordinal measure of investor's risk aversion", Ecole Normale Supérieure de Cachan, Department of Economics and Management, mimeo.

de Palma, A., M. Ben-Akiva, D. Brownstone, C. Holt, T. Magnac, D. McFadden, P. Moffatt, N. Picard, K. Train, P. Wakker and J. Walker (2008c), Risk, "Uncertainty and Discrete Choice Models", *Marketing Letters.*

Diderot, D. (1773), *Paradoxe sur le Comédien*, Gallimard, 1994.

Duroselle, J.B. (1992), *Tout Empire périra*, Armand Colin.

Ellsberg, D. (1961), "Risk, Ambiguity and the Savage Axioms", *Quarterly Journal of Economics*, 75, 643-669.

Haig, A. (2003), "The promise and perils of our times", International symposium on *Sino-US-Europe relations in the new century*, Beijing.

Hauriou, M. (1925), “La théorie de l'institution et de la foundation”, *Cahiers de la Nouvelle Journée*, 4, pp. 2-45.

Kahneman, D. and A. Tversky (1979), “Prospect theory: An analysis of decisions under risk”, *Econometrica*, 47, 313-327.

Keynes, J.M. (1921), *A treatise on probability*, Macmillan.

Knight, F.H. (1921), *Risk, Uncertainty, and Profit*, University of Chicago Press, 1986. See his thesis on: *Theory of Business Profit* (Cornell University, 1916).

Lesourne, J. and Chr. Stoffaës (1996), *La prospective stratégique d'entreprise: de la réflexion à l'action*, Dunod (2nd ed., 2001).

Lesourne, J. (2000), *Un homme de notre siècle*, Odile Jacob.

Lévi-Strauss (1943), “Guerre et commerce chez les Indiens d'Amérique du Sud”, *Renaissance*, I, 1-2, 122-139.

Lichtenstein, S., P. Slovic, B. Fischhoff, M. Layman and B. Combs (1978), “Judged frequency of lethal Events”, *Journal of Experimental Psychology: Human Learning and Memory*, 4, 565.

Meusnier, N. (2005), “Nicolas, neveu exemplaire”, *Journ@l électronique d'histoire des probabilités et de la statistique*, 2, 1.

Olson, M.L., (1965), *The Logic of Collective Action: Public Goods and the Theory of Groups*, Harvard University Press.

Pascal, B. (1660), *Pensées*, Paris, Seuil, 1963; Eng. tr.: *Pensées*, Dutton, 1958.

Popper, K. (1961), “La logique des sciences sociales”, presentation for the German Sociology Society.

Prelec, D. (2004), “A Bayesian truth serum for subjective data”, *Science*, 306, 5695, 462-466.

Rousseau, J.-J. (1755), *Discours sur l'origine et les fondements de l'inégalité*, Gallimard, 1989.

Sageman, M. (2004), *Understanding Terror Networks*, University of Pennsylvania Press.

Simon, H.A. (1982), *Models of Bounded Rationality*, MIT Press.

Stiglitz J. and L. Bilmes (2008), *The Three Trillion Dollar War*, Norton.

Thaler, R.H. (1993), *Advances in Behavioral Finance*, Russel Sage Foundation.

Tversky, A. and C. Fox (1995), “Weighting risk and uncertainty”, *Psychological Review*, 1995, 102, 2, 269-283.

Tversky, A. and Kahneman, D. (1992), “Advances in prospect theory: cumulative representation of uncertainty”, *Journal of Risk and Uncertainty*, 5, 1992, 297-323.

Valerius Maximus, G. (31), *Faits et dits mémorables*, Belles lettres, 2005.

Viscusi, K. (2003), *The Risks of Terrorism*, Kluwer.

Von Mises, L. (1940), *Nationalökonomie. Theorie Des Handelns und Wirtschaftens.* Eng. tr.: *Human Action: A Treatise on Economics*, Foundation for Economic Education, 1996.

von Neumann, J. and O. Morgenstern (1944), *Theory of Games and Economic Behavior*, Princeton University Press.

ECONOMIC IMPACT ANALYSIS OF TERRORISM EVENTS: RECENT METHODOLOGICAL ADVANCES AND FINDINGS

Peter GORDON
James E. MOORE, II
and
Harry W. RICHARDSON*

Center for Risk and Economic Analysis of Terrorist Events (CREATE)
University of Southern California
Los Angeles, Ca.
USA

SUMMARY

Los Angeles, November 2008

ABSTRACT

National security is a basic responsibility of national governments, but it is also intangible. What can economic analysis contribute? Benefit-cost analysis has rarely been applied because of the ambiguous and commons nature of the benefits. Our group at the University of Southern California's Center for Risk and Economic Analysis of Terrorism (CREATE) has worked to elaborate and apply economic impact analysis to describe the expected losses from various hypothetical terrorist attacks. Our innovation has been to add a spatial dimension to operational inter-industry models.

Plausible terrorist attack scenarios must include geographic detail. First, there is no generic national seaport, airport or similar targets. Second, most political decision makers represent geographic areas and have a keen interest in their local constituencies. Third, aggregation over spatial units may net out conditions where areas and sectors lose but others gain, especially if locations outside the impact area take over the functions that have been lost elsewhere. Fourth, by considering the spatial economy, interactions between places that rely on available infrastructure can be analysed.

This paper describes our modelling approaches (a metropolitan region model and two national models) as well as several of the results that we have developed. Our models are not formal cost-benefit analyses, but they demonstrate large business interruption costs from these events, implying that the results provide a rationale for expenditures on the benefits of protection and mitigation. We will also discuss important directions in which models such as ours could become the basis of some type of cost-benefit analysis.

*The authors would like to thank Ji Young Park and Qisheng Pan for their outstanding assistance.

1. INTRODUCTION

The US did not suffer enduring economic losses from the attacks of September 11, 2001. Estimates of GDP losses range from USD 22 to USD 34 billion; estimates of structure losses range from USD 27 billion to USD 95 billion[1]. But the former have to be qualified by the fact that the nation was in a mild recession in 2001, making the identification of terrorism-induced GDP losses difficult. US GDP in 2001 was more than USD 10 trillion, indicating that the estimated losses were smaller than might have been feared.

Significant impacts on government expenditures came later via the wars waged in Afghanistan and Iraq and the increased budgets for homeland security measures. Furthermore, enough time has elapsed since 2001 to ease any fears of a long-term productivity and/or output shock. The economic downturn of 2007-2008 is explained by credit market contractions, the mortgage crisis and commodity price increases that probably have nothing to do with the events of 2001.

However, proper risk management and contingency planning require efforts to understand the nature of any future attacks better. After all, through most of the Cold War, planners and policymakers developed scenarios to simulate the losses from hypothetical nuclear attacks.

The threats of transnational terrorism are different. First, there have been relatively few annual average fatalities from terrorist attacks. (Sandler *et al.*, 2008). Therefore, application of traditional cost-benefit analysis is probably inappropriate. Even if all fatalities could be averted, the benefits (the monetary value of deaths avoided using conventional statistical measures of the value of a life) are very small compared to the costs of achieving these benefits. Second, there is an uncountable number of global targets that terrorists consider attacking. It is impossible to protect them all.

These observations clarify the research challenge. The two realities cited make it important for homeland defence and national security decision makers to identify targets that are the most critical and harden these as much as possible. But how can these key targets be identified?

The task involves two research challenges. First, specify plausible attack scenarios. Given the capabilities of terrorists, which attacks could they plausibly execute? Second, estimate the economic losses from such attacks. Our interest is in the latter, but we rely on the work of other experts colleagues for the former.

In our work on a possible “dirty” bomb attack (i.e. a radiological device) on the twin ports of Los Angeles and Long Beach, we relied on the work of Rossoff and von Winterfeldt (2007), who examined 36 possible attack scenarios and reduced these to the two most plausible. We used their scenario information to apply the Southern California Planning Model (version 2 is discussed in what follows, SCPM) and the National Interstate Economic Model (NIEMO) to estimate plausible business interruption losses by industry and by place in the greater Los Angeles metropolitan area and beyond. This discussion, elaborated in Section 3, which highlights one of several examples that we present in order to establish the point that spatially detailed information is essential.

We discuss several applications of both of our models, starting with an application of the models to the same hypothetical attack. We also introduce a third model currently being developed, TransNIEMO, which integrates features of each approach. It adds an interregional highway model to NIEMO, allowing us to trace the economic impacts of various hypothetical shipment disruptions anywhere on the national highway network, one which includes thousands of major bridges. Credible cost-benefit analysis of protecting key bridges or tunnels requires a model that integrates the economy with the highway network.

2. OPERATIONAL MODELS[2]

2.1. The Southern California Planning Model (SCPM)

Inter-industry models, based on the transactions flows between intermediate suppliers and end producers, are widely used to measure regional economic impacts. They trace all economic impacts, including those of intra- and interregional shipments, usually at a high level of sectoral disaggregation. They are usually demand-driven, although there are some supply-driven applications.

The input-output model component of both models discussed in this paper is from the Minnesota Planning Group’s well-known IMPLAN model, which has a high degree of sectoral disaggregation (over 500 sectors). To make these data compatible with data from other sources, we aggregated them to 47 sectors, which we label the USC sectors. The second basic model component of SCPM is spatial; it allocates sectoral impacts across more than 3 000 small geographic zones (Traffic Analysis Zones, TAZs) throughout Southern California (the five-county region of greater Los Angeles). *The key capability of the model is to allocate the indirect and induced impacts generated by the input-output model spatially to these TAZs*. The direct impacts are always the final demand changes at the site of the attack (in this case, at the ports); the indirect effects trace the inter-industry linkages with other sectors, either forwards or backwards (locally, regionally, nationally and internationally); and the induced effects measure the secondary consumption impacts associated with the reduced spending of workers in both the direct and indirect sectors. To estimate the latter, we use a journey-to-work matrix that shows all the commuting flows between residential zones and workplace zones to trace wages earned back to the home and then we use a journey-to-services matrix to trace retail and personal service purchases from the home to retail and service establishments. This follows the logic first proposed by Ira Lowry (1964) and elaborated by Garin (1966). The journey-to-services matrix includes any trip associated with a home-based transaction other than the sale of labour to an employer. This includes retail trips and other service transaction trips, but excludes non-transaction-based trips such as trips to visit friends and relatives.

SCPM endogenizes traffic flows. It uses TAZs for traffic nodes. This feature of the model is important, because many types of terrorist attack are likely to induce changes in supply, including infrastructure capacity losses that will contribute to reductions in network level service and increases in travel delays.

Because traffic flows are endogenous, any change in economic activity that affects the travel behaviour of individuals or the movement of freight will influence how the transportation network is used and these impacts will work themselves out as a change from one network equilibrium to another. This means that the model has the important capability to estimate losses from concurrent attacks against shipping, infrastructure and productive capacity.

Treating the transportation network and its capabilities explicitly endogenizes the otherwise exogenous travel behaviour of households and intraregional freight flows, achieving consistency across network costs and origin-destination requirements. The model makes explicit distance-decay (i.e. the decline in the number of trips with increasing distance) and congestion functions (the build-up of traffic congestion and delay costs as particular routes attract more traffic when other parts of the network are disrupted).

This capability allows us to determine the geographical location of indirect and induced economic losses; essentially, we are endogenizing route and destination choice. This also enables us to allocate indirect and induced economic losses over TAZs in response to port-related direct losses in trade, employment and transportation accessibility more accurately. See Cho *et al.* (2001) for a technical summary of an earlier version of this model).

A flow chart of the model is shown in Figure 1.

Figure 1. **Southern California Planning Model (SCPM) 2005 Flow Chart**

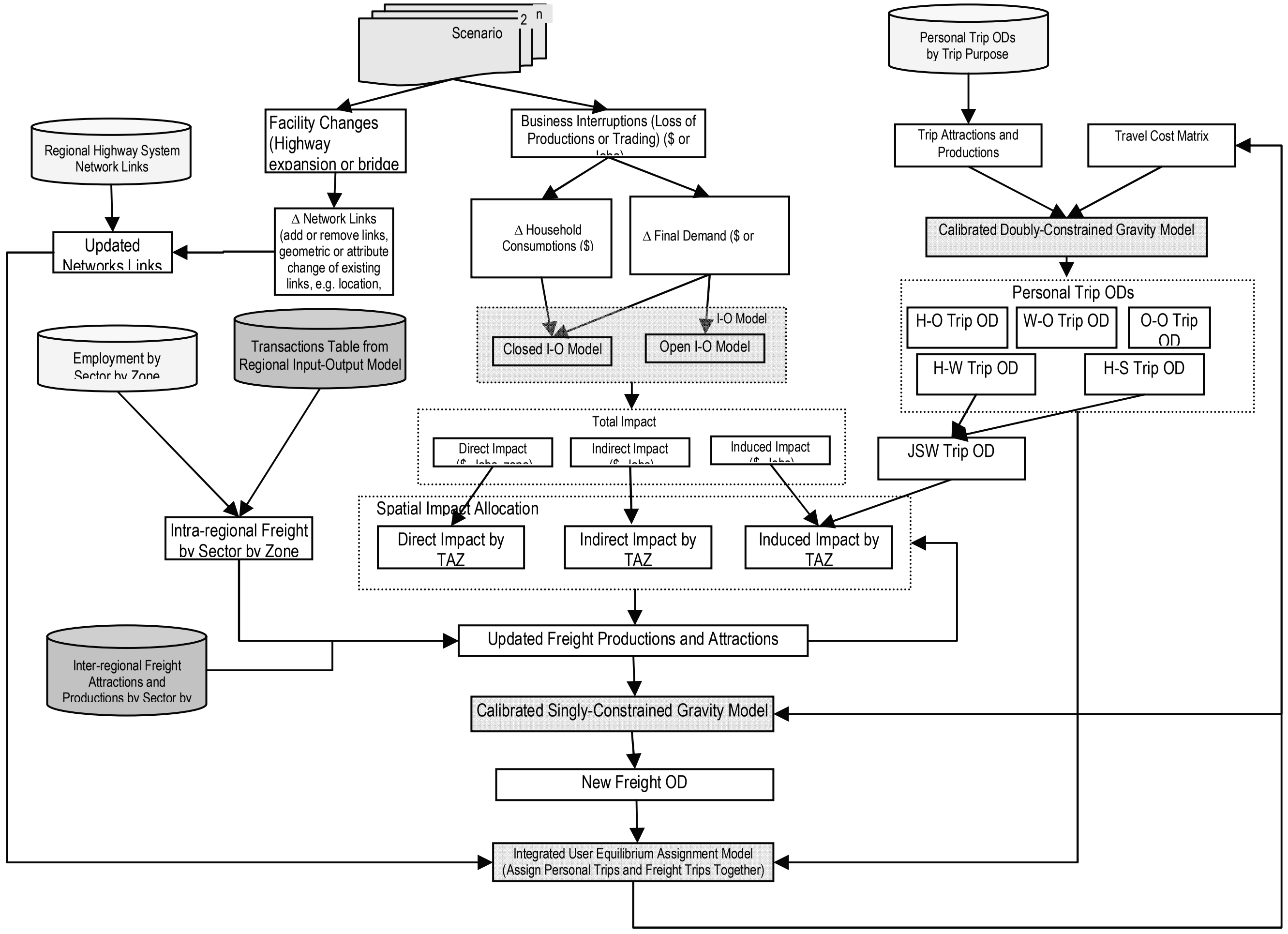

Scenario
2
n
Facility Changes (Highway expansion or bridge
Business Interruptions (Loss of Productions or Trading) ($ or Jobs)
Regional Highway System Network Links
Updated Networks Links
Δ Network Links (add or remove links, geometric or attribute change of existing links, e.g. location,
Δ Household Consumptions ($)
Δ Final Demand ($ or
I-O Model
Closed I-O Model
Open I-O Model
Employment by Sector by Zone
Transactions Table from Regional Input-Output Model
Total Impact
Direct Impact ($, Jobs, zone)
Indirect Impact ($, Jobs)
Induced Impact ($, Jobs)
Spatial Impact Allocation
Direct Impact by TAZ
Indirect Impact by TAZ
Induced Impact by TAZ
Intra-regional Freight by Sector by Zone
Inter-regional Freight Attractions and Productions by Sector by
Updated Freight Productions and Attractions
Calibrated Singly-Constrained Gravity Model
New Freight OD
Integrated User Equilibrium Assignment Model (Assign Personal Trips and Freight Trips Together)
Personal Trip ODs by Trip Purpose
Trip Attractions and Productions
Travel Cost Matrix
Calibrated Doubly-Constrained Gravity Model
Personal Trip ODs
H-O Trip OD
W-O Trip OD
O-O Trip OD
H-W Trip OD
H-S Trip OD
JSW Trip OD

Figure 1 Notes:

1. Baseline is established when all the changes (Δnetwork, Δfinal demand and Δ Household Consumptions) are zero

2. Initial travel cost matrix is established by loading empty personal and freight trip ODs to road network

3. User equilibrium is approached by multiple loops until the changes of objective function values become flat.

4. H-O, W-O, O-O, H-W, H-S are home-other, work-other, other-other, home-work and home-shop trip matrix.

5. JSW is journal-shop-to-work trip matrix.

6. Inter-regional freight attractions and productions are inbound and outbound freight trips at major freight generators (ports, airports, rail yards, warehouse/distribution nodes and highway entry-exit points).

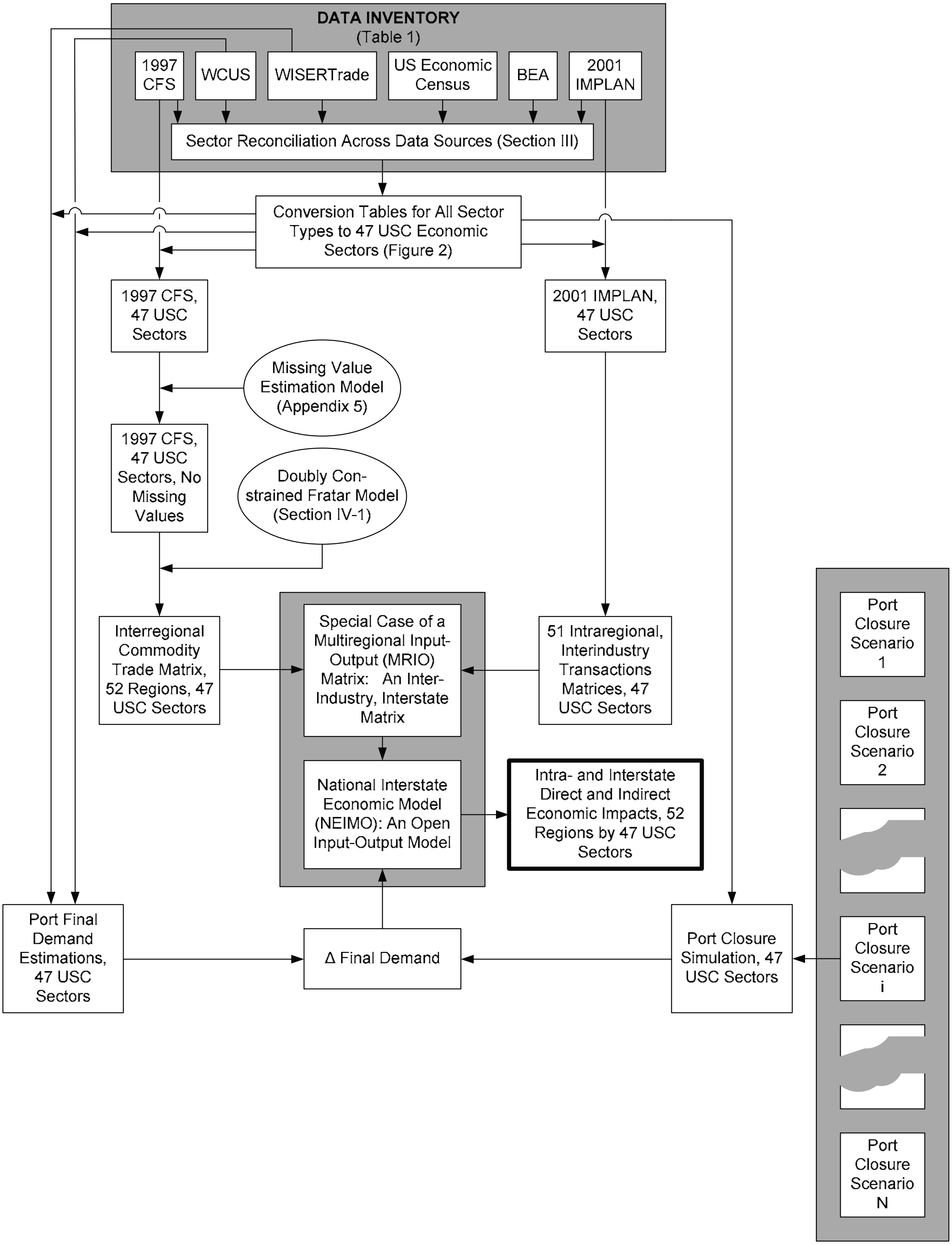
Please see “Assembled and processed freight shipment data by developing a GIS-Based origin-destination matrix for Southern California freight flows,” “Freight Data Assembling and Modelling: Methodologies and Practice,” and “Estimating Freight Flows for Metropolitan Area Highway Networks Using Secondary Data Sources” for details about inter-regional freight data collection and processing.

2.2. NIEMO (the National Interstate Economic Model)

In pursuing our research goal of creating operational models with sectoral and spatial detail, the choice of approaches involved difficult trade-offs. The use of linear economic models is justified by various factors, including the richness of the detailed results achieved at relatively low cost. NIEMO, for example, includes approximately 6 million multipliers. The principal insight that drives our research is that, with some effort, it is possible to integrate data from MIG, Inc.'s IMPLAN state-level input-output (IO) models with commodity flow (interstate shipments) data from the Department of Transportation's Commodity Flow Survey (and some other sources) for all individual States. The details of how NIEMO was constructed can be found in Park *et al.* (2007). Essentially the model is an operational version of the Chenery-Moses multi-regional input-output model (MRIO) that involves the 50 US States (plus the District of Columbia) and the 47 USC sectors. A flow chart of this model is shown in Figure 2.

And just as there are demand-driven and supply-driven, input-output models, we have developed demand-driven and supply driven versions of NIEMO. In each case, the supply-driven approach is most plausibly applied for the case of short-run disruptions. The interruption of purchasing by firms will have short term multiplier effects and the interruption of sales can also have short-term multiplier effects. Interrupting port services can cause both kinds of problems. Interrupted export opportunities suggest the application of the demand-side model. The case of interrupted imports is less clear because some are for final users while some are supplies to intermediate users.

Figure 2. **National Interstate Economic Model (NIEMO)**


DATA INVENTORY
(Table 1)
1997 CFS
WCUS
WISERTrade
US Economic Census
BEA
2001 IMPLAN
Sector Reconciliation Across Data Sources (Section III)
Conversion Tables for All Sector Types to 47 USC Economic Sectors (Figure 2)
1997 CFS, 47 USC Sectors
2001 IMPLAN, 47 USC Sectors
Missing Value Estimation Model (Appendix 5)
1997 CFS, 47 USC Sectors, No Missing Values
Doubly Con-strained Fratar Model (Section IV-1)
Interregional Commodity Trade Matrix, 52 Regions, 47 USC Sectors
Special Case of a Multiregional Input-Output (MRIO) Matrix: An Inter-Industry, Interstate Matrix
51 Intraregional, Interindustry Transactions Matrices, 47 USC Sectors
National Interstate Economic Model (NEIMO): An Open Input-Output Model
Intra- and Interstate Direct and Indirect Economic Impacts, 52 Regions by 47 USC Sectors
Port Final Demand Estimations, 47 USC Sectors
Δ Final Demand
Port Closure Simulation, 47 USC Sectors
Port Closure Scenario 1
Port Closure Scenario 2
Port Closure Scenario i
Port Closure Scenario N

3. APPLYING TWO OPERATIONAL ECONOMIC IMPACT MODELS TO SIMULATIONS OF HYPOTHETICAL ATTACKS

3.1. The Los Angeles/Long Beach Harbors

There are two adjacent ports in Southern California. Though administered separately, we treat them as one. The Los Angeles/Long Beach ports' role in the local and national economy is widely recognized. In a metropolitan region of more than 16.4 million people with a labour force of almost 7.5 million, the twin ports account for 111 million tons of seaborne trade and are the fifth largest port complex in the world after Hong Kong, Singapore, Shanghai and Shenzen. Directly and indirectly, the two Los Angeles ports employ 600 000 workers, accounting for more than seven per cent of the region's labour force. In terms of containerized traffic, the two ports rank first and second nationally. Their combined import and export trade flows of USD 300 billion (2004 data) is equivalent to about 30 per cent of the greater Los Angeles area gross regional product. Reflecting trends in the national economy, imports are much larger than exports. About one-half of the imports and two-thirds of the exports are to and from outside the region. The ports fulfil a national function; any loss of transhipment capabilities at these sites would have profound impacts both locally and nationally.

Such impacts would be much wider than a short-term deprivation of imported purchases by consumers or deferred export sales by producers. The supply chains for imported raw materials and intermediate inputs are would be interrupted and, as a result, the productive capacity of firms both inside and outside the region is reduced.

In the first application discussed, we assume that both export and import flows currently using local seaport facilities would terminate for as long as the ports were out of service. We have not yet modelled port diversion, but plan to do so in future research probably beginning with a survey of fleet operators.

We have applied SCPM to explorations of simultaneous radiological bomb attacks on the twin ports of Los Angeles and Long Beach. These could either be brought in by containers or planted within the country very close to the port perimeter, assuming that the terrorists have access to suitable radioactive material within the United States. The extent of the disruption would depend on the size of the bombs. Following Rossoff and von Winterfeldt (2007), we assumed the explosion of two small RDDs (radiological dispersal devices), each of them containing 5lbs of high explosive, more or less simultaneously at the two ports. The attack would require the closure of both ports on health even more than on security grounds. When the ports might reopen would be a policy rather than a technical decision, but without the transportation access the reopening would have minimal consequences

Although we estimated that the closure of the Los Angeles and Long Beach Ports for anywhere from 15 to 120 days (for the latter case we combined the radiological bomb attacks with conventional bombs blowing up three key access bridges/overpasses), Panel B of Table 1 (in Annex) shows the range of possible losses for various scenarios involving the plume of radioactive effects. Panel C is a summary of worst-case effects from port closure *and* plume effects. It could cost the US economy almost USD 49 billion – or more than 322 500 person-years of employment. Recall that SCPM actually reports results in much greater detail, to the level of census tracts or traffic analysis zones if required.

3.2. Plume Effects of the Harbour Attack

SCPM also made it possible to measure the economic impacts of plume effects in terms of household disruption, business losses and the decline in real estate values. This part of the simulation is discussed separately because it illustrates the complexity (and the benefits) of estimating traffic impacts simultaneously with economic impacts. The numbers shown are somewhat speculative, but our best estimate is a USD 4 billion loss in output and close to a decline of 42 600 person-years of employment. Blast damage would be limited, with deaths and serious injuries within a range of perhaps 50 metres and with moderate damage to physical infrastructure, except at ground zero. The outer evacuation zone would include all areas with exposure > 1 REM. We assume a hypothetical radiation plume, a long narrow ellipse four kilometres long and more than 200 metres wide with an inner and more contaminated zone of about 100 metres radius (an area of 0.03 km^2); there are standard formulae for converting releases of Curies of radiation to plume areas and shapes, subject to wind direction and other climatic conditions. In the ports case, the wind usually comes in from the South West, so the plume would not affect Los Angeles International Airport or other strategic locations except for the ports themselves. The critical early phase of exposure lasts about 4 days (EPA guidelines); the time frame for intermediate and later phases is variable and subjective and could range from weeks to years. We assume a one-week evacuation in the Outer Zone. With respect to the Outer Zone, this may be conservative because some firms and households may only slowly return with a lag after given permission to return. Health factors may dictate an immediate evacuation, but because the health effects are long-term, the decision to allow a return will be determined more by political than scientific considerations.

The more speculative economic impact consequences of a radiological bomb attack relate to the radiation plume. They depend on many variables: the size of the bomb, the amount of the radioactive release, the wind direction and prevailing climatic conditions and the downwind population and business densities. Moreover, much depends on the public policy reaction, for example, whether to mandate an evacuation and, if so, when to allow people to come back; or whether to proceed in a more measured if less cautious manner. Given these uncertainties, we report here only our best estimate of the *maximum* economic impacts of the plume to compare with the economic effects of the interruption of trade to and from the ports. By maximum, we mean under a reasonable set of assumptions.

Net input-output effects are very modest because shopping and services consumption shifts to other locations outside the plume area. Specifically, we assume in the first year after the attack a 25 per cent drop in residential property values, a 25 per cent reduction in retail trade, a 10 per cent fall in other business activities and that these businesses leave the region. An alternative assumption is that the businesses might relocate elsewhere in the region in which case the impacts would be primarily redistributional from a spatial perspective and the net effects would be minimal.

As for travel behaviour, we assume that driving through the plume area, with attendant advice about rolled-up windows, the use of air conditioning and regular car washing, will be permitted, rather than the more extreme measure of closing entry and exit roads, especially the freeways. However, there are network effects as the average length of personal trips increase as plume area residents are forced to shop and access services outside their neighbourhoods. Although there are fewer total trips, longer trips and more congestion results in significantly higher network costs. Our calculations of the additional network costs yield an estimate of USD 1.63 billion, based on a personal trip imputed cost of USD 13 per hour and a freight trip cost of USD 35 per PCE (Passenger Car Equivalent, based on the convention that one truck is the equivalent of 2.25 cars).

Based on the US Census of 2000, there were 401 147 persons living in the 30 TAZs of the impact area. The evacuated population would be 377 442. Table 1 (Panel B) summarizes the input-output consequences of reduced economic activity and lower property values in the outer plume area. The total output loss is more than USD 4.1 billion, of which only a small part, about USD 167 million, is associated with the decline in property values. Two-thirds of the losses take place within Los Angeles County and almost one-quarter leak outside the region. In terms of employment, the total job losses are 44 555 person-years of employment.

3.3. Plume effects of an attack on the Los Angeles CBD

To further illustrate our approach and for comparison, we have also undertaken another study of a radiological bomb attack, in this case on a prominent downtown Los Angeles office building. A radiological bomb attack on downtown Los Angeles might be a USD 6 billion event. If a similar attack were mounted in more CBD-oriented metropolitan areas (such as New York, Chicago or San Francisco), the economic impacts would be much larger. An attack on downtown would much less damaging than a similar attack on the ports because the economic disruptions resulting from closure of America’s largest port complex (in terms of USD of trade) would be far greater than a disruption to Los Angeles’ modest financial and office sector.

An important difference between an attack on the ports and an attack on downtown is that the critical public policy reactions might vary significantly in the two cases. In the ports case, there would be more economic pressure for the ports to reopen quickly and it would be feasible to put the port workers and/or the military back to handling trade (with protective clothing and equipment if necessary). In the downtown case, there are public spaces and more of the general public involved, and this might imply much more caution in allowing activities to resume sooner rather than later, especially in the inner plume zone.

3.4. NIEMO simulation of an attack on the Los Angeles/Long Beach harbors

We have not applied NIEMO to precisely same attack on the Los Angeles and Long Beach Ports discussed previously. But Table 2 (see Annex) shows results from the simulation of a slightly different scenario. The point that we want to make is that the sub-metropolitan results available from SCPM can be derived along with relevant state-by-state impact information. NIEMO applications to studies of this type are made possible by detailed (sector-specific and monthly) waterborne trade information from WISERTrade for each major seaport.

The loss of export opportunities lends itself to demand-multiplier analysis. Interrupted seaport export opportunities, then, are the final demand changes that are processed by NIEMO. And we chose to be conservative and avoided also using a supply multiplier for the loss of imports. So only direct effects of import losses are included. Combining these, we see that total damage resulting one-month closure of the three largest US Seaports compare to the costs of an LA/LB closure in approximate importance of their size. NIEMO’s information on the effects on the other states showed, in each instance, that the impacts where in approximate proportion to the size of the state and its nearness to the port that was affected.

3.5. Other model applications

Table 3 summarizes some of the other NIEMO applications. We include results from our study of a hypothetical terrorist attack on other major seaports as well as on US theme parks.

The seaports study (Park, *et al.*, 2007) was carried out in the same way as the NIEMO application to Los Angeles-Long Beach described in the previous section. As before, multiplier effects are applied to the interrupted export opportunities while only the direct effects of lost import opportunities are included. Again, state-level impacts were roughly in proportion to the size of the state as well as its distance from the attack. Congressional representatives from anywhere can use these results for an estimate of how a distant port supports their local economy – and thereby assess their constituents' willingness to support its protection or reconstruction.

NIEMO is also useful for assessing the value of a variety of targets. Theme parks attract a national and an international clientele. They may also attract the attention of terrorists for the reason that terror can be a psychological as much as an economic weapon. For this application, we identified 13 major parks (including two clusters of parks) that may be tempting targets in light of their size and prominence. We gathered information on the number of annual visitors as well as the average length of stay and the nature and size of expenditures for each visit. We tested park closure for one month followed by 30 per cent operations for the next six months followed by slow recovery to full operations by the eighteenth month after the attack. This schedule of reduced visits defined the direct effects that were used for runs of NIEMO.

Various scenarios were studied. Were there impacts only on the theme park that was attacked? Or were there psychological spillover effects that affected visits to other major parks? And for each scenario, were there substitutions by visitors to, for example, the major national parks? Total losses were sensitive to these assumptions. Results are shown in Table 3.

4.TRANSNIEMO

Work in progress involves adding a representation of the national highway network to NIEMO. We call this TransNIEMO. Whereas the endogenization of interstate trade flows is an important step, it is equally important to consider the media over which trade flows occur. In discussions of possible terrorist targets, it is clear that these lifelines include important targets. All of this is all the more important in an era of dispersed settlement, increased container shipping and distribution centres.

The application of TransNIEMO involves three major steps:

i. Use NIEMO to estimate baseline interstate trade flows and allocate the portion using the highway network to shortest path routes;

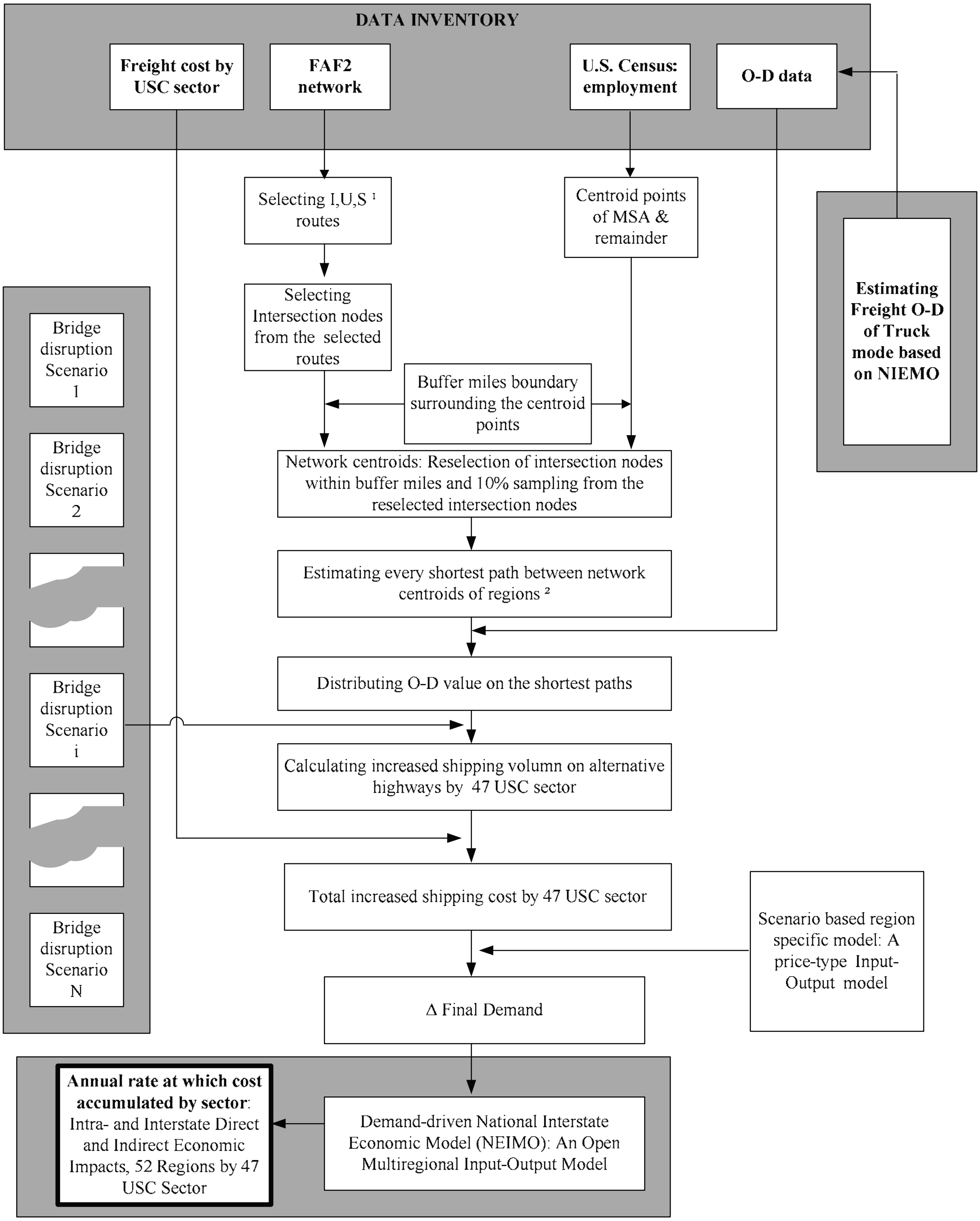
ii. Estimate increased costs due to re-routings on the modelled highway network system prompted by specific losses of network links; and

iii. Conduct state-by-state economic impact analysis by applying NIEMO again, to capture effects of decreased household consumption, resulting from price increase of products shipped via second-best routes.

The core idea of TransNIEMO involves the estimation of increased costs on the highway network system for a plausible scenario, e.g. destruction of a bridge. Figure 3 shows the framework for developing the model. The first major step in developing this model is to allocate commodity trade flows to the highway network, which accommodates approximately 73 per cent of total trade flows. The National Highway Planning Network (NHPN) has about 452 000 miles of roads, of which the Freight Analysis Framework (FAF) contains 245 500 miles. This includes 46 380 miles of Interstate Highways, 162 000 miles of National Highway System (NHS) roads, 35 000 miles of other national roads and 2 125 miles of urban streets and rural minor arterials, as well as many bridges and tunnels. However, rail, air and water networks cannot be ignored, and we plan to address integrating the other modes in future research.

Not surprisingly, combining the FHWA FAF network with NIEMO to create TransNIEMO involved many data manipulation and management challenges, because the FAF network seems to have been compiled from multiple sources. In addition, modelling transportation flows on a national network connecting urban centres includes requirements not associated with metropolitan level models. In particular, the national network is very complex. Economic space must be represented in a more aggregate way, making procedures for allocating freight demand to physical facilities much less obvious than in the metropolitan case. Our group has invested considerable attention in identifying meaningful, computationally tractable means of representing the details of the national economy in a way that articulates with the national highway network.

Figure 3. **TransNIEMO: NIEMO plus the road network**


DATA INVENTORY
Freight cost by USC sector
FAF2 network
U.S. Census: employment
O-D data
Selecting I,U,S ¹ routes
Centroid points of MSA & remainder
Estimating Freight O-D of Truck mode based on NIEMO
Selecting Intersection nodes from the selected routes
Buffer miles boundary surrounding the centroid points
Bridge disruption Scenario 1
Bridge disruption Scenario 2
Bridge disruption Scenario i
Bridge disruption Scenario N
Network centroids: Reselection of intersection nodes within buffer miles and 10% sampling from the reselected intersection nodes
Estimating every shortest path between network centroids of regions ²
Distributing O-D value on the shortest paths
Calculating increased shipping volumn on alternative highways by 47 USC sector
Total increased shipping cost by 47 USC sector
Scenario based region specific model: A price-type Input-Output model
Δ Final Demand
Annual rate at which cost accumulated by sector: Intra- and Interstate Direct and Indirect Economic Impacts, 52 Regions by 47 USC Sector
Demand-driven National Interstate Economic Model (NEIMO): An Open Multiregional Input-Output Model

We have, to date, made good progress and expect TransNIEMO to be operational very soon. We expect to apply it to the determination of the economic losses associated with the loss of any major highway link. This approach can also be the basis for assessing the value of any particular link, should a cost-benefit analysis rather than an impact study be necessary.

5. OTHER STUDIES

Our group undertook studies of two other terrorist issues that rely much less on our modelling methodologies. One is an attack on the airline system. One of the studies monitored the repercussions of the 9/11 attack. The loss estimates were large. When compared to the estimated costs of countermeasure deployment, it appears that the deployment is justified for a wide range of probabilities of attack. Using airport-level data to study the impact of the September 11th terrorist attacks on domestic air travel in the United States, the estimates are similar to those made by Ito and Lee (2005), who used nationally aggregated data in previous work. The study also found that 9/11 may have had more adverse impacts on large airports than on small airports. This could be the result of 9/11's various impacts (including its impact on risk perceptions and security procedures) being relatively severe in the case of large airports. It is also possible, however, that this result was the result of changing trends in the market for air travel. There was no evidence that east coast airports were more adversely affected than west coast airports, and it is possible that a companion study of international air travel would reveal somewhat different, perhaps stronger, results.

The second study used IMPLAN's national input-output model. A national model is preferred because the state-by-state airline revenue losses are difficult to estimate in light of the geographically dispersed nature of airline carriers and related infrastructure and vendors. In this case, the research considered the effects of a ground-based rocket attack on a single airplane. The scenario examined a seven-day shut-down of the entire US air transportation system, followed by a two-year period of recovery, using the post-9/11 experience of the system as a basis for analysis. The overall loss estimates for the two years range from USD 214 billion to USD 420 billion. There have been two other precursor attempts to model a disruption of the US air transport system. Balvanyos and Lave (2005) estimated consumer surplus losses from an air travel shut down and reported that the estimated loss would be up to USD 2 billion per day. Santos and Haimes (2004) have published results from an input-output impact simulation of a 10-per cent air transport system shutdown (USD 12 billion of direct effects). These authors derived input-output multipliers of 1.2 (Type I) and 3.6 (Type II) for the US to estimated a range of total losses from USD 14.2 billion to USD 43 billion for the year. Although our numbers are much higher, all the studies tend to justify that protective investments are justified, unless the probability of attack is perceived as very low.

Our research group also undertook two companion studies of the possible effects of border closure associated with a pandemic avian flu outbreak. This could be either a natural event or a planned terrorist attack. Such an attack might lead to an extreme response, border closure. This would include no international migration, no international travel and no commodity trade (apart from oil imports) for a full year. The economic costs are very high, about USD 2.1 trillion, and the impacts vary from state to state (Gordon *et al.*, 2008). Interestingly, the magnitude of estimated costs is close to the cited median dollar value of expected loss of life (386 000 deaths according to Murray *et al.*, 2006). However, a problem with this type of research is how can we model extreme events? Most available models focus on perturbations at the margin. Yet, policy makers are compelled to think about events beyond the margin. For example, work by RAND researchers on the effects of nuclear attack makes use of "scenario analysis" and "strategic gaming" exercises that rely fundamentally on expert judgment (Meade and Molander, 2007; see also Carter, *et al.*, 2007).

The second study (Rose *et al.*, 2008), using a macroeconomic model (the REMI model) predicted a reduction in GDP of as much as USD 1.4 trillion measured in 2006 dollars, or about 10.5 per cent of GDP (Rose *et al.*, 2008). Employment losses were predicted to be over 22 million, or more than 12 per cent below base levels. The authors suggested that these estimates might be upper bounded, and that inclusion of several aspects of resilience, such as input substitution and domestic excess capacity, might reduce them.

6. CONCLUSIONS

This paper sums up some of the research that our economic modelling team at CREATE has been working on for the past three years. The research is both methodological and substantive. The methodological innovation is to emphasize the spatial dimensions of the economy. This requires trade flows and the networks over which they flow be recognized in the models. The substantive approach is to consider the business interruption consequences of bomb attacks, both radiological and conventional, at the twin ports of Los Angeles-Long Beach. The economic impacts are very substantial. Although the potential loss of life from terrorist attacks attracts more attention and, no doubt, would have serious psychological effects, the business interruption impacts are large enough to persuade terrorists that economic targets are as "productive" as human targets.

How can our modelling approaches support standard benefit-cost analysis? We introduced our approach by noting that it is comparatively simple to apply and that its findings could aid policy makers concerned with hardening vital facilities. We can also indicate that our models emphasize network effects and are, therefore, a prerequisite to cost-benefit analysis. The marginal value of any facility is only known once the system-wide losses of its removal are known. But system-wide losses can only be estimated once adaptations and substitutions have been examined. This is the value of TransNIEMO and explains our high hopes for its widespread application.

Our position is that, both, plausible terrorist attack scenarios and the proper models to use must include geographic detail. There are several reasons for this. First, there is no such thing as a generic national seaport or airport or other similar target. Second, most political decision makers represent geographic areas and have a keen interest in these constituencies. Third, aggregation over spatial units may net out important distinctions because there may be situations where there are areas and sectors with losses but others with gains, especially if locations outside the impact area take on the functions that have been lost. Fourth, by considering the spatial economy, interactions between places that rely heavily on the available infrastructure, including major seaports and airports, can be analyzed.

NOTES

1. Sources summarized in Appendix Table 4.
2. Parts of sections 2.1 and 2.2 are drawn from Richardson *et al.* (2008).

ANNEX

Table 1. **SCPM Impact Studies**

Studies	Scenarios	Impact Areas	Direct Output Loss (USD Mil)	Total Output Loss (USD Mil)	Direct Job Loss	Total Job Loss	Passenger Travel Cost Loss[*a] (USD Mil)	Freight Travel Cost Loss[*b] (USD Mil)	Total Travel Cost Loss (USD Mil)	Total Loss (USD Mil)
Port Closure	15-Day Closure of the Ports of Los Angeles and Long Beach[*1, 2]	City of Los Angeles	264	423	1 187	2 640				
		City of Long Beach	69	88	502	657				
		Los Angeles Region	946	1 522	4 354	9 606				
		Out of Region	1 782	2 736	8 050	16 914				
		Total	2 728	4 259	12 404	26 521	24	25	49	4 284
	120-Day Closure of the Ports of Los Angeles and Long Beach[*1 2 3]	City of Los Angeles	2 114	3 386	9 496	21 116				
		City of Long Beach	554	700	4 009	5 249				
		Los Angeles Region	7 564	12 179	34 831	76 850				
		Out of Region	14 256	21 892	64 401	135 316				
		Total	21 820	34 071	99 232	212 165	-207	117	-90	34 189

	One Year Closure of the Terminal Island[*2]	City of Los Angeles	2 849	4 538	13 087	28 503				
		City of Long Beach	621	816	4 143	5 787				
		Los Angeles Region	9 991	16 115	45 749	101 485				
		Out of Region	18 687	28 755	84 920	178 482				
		Total	28 678	44 870	130 669	279 967	-395	337	-58	45 207
Plume	All people in the plume area will evacuate for one week and they can travel through the plume area through highway and local roads	County of Los Angeles	0	0	0	0				
		Los Angeles Region	0	0	0	0				
		Out of Region	0	0	0	0				
		Total	0	0	0	0	-4 818	-436	-5 254	-5 254
	All businesses in the plume area are shut down for a week.	County of Los Angeles	0	0	0	0				
		Los Angeles Region	0	0	0	0				
		Out of Region	0	0	0	0				
		Total	0	0	0	0	-3 970	-923	-4 893	-4 893
	Property values in this area drop by 25% for a year, then come back to their original values	County of Los Angeles	86	118	1 163	1 498				
		Los Angeles Region	86	138	1 163	1 702				
		Out of Region	19	29	168	278				
		Total	104	167	1 332	1 981	104	-2	101	269

	Retail business drops by 25% for one year, due to customers not wanting to drive into these areas, then come back to their original levels	County of Los Angeles	0	0	0	0				
		Los Angeles Region	0	0	0	0				
		Out of Region	0	0	0	0				
		Total	0	0	0	0	68	21	89	89
	The impact area lost 25% Retail and 10% other businesses. The impacted businesses are gone rather than relocated to other part of the region.	County of Los Angeles	1 755	2 519	21 156	29 000				
		Los Angeles Region	1 755	2 981	21 156	33 828				
		Out of Region	576	970	4 856	8 741				
		Total	2 331	3 950	26 013	42 574	-232	-50	-281	3,669
	The impact area lost 25% Retail and 10% other businesses. They will be relocated to the area with maximum attractiveness to the origin and also within 30 minute travel time from the origin	County of Los Angeles	0	0	0	0				
		Los Angeles Region	0	0	0	0				
		Out of Region	0	0	0	0				
		Total	0	0	0	0	-290	-38	-328	-328

Worst Case Port Closure and Port Plume	One Year Closure of the Terminal Island	County of Los Angeles	8 662	13 434	53 369	97 535				
		Los Angeles Region	11 745	19 096	66 905	135 313				
		Out of Region	19 263	29 724	89 776	187 223				
		Total	31 009	48 820	156 682	322 541	-627	288	-339	48 877
Downtown Los Angeles	Exit Scenario for All Businesses and Households Moving out of the Inner and Outer Impact Zones[*4]	City of Los Angeles	2 304	2 941	7 257	13 389				
		Los Angeles Region	2 304	5 175	7 257	34 983				
		Out of Region	313	726	1 363	5 408				
		Total	2 617	5 901	8 620	40 391				5 901
	Relocation Scenario, for All Businesses and Households Moving out of the Inner and Outer Impact Zones and Relocating in the Region[*4]	City of Los Angeles	1 567	1 567	5 099	5 099				
		Los Angeles Region	0	0	0	0				
		Out of Region	0	0	0	0				
		Total	0	0	0	0				0
	Hybrid Scenario Inner Zone Firms Exit While Outer Zone Firms and Households Relocate[*4]	City of Los Angeles	2 162	2 771	6 643	12 503				
		Los Angeles Region	2 220	4 968	6 643	33 157				
		Out of Region	284	656	1 200	4 843				
		Total	2 504	5 624	7 843	38 000				5 624

Notes: a. Personal trip cost is assumed to be USD 13.00 per passenger car equivalent (PCE) per hour.
b. Freight trip cost is assumed to be USD 35.00 per PCE per hour.

Citations:

Port Closure

1. H. W. Richardson, P. Gordon, J. E. Moore, J. Park and Q. Pan (2008), “The economic impacts of alternative terrorist attacks on the twin ports of Los Angeles – Long Beach,” in J. M. Quigley and L. A. Rosenthal, eds., Risking House and Home: Disasters, Cities, Public Policy, Berkeley, California: Berkeley Public Policy Press.
2. Gordon, P., J. Moore, H. W. Richardson and Q. Pan (2006) “The costs of a terrorist attack on Terminal Island at the twin ports of Los Angeles and Long Beach, ” in J. Haveman and H. Schatz, eds., Protecting the Nation’s Seaports: Balancing Security and Cost, Public Policy Institute of California.
3. Gordon, P., J. Moore, H. W. Richardson and Q. Pan, (2005) “The economic impacts of a terrorist attack on the twin ports of Los Angeles – Long Beach,” in H. W. Richardson, P. Gordon and J. E. Moore, eds., The Economic Impacts of Terrorist Attacks, Cheltenham, UK: Edward Elgar Publishing.

Downtown LA

4. Pan, Q., Gordon, P., J. Moore and H. W. Richardson (2008) “Economic impacts of terrorist attacks and natural disasters: Case studies of Los Angeles and Houston,” in Daniel Z. Sui and Susan L. Cutter (ed.) Geospatial Technologies and Homeland Security: Research Frontiers and Challenges, Springer.
5. Pan. Q. , H. W. Richardson, P. Gordon and J. Moore (2007) “The Economic Impacts of a Terrorist Attack on the Downtown Los Angeles Financial District,” Spatial Economic Analysis (submitted and under review)

Table 2: **Sum of Intra- and Interstate Impacts Associated with a 120-day Shutdown of the Ports of Los Angeles and Long Beach** (USD M)

Location	**Impacts**	**Interstate Impacts Calculated via NIEMO**							
Southern CA	4 874.58	AL	106.35	IN	209.76	NE	99.9	RI	19.14
Rest of CA	5 545.64	AK	12.17	IA	142.25	NV	51.6	SC	66.12
Direct Impact: Exports:	16 233.20	AZ	211.83	KS	126.21	NH	28.48	SD	26.52
Direct Impact: Imports	56 107.13	AR	100.69	KY	115.05	NJ	167.	TN	132.92
US Total	89 817.26	CO	123.88	LA	307.54	NM	26.1	TX	1 546.39
Rest of World	492.02	CT	63.28	ME	21.25	NY	216.38	UT	125.31
World Total	90 309.29	DE	20.04	MD	45.09	NC	130.76	VM	9.51
		DC	2.47	MA	86.01	ND	19.22	VA	66.99
		FL	123.19	MI	216.96	OH	303.19	WA	313.64
		GA	102.26	MN	133.34	OK	106.47	WV	41.75
		HI	21.31	MS	57.91	OR	198.81	WI	208.17
		ID	48.57	MO	141.71	PA	243.81	WY	25.71
		IL	279.47	MT	64.21				

Table 3. **NIEMO Impact Studies**

Source of Economic Impact	Targets	Total Economic Impacts (USD M)					Base-year, Duration and Model
		Supply-side (or Imports)		Demand-side (or Exports)		Total	
		Direct Impacts	Indirect Impacts	Direct Impacts	Indirect Impacts		
Sea Ports Shut Down[1,2]	LA / LB,	14 222	0	4 115	4 921	23 258	2001, one-month, and demand-driven NIEMO
	Houston	3 219	0	3 141	3 690	10 050	
	NY / NW	6 700	0	4 694	5 430	16 824	
Theme Parks Shut Down[3]	Cluster A (FL)			14 185	10 736	24 921	2004, 18 months, and demand-driven NIEMO
	Cluster B (CA)			13 470	10 146	23 616	
	NV			11 944	8 991	20 935	
	FL (i)			11 884	8 974	20 858	
	CA (i)			11 933	9 006	20 939	
	OH (i)			11 886	8 988	20 874	
	OH (ii)			11 871	8 975	20 846	
	NJ (i)			11 866	8 949	20 815	
	CA (ii)			11 899	8 981	20 880	
	NJ (ii)			11 851	8 939	20 790	
	PA			11 836	8 941	20 777	
	VA			11 818	8 929	20 747	
	IL			11 839	8 942	20 782	

Citations:

1. Park, J.Y., P. Gordon, J. E. Moore II and H. W. Richardson, L. Wang, 2007, "Simulating The State-by-State Effects of Terrorist Attacks on Three Major US Ports: Applying NIEMO (National Interstate Economic Model)"p.208-234, in H.W. Richardson, P. Gordon and J.E. Moore II, eds., The Economic Costs and Consequences of Terrorism. Cheltenham: Edward Elgar.

2. Park, J.Y., 2008, "The Economic Impacts of a Dirty- Bomb Attack on the Los Angeles and Long Beach Port: Applying Supply-driven NIEMO," Journal of Homeland Security and Emergency Management, 5 (1), Article 21.

3. Richardson, H. W., P. Gordon, J. E. Moore, II, S.J. Kim, J.Y. Park and Q. Pan, 2007, "Tourism and Terrorism: The National and Interregional Economic Impacts of Attacks on Major US Theme Parks," p.235-253, in H.W. Richardson, P. Gordon and J.E. Moore II, eds., The Economic Costs and Consequences of Terrorism. Cheltenham: Edward Elgar.

Table 4. **Estimates of the Costs of the 9/11 Attack**

Total Costs (billions)	Capital Losses	Job Losses	Loss of Life	Airlines Losses	Disability	Travel	GDP[1]/ GCP	Other Costs	Total
New York City									
Bram *et al.* (2002)	21.6	3.6-6.4	7.8						33-36
Chernick & Haughwout (2006)	30						11.5	0.897	
Ito & Lee (2005)				1.1					
Looney (2002)	27.2								27.2
NY Governor and State Division of the Budget[2] (2001)	33.8							20.2	54
NY State Ways and Means Committee (2002)			11					16	27
NY State Senate Finance Committee[3] (2002)	33	15.145	4-6			4.6		0.341	57.1-59.1
NYC Office of the Comptroller (2002)	21.8		8.7		0.944		52.3-64.3	0.943	82.8-94.8
NYC Partnership and Chamber of Commerce[4] (2002)	44		10	0.75-1.0		7-11		7.6	83
United States									
DeVol *et al.* (2002)				1.1			175		176.1
NY State Senate Finance Committee[3] (2002)		424.4					639.3		639.3

Notes:

1. GDP is only used in the total estimate when it would not double count other costs. Some articles do not contain a total cost as they only examined specific aspects of the economy. Individual costs do not necessarily add up to total costs as some studies are incomplete.
2. It is unclear how the NYC Partnership and Chamber of Commerce counts different types of costs.
3. The NY State Senate Finance Committee uses the estimated amount of compensation claims for potential earnings. This article is also used twice: once for national losses and once for New York City losses. For the capital costs they used figures calculated by the NY Governor and State Division of the Budget and the New York City Mayor's Office.
4. The NY Governor and State Division of the Budget count USD 3 billion as losses from 9/11 that is actually part of a separate economic stimulus package, according to the GAO study, "Impact of Terrorist Attacks on the World Trade Center."

Assembled by Philip Partyka-Hall.

BIBLIOGRAPHY

Balvanyos, T. and L.B. Lave (2005), “The Economic Implications of Terrorist Attack on Commercial Aviation in the USA,” report to the Center for Risk and Economic Analysis of Terrorism (CREATE), University of Southern California, Los Angeles.

Carter, A.B., M.M. May and W.J. Perry (2007), “The Day After: Action Following a Nuclear Blast in a US City”, *Washington Quarterly*, 30: 19-32.

Cho, S., P. Gordon, J.E. Moore, II, H.W. Richardson, M. Shinozuka and S.E. Chang (2001), “Integrating Transportation Network and Regional Economic Models to Estimate the Costs of a Large Urban Earthquake”, *Journal of Regional Science*, **41** (1): 39-65.

Garin, R.A. (1966), “A Matrix Formulation of the Lowry Model for Intrametropolitan Activity Allocation”, *Journal of the American Institute of Planners,* **32**: 361-364.

Gordon, P, J.E. Moore, II, J.Y. Park and H.W. Richardson (2007), “The Economic Impacts of a Terrorist Attack on the US Commercial Aviation System”, *Risk Analysis*, **27**:505-512.

Gordon, P, J.E. Moore, II, J.Y. Park and H.W. Richardson (forthcoming), “The Economic Impacts of Border Closures: A State-by-State Analysis”, in H.W. Richardson, P. Gordon and J.E Moore, II (eds.), *Global Business and the Terrorist Threat*, Cheltenham, UK, Northampton, MA, USA: Edward Elgar.

Ito, H. and D. Lee (2005), “Assessing the Impact of the September 11 Terrorist Attacks on US Airline Demand”, *International Journal of the Economics of Business*, **57**:75-95.

Lowry, I.S. (1964), *A Model of Metropolis*, Report RM 4125-RC, Santa Monica: Rand.

Meade, C. and R.C. Molander (2007), *Considering the Effects of a Catastrophic Terrorist Attack*. Santa Monica, CA: Rand, Center for Terrorism and Risk Policy.

Murray, C.L., A.D. Lopez, B. Chin, D. Feehan and K.H. Hill (2006), “Estimation of potential global pandemic influenza mortality on the basis of vital registry data from the 1918-20 pandemic: a quantitative analysis,” *The Lancet*, 368, 2211-18.

Park, J., P. Gordon, J.E. Moore, II and H.W. Richardson (2007), “Simulating the State-by-State Effects of Terrorist Attacks on Three Major US Ports: Applying NIEMO”, in H.W. Richardson, P. Gordon and J.E. Moore, II (eds.), *The Economic Consequences of Terrorism*, Cheltenham, UK, Northampton, MA, USA: Edward Elgar, 208-234.

Richardson, H.W., P. Gordon, J.E. Moore, II, S. Kim, J. Park and Q. Pan (2007), “Tourism and Terrorism : the National and Interregional Economic Impacts of Attacks on Major US Theme

Parks", in H.W. Richardson, P. Gordon and J.E. Moore, II (eds.)., *The Economic Consequences of Terrorism*, Cheltenham, UK, Northampton, MA, USA: Edward Elgar, 235-253.

Richardson, H.W., P. Gordon, J.E. Moore, II, J. Park and Q. Pan (2008), "The Economic Impacts of Alternative Terrorist Attacks on the Twin Ports of Los Angeles and Long Beach", in J.M. Quigley and L.A. Rosenthal (eds.), *Risking House and Home: Disasters, Cities, and Public Policy*, Berkeley, California: Berkeley Public Policy Press, 173-19.

Rose, A., R.B.G. Asay, D. Wei and B. Leung (forthcoming), "Macroeconomic Impacts of Shutting down the US Borders in Response to a Security or Health Threat", in H.W. Richardson, P. Gordon and J.E. Moore, II, *Global Business and the Terrorist Threat,* Cheltenham, UK, Northampton, MA, USA: Edward Elgar.

Rossoff H. and D. von Winterfeldt (2007), "A risk and economic analysis of dirty bomb attacks on the ports of Los Angeles and Long Beach", *Risk Analysis*, **27** (3): 533-554.

Sandler, T., D.G. Arce and W. Enders (2008), *Terrorism*, Copenhagen Consensus 2008 Challenge Paper.

Santos, J.R. and Y.Y. Haimes (2004), "Modelling the Demand Reduction Input-Output (I-O) Inoperability Due to Terrorism of Interconnected Infrastructures", *Risk Analysis*, 24:6, 1437-1451.

TOWARDS A RISK-BASED AVIATION SECURITY POLICY

Robert W. POOLE, Jr.

Reason Foundation
Los Angeles, Ca.
USA

SUMMARY

Los Angeles, November 2008

1. INTRODUCTION

The well-coordinated terrorist attacks on Sept. 11, 2001 presented the world with a new aviation security threat: the capture of aircraft in flight to be used as human-guided missiles. The two previous threats – hijacking an aircraft for ransom and putting a bomb aboard an aircraft – had led to varying degrees of screening of baggage and passengers in developed countries, plus some use of on-board security personnel on selected flights in some countries.

In the wake of 9/11, governments in the United States, Canada, and Europe (at both national and EU levels) implemented a number of additional aviation security measures, among them:

- strengthened (and locked) cockpit doors;
- 100% screening of checked baggage;
- more thorough screening of passengers and their carry-on baggage;
- increased use of on-board security officers;
- increased attention to air cargo; and
- greater attention to airport access control and perimeter control.

Although the rhetoric of risk-assessment and claims that security policies are risk-based are often heard, much of the actual policy change appears to have been driven by political imperatives to reassure frightened populations that air travel is still safe. In the United States, for example, although the initial legislation, enacted within two months of the 9/11 attack, was called the Aviation and Transportation Security Act (ATSA), and it created the Transportation Security Administration, nominally to protect all of transportation, the vast majority of the TSA's budget has gone for legislatively mandated aviation security (with by far the largest share concentrated on passenger and baggage screening). No risk assessment preceded this statute's enactment, nor has this initial allocation of resources been changed significantly by the subsequent large-scale reorganization that created the multi-faceted Department of Homeland Security, into which the TSA and many other agencies were transferred.

Economics reminds us that resources are always limited, and that resources allocated to X are not available for Y. The challenge in dealing with terrorist threats – whether to a nation, a sector such as transportation, or a sub-sector such as aviation – is always one of deciding where to invest scarce resources to maximum benefit. This inevitably requires difficult choices to be made, and the premise of this paper is that risk assessment provides an essential framework for making such choices and should be applied more consistently to aviation security.

This paper is organised as follows. First, to provide context, it discusses macro-level considerations in countering terrorism. Next, it provides a provocative example of applying risk analysis to assess the cost-effectiveness of several post-9/11 aviation security measures. With that as background, the paper then compares and contrasts the post-9/11 aviation security policies of the USA, Canada, and the EU countries, with costs and risks as a principal focus. Finally, it provides suggestions for making aviation security policy more consistently risk-based.

2. CONTEXT: THE PROBLEM OF DEFENDING AGAINST TERRORISM

2.1. The basic problem

The sector-specific approach that has been applied to aviation is an example of target-hardening. The problem with this approach is that we live and function in a target-rich world, and this is inherent in the nature of developed economies. Because resources are limited, all conceivable targets cannot be hardened. But terrorists can readily shift from hardened to non-hardened targets. Target-hardening is an example of what analysts have called "asymmetries" between terrorists and their target governments. As Sandler, Arce, and Enders [1] point out, there are a number of such asymmetries. Terrorists operating in loosely connected networks appear to cooperate more readily than governments. Terrorists also seem to operate with longer time horizons than the political process. Because terrorists hide among the general population, they present a target-poor environment to governments, compared with the terrorists' target-rich environment. And the cost to terrorists of wreaking destruction and creating fear are modest, in comparison to the costs of governmental attempts to defend (everything) against terrorist attack.

2.2. Macro-policy alternatives to counter terrorism

In 2008, the Copenhagen Consensus project commissioned a challenge paper on terrorism. In the paper, Todd Sandler and Daniel Arce of the University of Texas at Dallas and Walter Enders of the University of Alabama focus on transnational terrorism as a problem fundamentally different from other global crises [1]. Their basic message is that "there is no solution to transnational terrorism because it is a cost-effective tactic of the weak against a more formidable opponent." Thus, they conclude, "terrorism can be put into remission but it cannot be eliminated."

To illustrate the difficulties involved in cost-effectively countering terrorism, they outline five conceptual global strategies and estimate the benefit/cost ratio of each. Before doing so, they discuss why doing benefit/cost (B/C) analysis is so difficult in the case of counter-terrorism efforts. First, there is no permanent solution, so benefits from a counter-terrorist strategy are likely to last only two to five years. Second, there is no reliable way to know what level of terrorist activity there would have been in the absence of the strategy. Third, the cost of such strategies is difficult to ascertain, since much information is classified.

The benefits of preventing terrorist actions consist primarily of the value of lives saved and injuries prevented, along with avoided reductions in gross domestic product (GDP). Because (at least thus far) terrorist incidents are infrequent and of relatively small impact, it turns out that homeland security expenditure, as a fraction of GDP, dwarfs the other variables in the B/C calculations, over a wide range of assumed values for the parameters.

The first of the five strategies, called "business as usual" is basically the current policies adopted by the developed world. The authors' B/C ratio for this is .095 – i.e. benefits of less than 10 cents per dollar spent. A policy of increased proactive steps (taking the battle to terrorist havens) would have much higher costs and somewhat larger benefits, resulting in a B/C ratio of .077. Augmented defensive measures (more-aggressive target-hardening globally) has an estimated B/C ratio of 0.28 - higher than the first two, but still far less than 1.0. A more sensitive foreign policy for western governments (instead of current measures), although the most difficult to evaluate, was judged to possibly have a B/C ratio exceeding 1.0. The only one of the five strategies estimated as having benefits considerably in excess of costs was “greater international cooperation” (such as freezing assets and cutting off terrorist resources, along with increased police cooperation among countries), as opposed to the current combination of target-hardening and striking at terrorist havens. The B/C ratio for this approach was estimated at 5.3 – but it was also considered the most difficult strategy to implement.

Overall, Sandler, Arce, and Enders conclude that “security-based solutions display adverse B/C (ratios)” and that it would be better to shift to low-cost strategies based on greater international cooperation and changed foreign policy.

One important caveat to this assessment is that the authors do not factor in possible terrorist use of biological, chemical, radiological, or nuclear materials, since their estimates of lives lost, injuries sustained, and reductions in GDP are based on historical trans-national terrorist activity, none of which has involved these more serious threats. Had data been available to quantify such costs, their B/C ratios for several of the strategies would have been “much larger”, they write. However, for our purposes, aviation does not appear to be a current target for such weapons.

2.3. The dynamics of counter-terrorism

The Maginot Line is a classic case of a static defence that failed. Target-hardening approaches risk making the same mistake, via the equivalent of building walls to prevent the previous kind of attack. But terrorists adapt to the creation of defences.

In *Breaching the Fortress Wall*, a nine-member RAND Corporation team sought to understand terrorist groups’ efforts to overcome defensive technologies [2]. Their 139-page assessment reviews four such groups, in Palestine, Southeast Asia, Sri Lanka, and Northern Ireland. Across the board, they found that terrorist groups responded to the use of defensive technologies by:

- Altering operational practices;
- Making technological changes or substitutions;
- Avoiding the defensive technology; or,
- Attacking the defensive technology.

In the case of technologies used to harden targets, terrorists’ most effective approach was “operational changes that allowed penetration of target defenses”. In an example with direct relevance to airport security, when security forces used terrorist profiling, “every group sought and used terrorists with characteristics that were inconsistent with the profile and could therefore avoid detection.” Most groups also shifted to different targets or different tactics altogether.

The RAND researchers concluded that “the historical record of terrorists’ efforts to counter defensive technologies is not encouraging.” They found that “for most technologies, the groups will adapt to circumvent them”, and the security forces will have to respond. Thus, technology cannot be “the” solution to terrorism. They recommend that new defensive technology systems “must be designed with terrorist counter-technology behaviors and past successes in mind.” In particular, they suggest designing flexibility into defensive technologies, and frequently testing them against "red teams" trying to get past them.

3. AN EXAMPLE OF COST-EFFECTIVENESS ANALYSIS IN AVIATION SECURITY

The previous section discussed the difficulty of conducting overall benefit/cost analysis of anti-terrorist strategies. But there are other approaches to assessing the value of security measures. A recent paper from the University of Newcastle analyzes several components of the TSA's aviation security program in the United States [3]. In this paper, there is no attempt to make absolute B/C ratio calculations, as in the Copenhagen Consensus paper discussed previously. Instead, Stewart and Mueller assess the relative cost-effectiveness of several measures, using as a metric the cost per life saved. This approach has been used extensively in studies of the relative cost-effectiveness of safety-related regulatory measures. A table in their report draws on regulatory analyses of measures enforced by six US safety regulatory agencies (including the Federal Aviation Administration). The annual cost per life saved (in 1995 dollars) ranges from a low of USD 0.1 million for FAA's aircraft cabin fire protection standard to a high of USD 6.78 trillion for EPA's hazardous waste listing for wood-preserving chemicals. In reviewing possible safety regulations, the US Department of Transportation uses a figure of USD 3 million per life saved as a ceiling for acceptable regulatory costs.

Stewart and Mueller present a list of 20 TSA aviation security efforts, 14 of which apply in the airport environment (mostly concerning passenger and baggage screening, but also access control and other issues) and six that deal with in-flight security. They group the six in-flight measures into three: crew and passenger resistance, hardened cockpit doors, and Federal Air Marshals (FAMs). Consistent with much informal thinking within aviation security circles, they assume that in-flight efforts have made a considerable difference in reducing the probability that a plane will be hijacked and turned into a weapon. Hence, their starting assumption is that the in-flight measures account for 50% of the reduced risk of a 9/11 takeover, with the 14 pre-board security measures adding up to the other 50%. And as a starting assumption, they assume that the three in-flight measures are each equally effective - i.e. each accounts for 16.67% of the total reduced risk. They then factor in a generous 10% probability that Federal Air Marshals will be present on any plane. That reduces the risk reduction due to FAMs alone to 1.67%.

How likely would another 9/11 attack be were these 20 security measures not in place? Stewart and Mueller postulate that in the absence of those measures, there would be a 9/11 repeat (with approximately 3 000 deaths) once every 10 years. Hence, they assume this set of measures prevents 300 deaths per year in the United States.

From there on, it is a simple matter of doing the math, using the best available information on the annual costs of each measure. The results they present for the annual cost per life saved are as follows:

Hardened cockpit doors:	USD 800 000
Federal Air Marshals:	USD 180 000 000

They follow this with a sensitivity analysis that varies the probability of success of each measure, showing that the general results in terms of relative cost effectiveness hold true over a wide range. They conclude that “even an order of magnitude reduction in the effectiveness of hardened cockpit doors (resulting in a cost per life saved of USD 8 million) would not change the conclusion” that the cockpit doors are a far more cost-effective measure than air marshals.

That is as far as Stewart and Mueller take their analysis, but the same calculation can be applied to the set of pre-board security measures. Using their assumption that 50% of the reduced risk of a 9/11 attack is due to the pre-board measures, we use their basic equation:

$C_{ls} = C_r$ / (annual lives saved due to security measure)

where C_{ls} is the annual cost per life saved and C_r is the annual cost of regulation r.

According to Oster and Strong [4], about USD 4.7 billion of TSA’s annual USD 6.7 billion budget is spent on airport-related security (excluding cargo security). Using that figure for C_r yields an estimated cost of USD 31.3 million per life saved thanks to pre-board airport security measures – more than 10 times the US DOT standard, and 39 times as great as hardened cockpit doors.

While this approach obviously has its limitations, depending critically on assumptions about annual lives saved, thanks to reasonably good cost data and sensitivity analysis, it does make it possible to estimate the relative cost effectiveness of various aviation security measures.

4. US, CANADIAN AND EUROPEAN APPROACHES TO AVIATION SECURITY

4.1. Introduction

Aircraft hijackings in the late 1960s and early 1970s led the member states of the International Civil Aviation Organization (ICAO) to adopt Annex 17 to the Convention on International Civil Aviation, commonly known as the Chicago Convention. Annex 17 requires each member state to designate a single agency to develop national policy on aviation security – specifically, objectives, policies, and programs to prevent unlawful acts that threaten the safety of civil aviation. Annex 17 has been amended several times in subsequent decades, in response to the emergence of new threats and trends.

This section provides an overview of the development of aviation security policies since the adoption of Annex 17 in Europe, Canada, and the United States.

4.2. Europe

In Europe, hijacking was primarily a terrorist activity from the start, in contrast to the lone-hijacker-for ransom pattern in the United States in the 1960s and 1970s. Groups such as the Popular Front for the Liberation of Palestine and the Red Army Faction presented a larger and more organised threat than lone hijackers interested in money or momentary fame.

Prior to 9/11, aviation security was handled on a national basis in Europe. In Germany, as described by Hainmuller and Lemnitzer [5], the federal government urged its states (*Lander*) to implement airport security measures in 1970, and the larger airports did so. In 1980, after additional hijackings led to years of debate, a national civil aviation act was enacted, mandating that airports screen baggage and passengers, funded out of state budgets. Screeners were state employees, mostly drawn from the ranks of Federal Border Guards. In 1990, however, state budget pressures led to federal enactment of an aviation security fee, added to airline tickets, to recover part of the cost of staff and equipment for passenger and baggage screening. Continued cost pressures led to federal permission for screening to be outsourced to private security companies, with the first such contracts beginning in 1995. By 2000, "most of the German airports employ private screening firms or conduct screening themselves (e.g. Frankfurt)", according to Hainmuller and Lemnitzer's 2003 paper.

The pattern has been similar in other European countries, with airport security measures (mostly passenger and baggage screening) introduced in the 1970s and 1980s in response to hijackings. As in Germany, most such screening began with screeners as state employees. But the combination of airport privatization (beginning with the initial public offering of all shares in the British Airport Authority in 1987) and cost pressures led to the outsourcing of screening functions at most major airports by 2000. According to data compiled in 2001 by the (US) Aviation Security Association and reported in Poole [6], as of that year passenger and baggage screening was handled by either private security firms or a privatized airport company at 22 of the largest 25 European airports (ranked by international passengers). The exceptions were in Portugal, Spain, and Switzerland.

The destruction of Pam Am Flight 103 over Lockerbie, Scotland in December 1988, via a bomb in an unsuspecting passenger's checked bag, led to further changes in European aviation security. Positive matching of passengers and bags became mandatory in most European countries by 1989, and Germany had implemented 100% checked baggage screening at all 37 major airports by the end of 2002 [5]. The United Kingdom and a number of other countries did likewise.

Payment of aviation security costs in Europe follows no clear pattern. In some countries, such security is considered a national defense expense and is funded primarily by the national government out of general tax revenues. In the UK, by contrast, the privatized and commercialized airports are responsible for airport security costs, and recover those costs in their fees and charges to airlines. In Germany, as noted previously, a security tax on airline tickets covers a portion of security costs, with the balance shared between airports and the federal government.

No EU-wide aviation security policy existed until 2002, when the European Parliament and Council agreed upon Regulation No. 2320/2002 establishing common rules for civil aviation security. Those regulations were revised substantially in 2008, with Regulation No. 300/2008 repealing and replacing the 2002 regulation. Consistent with ICAO Annex 17, each Member State of the EU must have a national civil aviation security program, with a single agency in charge. Member States may adopt more stringent measures (on the basis of risk assessment), but the objective of No. 300/2008 is to provide a "common interpretation of Annex 17" within Europe [7].

4.3. Canada

As in Europe, aviation security precautions began as a response to hijackings in the 1970s. The government designated Transport Canada as its aviation security agency under ICAO Annex 17, and developed an airport security policy and program based on ICAO recommended specifications and practices for international airports [8]. Hijacking, taking on board offensive weapons and/or explosives, and endangering the safety of an aircraft in flight were made federal criminal offenses in

1972, and security-related measures were added to the Aeronautics Act in 1973. Those changes made airlines responsible for aircraft security and Transport Canada for overall security standards for airlines and major airports (of which Transport Canada was then the owner). That agency provided and operated checkpoint metal detectors and X-ray machines to screen passengers and carry-on bags.

In June 1985, an Air India flight from Toronto to New Delhi was destroyed in flight by a bomb, and on the same day two baggage handlers in Tokyo were killed by a bomb that originated on a flight from Vancouver and was destined for another Air India flight. Those events led to stepped-up passenger checkpoint screening, and physical inspection or X-ray of all checked luggage on international flights, as well as the installation of 26 explosive detection system (EDS) units for checked baggage screening and the use of passenger bag matching on international flights, and other policy changes to strengthen airport security. After 1992, when airports were divested by the national government to newly-created airport authorities, responsibility for passenger and baggage screening shifted to airports and their airline tenants.

In the wake of the 9/11 attack, new legislation was enacted in March 2002, the Canadian Air Transport Security Act. It created a new crown corporation, the Canadian Air Transport Security Authority (CATSA), which was given responsibility for several core functions, including provision of passenger and baggage screening at 89 airports, as well as developing a program for screening persons with access to secure areas of airports and assisting airports financially with the cost of increased policing at the 17 largest airports. CATSA has also been given responsibilities to develop and implement biometric identity cards for persons needing access to restricted areas at airports and to enter into financial agreements with the Royal Canadian Mounted Police to provide air marshals on selected flights.

Transport Canada's role was changed by the 2002 legislation. The creation of CATSA refocused Transport Canada on security policy and regulation, rather than the direct provision of security services, which became CATSA's responsibility.

In part because of the need to get into operation rapidly, and perhaps in part based on the success of outsourced screening functions in Europe in the 1990s, CATSA opted to contract with private service providers for those functions at all 89 airports. As of 2006, CATSA had more than 20 contracts with 12 different security companies to provide screening at these airports [8].

Along with creating CATSA, the government enacted an Air Travelers Security Charge (ATSC), to be paid by passengers "at a level sufficient to fund the enhanced air travel security system". The charge is added to airline tickets and remitted to the government, and the funds are appropriated annually for CATSA's use. Since its inception, revenues from ATSC have exceeded CATSA expenditures, resulting in several decreases in the rates charged for various categories of air service.

4.4. United States

As in Europe and Canada, the evolution of the US aviation security system was driven by the changing nature of the threat. The first US hijacking took place in 1961, the first of many such hijackings that ended up in Cuba. The Federal Aviation Administration, which included security among its safety regulatory duties, persuaded airlines to install a limited number of walk-through metal detectors and X-ray machines for carry-on items at selected airports from which hijacked flights had originated. With the airlines resistant to mandates that would increase their costs, the FAA did not pursue legislation. A further rash of hijackings for ransom in 1971 led to legislative proposals that did not pass, and a 1972 emergency rule by FAA requiring airlines to screen all passengers and carry-on bags. That policy was given the force of law by the Anti-Hijacking Act of 1974 and the Air Transportation Security Act of 1974. Airports were made responsible for the security of their premises, while airlines were responsible for screening (including the purchase and maintenance of the equipment). Since those costs became new airline operating expenses, the airlines had an incentive to keep them as low as possible, especially once price competition became important, following the Airline Deregulation Act of 1978. Airlines opted to outsource screening to private security companies, at the lowest possible cost.

The next changes, as in Europe and Canada, came about in response to the new threat of bombs in checked luggage, with the Pan Am 103 bombing as the trigger. The Presidential Commission on Aviation Security and Terrorism issued its report in May 1990, criticizing both Pan Am and the FAA for not making use of passenger bag matching. In response, Congress that year passed the Aviation Security Improvement Act, which ordered the FAA to launch an accelerated research & development program to produce an effective explosive detection system for checked baggage, and introduced background checks for new employees and contract personnel with access to secure areas.

In response to two (non-terror-related) airline crashes in 1996, a White House Commission on Aviation Safety and Security was created. Its final report recommended government funding for aviation security, licensing and performance standards for screening companies, background checks for all screeners and persons with access to secure areas, expanded testing of airport security, and comprehensive passenger-baggage matching [8]. It also recommended that a passenger pre-screening system developed and used by Northwest Airlines called CAPPS (Computer Assisted Passenger Prescreening System) be used by all airlines, which took place starting in 1998. However, the FAA's 1999 rules on CAPPS limited its use to determining which passengers should have their checked baggage screened for explosives. The FAA barred its use for selecting passengers for extra screening and searching, on grounds that this might be interpreted as discrimination [9].

The poor quality of passenger and baggage screening had been the subject of several reports by the government's General Accounting Office, starting in 1987. In that first report, GAO recommended that FAA set performance standards for passenger screening, but the FAA failed to act. In 1996, Congress included in legislation re-authorising the FAA the requirement that it "certify companies providing security screening and improve the training and testing of security screeners through the development of uniform performance standards for providing security screening services." FAA finally issued a proposed rule in January 2000, but when it had not been finalised by November of that year, Congress directed the FAA to issue the final version by May 31, 2001. The FAA failed to meet that deadline, and as a result, no such standards were in place by Sept. 11, 2001 [10].

Thus, when the 9/11 attack occurred, the United States had a mediocre, low-performing passenger and baggage screening system. Fewer than 150 EDS machines were in use (at larger airports), background checks had been expanding but were far from universal, and passenger-bag matching was in use only for flights to and from Europe and the Middle East. However, none of these factors were implicated in the 9/11 attackers' success with a new mode of attack on aviation. The only measure that might have stopped them – the use of CAPPS to select higher-risk passengers for what we now term "secondary screening" – had been forbidden by the FAA.

Nevertheless, the well-documented poor performance of airline-hired screening companies became the main focus of attention as Congress debated legislation to beef up US aviation security. The resulting Aviation and Transportation Security Act of 2001 (ATSA), enacted barely two months after 9/11, "federalized" airport screening by creating a new federal government agency, the Transportation Security Administration to carry out expanded passenger and baggage screening using a large new cadre of government employees. It set aggressive deadlines for TSA to staff up and take over screening from the security companies and appropriated funds to purchase several thousand EDS machines and many more electronic trace detection (ETD) machines, to permit 100% screening of all checked bags for explosives by a date certain (which subsequently had to be extended by one year). CAPPS was allowed to be used to designate selectees for secondary screening, and a more advanced successor version (CAPPS-2) was promised [11].

ATSA also created two sources of funding for aviation security. The Sept. 11th Security Fee, like Canada's ATSC, is imposed on airline tickets. The Aviation Security Infrastructure Fee is a tax on airlines, intended to raise approximately the amount they had been spending on outsourced screening services each year. Together, these two sources covered 42% of TSA's aviation security budget in 2005, 43.6% in 2006, and 51.8% in 2007 [4].

The TSA was originally housed within the US Department of Transportation, with its initial staff coming mostly from the FAA's former security operation. But in November 2002 Congress passed legislation creating the new Department of Homeland Security [11]. TSA was one of dozens of federal agencies shifted into the new department.

5. COMPARISON OF CURRENT AVIATION SECURITY POLICIES

5.1. Who pays for aviation security?

Our first point of comparison among Canada, Europe and the United States will be to examine which parties are responsible for paying for the aviation security regimes enacted following the 9/11 attacks. The Canadian system represents the most transparent case. As noted in the previous section, the Air Travelers Security Charge is applied to all airline tickets (with different rates for domestic, trans-border to/from the USA, and other international flights). Its proceeds fund 100% of the budget for CATSA, which handles airport security and the funding of air marshals; it also paid for strengthening the cockpit doors of Canadian airliners and pays the costs of additional Transport Canada security inspectors.

Thus, Canadian policy on transportation security appears to be mode-specific, i.e. the costs of protecting a mode of transportation are borne by the users of that mode. (Whether Canada is applying that policy consistently to other modes is beyond the scope of this paper.) Canadian airport and airline trade associations argue that "*aviation security is a 'national defence' issue and as such should be funded from general revenues* [12]". But after making this point, their recommendations (during a five-year review of CATSA in 2006) all focus on making the present funding mechanism more transparent and responsive to changing needs.

In Europe, the pattern varies by country. In the United Kingdom, the major airports (all of which are commercialised, with most now in the private sector) are responsible for all airport security, at their own expense. These costs get factored into the cost base on which they charge airlines for airside and landside services. Germany has a federal aviation security tax which is added to airline tickets, but that tax covers only a portion of the capital and operating costs of airport security, the balance of which are paid for out of airport budgets. Some German airports (e.g. Frankfurt, Hamburg, Dusseldorf) have been privatized, while others remain owned by some combination of state (*Land*)

and municipal governments. Thus, ultimate responsibility for aviation security costs in Europe seems to be a mix of passenger taxes and airport costs, with the latter being absorbed by airline charges. Article 5 of 2008 EC Regulation No. 300/2008 allows for each Member State to decide the mix of funding, from the state, airports, airlines, other agencies, and users (presumably passengers and shippers). Thus, Europe is not as mode-specific in its approach to security funding as is Canada.

The United States presents the most complex assortment of funding sources. As noted in the previous section, by 2007 the fraction of TSA's aviation budget that was provided by security taxes on airlines and passenger tickets slightly exceeded 50%. The balance of TSA's funding comes from the federal government's general fund. In addition, airports themselves are responsible for access control and airside security, costs which become part of their cost base and are passed along to airlines via airport rates and charges. Cost estimates for those portions of aviation security expense are not readily available. But because of significant federal general-fund support of TSA's aviation security budget, the United States departs significantly from the mode-specific funding approach of Canada. (Incidentally, US airlines make the same argument as their counterparts in Canada: that aviation security is basically a national defense function and should be covered entirely from the federal government's general fund.)

There is some merit to the argument that transnational terrorism is a threat to entire societies and therefore that measures taken against it could be considered one component of national defense and hence paid for out of general government revenues. However, if some components of a society present larger targets to terrorists, there is some justification for deciding that those who make use of that component should bear the costs. In this sense, security expenses can be seen as analogous to insurance. In general, in free societies, we allow people to engage in activities with various levels of risk (such as building homes in flood plains or on earthquake faults, or building and operating oil refineries). Those activities that are inherently higher-risk generally carry higher insurance costs, reflecting those risks. The existence of high insurance costs generally provides incentives for those incurring those costs to take protective measures to minimize risks. In hindsight after 9/11, US airlines learned that their low-performance contracts for passenger screening were inadequate to the task of coping with suicide-bomb threats. If the federal government had not taken over that function shortly thereafter, it is likely that airlines would have insisted on higher-quality screening thereafter.

If those involved with a particular type of transportation must bear the costs of securing that mode against terrorism, they presumably will be more concerned than otherwise about the cost-effectiveness of those protective measures. Given the tendency of elected officials to enact grandiose target-hardening plans without benefit of analysis, a countervailing force directly concerned with the costs of those plans seems wise.

5.2. Who provides aviation security?

As is the case with funding, the provision of aviation security varies considerably among countries. All OECD members have designated a single national agency to be responsible for aviation security – Transport Canada in the case of Canada, the Transportation Security Administration in the United States, and usually a transport ministry in European countries. Those agencies are responsible for making policy decisions about security (within the constraints of legislative direction), and for regulating the various entities involved in aviation – airports, airlines, pilots, etc. But which party actually delivers various security functions differs considerably.

Canada is unique in having created a crown corporation to carry out most aviation security functions: passenger and baggage screening, access control, biometric identity cards, etc. In Europe, these functions are usually the responsibility of each airport. The United States is unique on having a decidedly mixed system, thanks to the way Congress defined the TSA in its 2001 legislation. By law, TSA must carry out passenger and checked-baggage screening at nearly 450 commercial airports, despite TSA also being the national aviation policy-maker and regulator. Yet nearly all the remaining airport security functions – access control, perimeter protection, terminal-area policing, etc. – are the responsibility of the airport, under TSA's regulatory oversight. Thus, the TSA combines regulation and service provision within a single entity – a troubling conflict of interest, which violates the principle of arm's-length regulation. And TSA's responsibility for providing some but not all airport security functions means divided airport security, when unified security and single-point responsibility would be wiser.

One of the largest contrasts in the provision of security functions is the use of private security firms for passenger and baggage screening. Where this function has been devolved from the national policy-maker to either the airport level (Europe) or to a crown corporation (Canada), the inherent advantages of outsourcing have led to its universal adoption in Canada and to its widespread use in Europe. But in an over-reaction to the low-performing airline security contractors in place at US airports prior to 9/11, Congress mandated that a federal government workforce carry out all passenger and baggage screening. Only after a bitter battle in Congress was a small pilot program included in the legislation, under which five airports (one in each size category) would be permitted to use private security companies for screening, and after two years of TSA provision at all other airports, those airports would be permitted to ask TSA to leave and replace their people with a TSA-approved security company, selected by TSA and assigned to that airport. Despite better performance by security companies at the five pilot-program airports, no airport has asked TSA to leave (perhaps because TSA is also its security regulator).

An important advantage of outsourcing passenger and baggage screening is flexibility. An increasingly deregulated airline industry is dynamic, with new airlines being created, older ones merging or failing, and services being increased or decreased both seasonally and in response to airline initiatives and the ups and downs of the economy. Numbers of emplaned passengers at US airports fluctuate up and down from one month to the next from 10 to 20% for most airports, with some smaller airports experiencing much larger monthly changes [13]. Yet the TSA's allocation of screeners to airports is done on an *annual* basis, making it difficult to match staffing to workload. That is the kind of short-term flexibility that outsourcing facilitates. Another problem that has manifested itself in both Canada and the United States is uniform national compensation levels for airport screeners. In both countries, the cost of living (and hence pay scales) varies considerably from one region to another, with CATSA having particular difficulties attracting and retaining screeners in the booming oil province of Alberta.

But the larger, long-term advantage of outsourcing was noted in the RAND Corporation paper on how terrorists adapt to defensive technologies. Over time, terrorists may avoid the technology or alter their operational practices. Five years from now, a 43 000-person civil service work force of TSA airport screeners may no longer be appropriate, due either to changes in terrorist methods of operation or to improved technologies. In that eventuality, it would be far easier to down-size outsourced screening workforces – and redirect the resources to higher-priority uses – than to reduce the number of civil servants expecting something akin to lifetime tenure.

5.3. How risk-based are current security policies?

5.3.1 ICAO sets the context

ICAO’s Annex 17 sets forth the minimum aviation security standards expected of all member states [14]. As noted previously, it requires each state to have a civil aviation security organization and a written aviation security program, as well as requiring each airport and airline to have a written security program. Supplementing Annex 17 is the *Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference*, commonly referred to as ICAO DOC 8973. It provides detailed procedures and guidelines on how states may go about implementing the provisions in Annex 17, but is guidance, not a standard.

Standard 3.1.3 of Annex 17 states that each contracting state “shall keep under constant review the level of threat to civil aviation within its territory, and establish and implement policies and procedures to adjust relevant elements of its national civil aviation security program, *based on a security risk assessment* carried out by the relevant national authorities” (emphasis added). As interpreted by the review panel on CATSA in 2006, this establishes two basic principles for aviation security policy:

- “[I]t must be intelligence-led, based upon up-to-date threat assessments and resilient enough to adapt to new threats as they emerge.”
- “Risk analysis and assessment are the basis for effective use of security resources [8].*”*

While this might sound like a grant of considerable freedom, the document goes on to provide standards for pre-board screening of passengers and baggage, the quality of screeners and periodic testing of them, passenger-bag reconciliation, cargo security controls, access control via secure identification and random screening, and airport perimeter control. Other annexes provide for secured cockpit doors, procedures for dealing with disruptive passengers, and air marshals.

Thus, while the ICAO Annexes seek to ensure that at least minimum attention is given to all of these areas, there is potential tension between the implication that various inputs and methods must be used and the directive that decisions should derive from risk analysis based on up-to-date intelligence.

5.3.2 Canada’s aspirations for risk-based policy

The 2006 Advisory Panel review of the Canadian Air Transport Security Authority Act includes a section called “Risks and Layers: Envisioning Aviation Security.” It cites the ICAO rhetoric and notes that “[Security] resources, financial and human, are not unlimited and should be allocated according to assessed risk” [8]. It notes that Canada’s Auditor General the previous year had insisted that a risk-based approach is desired and expressed disappointment that Transport Canada “has not fully implemented formal risk management” [15]. The Advisory Panel report goes on to say that in its presentations to the Panel, “CATSA referred to its concept of security screening as risk-based”, and that: “Priorities must be established, and these should be based on assessments of the relative level of risk.”

But industry stakeholders, such as airports and airlines, told the Panel that CATSA should follow a more seriously risk-based approach. For example, in passenger screening, the agency should “focus on higher-risk passengers, rather than on the objects carried by all passengers.” They also called for better background vetting, so as to streamline the screening that takes place at the airport, “such as [via] a Registered Traveler Program.” The submission by the Canadian Airports Council (CAC) used stronger language, saying that the current “one-size-fits-all approach wastes precious resources [12].” CAC urged that CATSA move to “a standard that allows different levels of screening at sites and between sites based on risk assessment criteria", and recommended that a Registered Traveler program be implemented.

According to an interview with the chief executive of CAC, as of 2008 none of the changes the organization recommended have been implemented, but he believes that risk-based changes are coming, with ICAO encouragement [16].

5.3.3 Europe's steps toward risk assessment

The fourth section of Article 4 of EC No. 300/2008 permits member states to "adopt alternative security measures that provide an adequate level of protection on the basis of a local risk assessment." By being presented in the context of criteria that would allow states to "derogate from the common basic standards", this wording implies that less-stringent protection may be provided if justified by lower levels of risk or certain locations, aircraft sizes, or infrequency of operation.

According to European airport and airline groups, efforts to implement a truly risk-based system are at an early stage within the EU. In October 2006 the Airports Council International-Europe and the Association of European Airlines created a joint effort "to address shortcomings of the current system" [17]. In its news release announcing the launch of the European Strategic Partnership for Aviation Security (ESPAS), the Director General of ACI Europe said that "Any new security rule should focus specifically on the threat or risk that needs to be eliminated, taking account of the impact on passenger mobility and convenience, operations, and cost." Industry sources portray the replacement of EC No. 2320/2002 with No. 300/2008 as a step toward a more flexible and better-harmonized aviation security system within Europe. The online publication, *HomelandsecurityEU.com* commented, "From an industry standpoint, the inclusion of risk assessment is the key element of the new regime. By ensuring that the new security measures deriving from the framework are risk-based, each party will fully accept its responsibilities and its role in the security chain." [18]

However, as of early November 2008, the Policy Manager for ACI Europe stated that "We are still in the early process of a truly risk-assessment-based system in aviation security in the EU." [19]

5.3.4 The USA – mostly rhetoric on risk-based policy

The Transportation Security Administration is one of many agencies that are part of the Department of Homeland Security. In 2005, the relatively new DHS Secretary Michael Chertoff announced a sweeping reorganization of the agency, shifting to what appeared to be a more risk-based approach to security. The well-respected former Inspector General of DHS, Clark Kent Ervin, praised the new approach as "a threat-based, risk-based, consequence-based approach." And then-new TSA Administrator Kip Hawley said that "The federal government must focus resources on the basis of consequences, threat and vulnerability assessments, and the prioritization of risks." [13]

In the three years since 2005, very little evidence of risk-based policy change has emerged from the TSA. In an August 2007 report on DHS's progress in implementing its mission, the Government Accountability Office assessed the department's progress in aviation security as "moderate" and said: "Th[e] lack of a comprehensive strategy and integrated management systems and functions limits DHS's ability to carry out its homeland security responsibilities in an effective, risk-based way. DHS has also not yet fully adopted and applied a risk management approach", although the TSA had taken some steps in that direction [20]. In June 2008, GAO published a summary of a forum in which 25 experts discussed the issue of applying risk management to homeland security [21]. They considered the Coast Guard (but not TSA) to be one of the few federal government agencies that had effectively incorporated risk management principles into its decision-making; they also suggested that responsibility for risk management has been so distributed as to inhibit coordination on overall security priorities.

An example of TSA's unwillingness to embrace a risk-based approach is the evolution of the US Registered Traveler (RT) program. When the idea was first introduced to the aviation security community shortly after 9/11, it was presented as a risk-based program that would lead to better allocation of airport screening resources, by permitting those who had been "pre-screened" to receive a lower level of scrutiny at the checkpoint.

Unfortunately, once TSA permitted the RT program to be launched by private provider companies, the agency was unwilling to do more of a check than simply to verify that an applicant was not on the TSA watch list. Since TSA Administrator Kip Hawley believes that carefully-selected "sleeper" terrorists could pass that test, he concluded of RT that "It's not a security program but an ID [identification] program" [22]. Screening of RT members is therefore exactly the same as for non-members.

Despite this rather dismal record, US aviation stakeholders and TSA have been conferring about a methodology for risk-based assessment of aviation security policies. A group of stakeholders, including airlines, airports, law enforcement, and Boeing Company have been working with TSA and DHS starting in 2007 and continuing in 2008 to develop a Risk Management Assessment Plan (RMAP). Reportedly, the group has developed a risk assessment model, as a tool for better decision-making. One application would be for a TSA Federal Security Director for a particular airport to be able to use RMAP to put in place various changed policies that would not likely be anticipated by terrorists [31].

6. TOWARD A MORE RISK-BASED APPROACH

6.1. Introduction

As we have seen, aviation security officials in Canada, Europe, and the United States have all professed the importance of risk assessment as an important tool for allocating limited resources to protect civil aviation from terrorist attacks. But thus far, there is little evident use of such assessment to make judgments about which current policies are worth their costs. In section 3, we saw an example that suggested poor cost-effectiveness for air marshals, in terms of likely lives saved per million dollars spent. That example concerned in-flight security, where all the countries under consideration in this paper have adopted the cost-effective measures of strengthening cockpit doors and changing the protocols by which flight and cabin crew deal with attempts to commandeer an aircraft in flight. In this section we will consider what similar risk assessment might imply, for screening of passengers and baggage and for air cargo.

6.2. Risk-based passenger and baggage screening

Current screening practices are very similar in Canada, Europe, and the United States – and indeed, given the extensive travel among these jurisdictions, reasonably common and consistent policies make good sense. The major change entailed by the proposed risk-based policy would be to alter the present de-facto policy of treating all passengers and bags as needing equal scrutiny. Instead, the system would be based on applying somewhat different procedures to different passengers and their bags, based on an assessment of their relative riskiness.

6.2.1 Three-tiered approach for air travellers

The basic approach was outlined in this author's 2006 paper on risk-based airport security [13]. Its premise is that the task of airport screening should be to identify and isolate dangerous persons, not dangerous objects *per se*. The challenge is to keep those persons from causing harm, either in the terminal area or to the planes themselves. There are many ways in which terrorists can cause great harm in connection with airports: getting on board with the aim of hijacking, getting on board as a suicide bomber, putting explosives into checked luggage but not getting on board, or targeting large concentrations of passengers in terminals. Current policies devote the major share of airport security resources to just one of these threats: preventing would-be hijackers from boarding with weapons. Yet strengthened and locked cockpit doors (along with changed protocols for how crews deal with hijack threats), have greatly reduced the hijack threat. Far less money and effort is spent on securing airport terminal lobby areas and the ramp area where planes park. Thus, current policy in-effect downplays the threat of suicide bombers targeting crowds at checkpoints and lobby-based EDS installations, and the threat of bombs being smuggled onto planes from the ramp (as opposed to the terminal).

The proposed risk-based approach would shift the focus to identifying dangerous people. This could include greater security guard presence in terminal lobby areas and outside the terminal, in ramp areas and around the airport perimeter. And within the terminal, at the checkpoint it requires separating passengers into at least three defined groups, based on the quantity and quality of information about each:

- Low-risk passengers, about whom a great deal is known;
- High-risk passengers, based either on no knowledge or on specific, negative information;
- "Ordinary" passengers, mostly infrequent flyers and leisure travellers.

A different approach to both passenger screening and bag screening would be applied to each group.

Low-risk passengers are defined as those who possess a current government security clearance or who have been accepted into a Registered Traveler program by passing a background check and being issued a biometric identity card. Passengers in this group would go through express lanes at checkpoints, with something like pre-9/11 protocols (e.g. no shoe or jacket removal, not having to remove laptops or video cameras, etc.). Their checked bags would not have to be EDS-screened. The point is to not waste the system's resources or those passengers' time on procedures that add very little value to airport security. As a safeguard against the small probability that a dangerous person might slip into this category, a certain percentage of these people and their bags would be randomly selected for "ordinary passenger" screening, and this policy would be well-publicized.

High-risk passengers include those with no paper trail, about whom so little is known that the safest thing to do is to assume the worst and do a thorough screening of both person and bags (both checked and carry-on). Everyone in this group, in other words, would receive a more rigorous version of today's "secondary" screening, to include both explosive-detection screening of their carry-ons and either see-through scanning to detect non-metallic objects or a thorough pat-down search. The same protocol would apply to those whose names appear on government-maintained watch lists. Some of those in the latter category – those on a No-Fly list –would be detained rather than being put through a screening process.

Ordinary travellers are those in-between the other two risk categories. These people would receive something like today's level of passenger screening (but with a better-justified list of banned objects). A fraction of this group would be randomly selected for secondary screening, as described above.

6.2.2 Identifying low-risk passengers (registered traveller)

Michael Levine and Richard Golaszewski suggested the idea of separating out low-risk travelers and expediting their processing at airports in an article published two months after 9/11 [23]. Frequent flyers would be able to apply to TSA for membership by submitting to a background check, equivalent to a low-level security clearance. Those who passed this one-time screening would obtain a biometric identity card, and when they used the card at the airport to prove they were the person who had been cleared, they could bypass the more-stringent post-9/11 screening.

The concept was first subject to detailed analytical scrutiny by a team of graduate students in operations research at Carnegie Mellon University in 2003 [24]. They first created a model of passenger checkpoint processing, based on data from Pittsburgh International Airport (PIT). Next they created a design for a Registered Traveler program called SWIFT and simulated its operations using the model. Based on data from two surveys of airline passengers, they estimated that 40% of originating passengers would sign up for and be accepted into the system. Based on their simulation, first-class and elite frequent flyers (who already had a priority line at PIT) would see their average throughput time cut nearly in half, from 2.5 minutes down to 1.35. Coach passengers joining the program would have their average time slashed from 19.5 to 1.35 minutes. But those still using the regular lanes would benefit also. Since 40% fewer people would be using the regular lanes, their average processing time would drop from 19.5 to 12.1 minutes. The paper estimates that first-year benefits would exceed first-year costs by USD 2 million.

The RAND Corporation subsequently estimated that a protocol that would exempt Registered Travelers from the mandate for 100% screening of their checked baggage via explosive detection systems (EDS) would reduce the number of these costly machines required nationwide by approximately one-half [25].

As noted in the previous section, when TSA allowed RT to be introduced, the only background check it carried out was to check applicants against its watch list – the same procedure applied to every air traveler prior to issuance of their boarding pass. Understandably, this was inadequate for allowing RT members to get less screening at the checkpoint than other air travelers. TSA has implied that the cost of a "real" background check would be prohibitive. Yet several million aviation workers have been subjected to criminal history background checks since 9/11, as a condition of being allowed access to secure areas of the airport on a regular basis. This program is operated by the American Association of Airport Executives (AAAE), in cooperation with the Federal Bureau of Investigation, at a cost of USD27 per person [32]. At nearly all US airports, such airport workers do not have to pass through metal detectors nor have their tools X-rayed when entering secure areas. In fact, from the inception of the RT program, the certified RT companies sent the fingerprints of all applicants to the AAAE clearinghouse, but TSA never gave permission for these 200 000 sets of prints to be sent to the FBI for the expected criminal history background check [33]. Thus, a background check that TSA deems sufficient to allow unescorted and unscreened airport workers access to planes is deemed insufficient to allow RT members to pass through a streamlined version of checkpoint screening, as envisioned in the original RT concept.

As of this writing, the only Registered Traveler program in operation is the non-risk-based one in the United States. (A few countries' border control agencies have begun International Registered Traveler programs, but these merely permit expedited entry of frequent air travelers to the country in question; they are not part of an airport security program.)

6.2.3 Separating ordinary and high-risk passengers

Once low-risk passengers have been self-selected out of the mix, the remaining task is to use all feasible information to separate high-risk passengers from all the rest. One tool for doing this is a government-maintained watch list, continuously updated, against which all airline passenger reservations would be checked by the national aviation security agency in real time. In the United States, such a program is scheduled for implementation in 2009, under the name Secure Flight.

A second approach is to assess what is known about each passenger, based on information provided at the time of ticket purchase. In the United States until 2009 this has been carried out by the Computer Assisted Passenger Prescreening System (CAPPS), which dates from pre-9/11 days. The idea of such risk-screening systems is to use various algorithms to 1) verify the passenger's identity, and 2) look for patterns that might suggest high risk. CAPPS, and presumably Secure Flight, uses algorithms to flag some passengers for secondary screening.

To supplement the above tools, and to deal with lobby-area persons not holding tickets (and therefore not passing through the screening checkpoints), a technique called "behavioral profiling" is being used at Israeli airports [26], Boston's Logan Airport, and Las Vegas casinos. The general idea is to unobtrusively monitor people's behavior, looking for suspicious activities, to be followed up by questioning by security personnel.

6.2.4 Redesigning passenger checkpoints

Security checkpoints for a risk-based system would be different from those at today's airports. First, there would be two different sets of lanes, one set for Registered Travelers and the other set for all others. The proportion of each would have to be varied over time, depending on the fraction of daily originating passengers who were RT program members. Space would be required on the approach to the RT lanes for kiosks at which members would insert their biometric identity cards to gain admission to the line for these lanes. These kiosks might be combined with common-use boarding-pass kiosks, saving RT members without checked baggage from having to stop at two different kiosks.

On the sterile side of the checkpoint, additional space would be required for secondary screening portals to check the bodies and carry-on bags of selectees for explosives and potential weapons. All high-risk passengers (except those on the No Fly list, who would be detained) would automatically go through secondary screening. Boarding passes would be coded electronically, not visibly, so that a selectee would not know whether he/she had been selected by an algorithm or at random.

Meeting this set of requirements may require somewhat more square footage than is now allocated for checkpoints, though this will vary from airport to airport. On one hand, added space would be needed for RT kiosks and for expanded secondary screening equipment for selectees. On the other hand, significant RT enrollment should reduce the length of waiting lines (and hence reduce the area needed for that purpose). And a smaller total number of selectees (thanks to more precise identification of people leading to fewer false positives in checks against watch lists) would lead to a smaller secondary screening area than if current percentages of passengers continued to be selected.

6.2.5 Redesigning checked baggage screening

Neither Canada nor most European countries requires 100% of all checked baggage to be scanned by costly EDS machines. But where that mandate applies (as in the United States), the risk-based model would reduce the size and cost of checked baggage screening. The bags of RT members could be screened via two-dimensional X-ray machines, and would only move on to the more costly screening if a possible problem was detected by the initial X-ray. RAND Corporation has done a number of studies of the impact that an RT program (which RAND refers to as "positive profiling") could have on the size and cost of EDS installations at large and medium airports. In a 2004 report, one simulation modeling exercise used the following parameters: size the system to ensure that bags get to the intended flight 99% of the time, assume 90% reliability (up-time) of the EDS machines, and assume that 50% of all bags are exempted from EDS screening [25].

For this particular set of assumptions, the RAND team estimated the total cost to the flying public of various levels of EDS deployment, where cost includes both the capital and operating costs (screener payroll) of the EDS machines and the extra time currently wasted by passengers getting to the airport early enough to ensure that their flight is not delayed due to slow bag processing. In the absence of an RT program, the optimal number of EDS machines under these assumptions (nationwide) was found to be 6 000. But with an RT program that exempts 50% of all bags from screening (defined as screening all bags of non-members plus one-sixth of the bags of the 60% of passengers who are RT members), the optimal number of EDS machines declines to about 2 500. That's a very large difference in both the space required at airports and also in capital and operating costs. In round numbers, under a reasonable set of assumptions, an RT program could cut costly EDS deployment by up to 50%.

Some of the capital cost savings could be used for expanding passenger checkpoints and/or for improving terminal access control and airport perimeter control. The latter two uses aim at protecting planes on the ramp from unauthorized persons. And some of the payroll cost savings (from fewer EDS machines) could be used to add security personnel in lobby areas and to add staff for access control and perimeter control, as necessary.

The risk-based approach should produce significant savings in passenger time, by speeding up baggage screening and passenger screening alike. While the modeling necessary to quantify such savings is beyond the scope of this paper, the ultimate impact would be that people would not have to arrive at airports as early as they have learned to do in the post-9/11 era, reclaiming that time for personal or business purposes.

6.3. Air cargo security

This discussion is limited to "belly cargo", i.e. cargo that is carried in the baggage compartment of passenger planes. In sharp contrast to the non-risk-based approach to airport screening followed in Canada, Europe, and the United States, a generally risk-based approach to air cargo has been used since 9/11 in all of these jurisdictions. It parallels the way cargo is dealt with in the maritime system and in cross-border trucking and railroads. That general approach is to rely on a combination of intelligence information, "known shippers", and random screening.

The enormous volumes of cargo in all of these modes, and the very high costs in both time delays and equipment that would be required if all cargo had to be physically screened seems to underlie the acceptance of risk-based approaches as a practical reality. Yet when it comes to belly cargo on passenger planes, the inconsistency between the US policy of requiring 100% of all checked baggage to be screened by the most costly form of equipment (EDS) while belly cargo that sits next to those bags in the cargo hold is largely unscreened has led to repeated calls to close the belly cargo "loophole".

In Canada, as of the 2006 review, CATSA had no mandate to screen cargo, but in its Budget 2006 document, the Government allocated USD 26 million over two years to design and test an air cargo security initiative, while Transport Canada was developing an Air Cargo Security Strategy in consultation with aviation stakeholders. Canada's Border Security Agency in December 2005 required all air carriers and freight forwarders to electronically transmit air cargo data to it before loading the cargo at foreign airports. The CATSA Advisory Panel recommended that a similar program be implemented for air cargo originating in Canada.

In Europe, the new EC Regulation No. 300/2008 calls rather vaguely for member states to determine "conditions under which cargo and mail shall be screened or subjected to other security controls, as well as the process for the approval or designation of regulated agents, known consigners, and account consigners." The CATSA Advisory Panel singled out the U.K. approvingly for its existing air cargo screening system, "with its process for certification and verification of the security practices of known shippers, including periodic inspection of their facilities."

The struggle between risk-based and 100% physical screening approaches was highlighted in the United States when Congress included a measure based on the latter approach as part of the 9/11 Commission Act of 2007. The air cargo provisions called for TSA to physically screen all belly cargo, with 50% of this to be accomplished by February 2009 and 100% by August 2010. Airlines and airports objected that enforcing such a requirement at airports would be very difficult. There would be space problems, since belly cargo for wide-body planes often arrives on pallets, which are far too large to screen using the equipment in place for baggage screening; hence, large new facilities would be required to house costly new equipment. Moreover, the time required to physically screen all such cargo would disrupt schedules, undercutting the rationale for shipment of high-value, time-sensitive cargo by air [27].

In response, TSA has developed the Certified Cargo Screening Program (CCSP), which would distribute most of the screening function to various points in the supply chain. Shippers and freight forwarders may opt to become Certified Cargo Screening Facilities, which would screen and seal shipping crates, pallets and/or containers. The sealed boxes would be delivered by them to the airport by certified personnel, to be turned over to the airlines for loading. In effect, this represents an elaboration of the previous "known shipper" program. Under that program, shippers and freight forwarders who met certain TSA requirements (mostly about supply-chain integrity and control) were deemed to be safe originators of air cargo, whose packages required no more than occasional random screening at the airport, supplemented by periodic vetting of the shippers by TSA inspectors.

The new CCSP carries a high cost. An initial 2007 estimate from the Congressional Research Service was a cost to shippers and forwarders of USD 3.7 billion over its first 10 years [28]. In 2008, the Government Accountability Office provided information enabling a more current estimate to be made [29]. For an estimated 12 000 forwarders and shippers who may participate in CCSP, using screening equipment costing an average of USD 375 000 each, the total cost of just the equipment would be USD 4.5 billion. To that must be added the ongoing costs of staff doing the screening, paperwork, and transportation plus the cost of expanded TSA staff to inspect these 12 000 sites. For context, US belly cargo consists of about 250 million individual packages per year, providing USD 4.4 billion in airline revenue [27].

In October 2008, the United States and the European Union announced an agreement under which the EU agreed to comply with the US deadlines for belly cargo screening on flights from EU countries to the United States (i.e. 50% screened by February 2009 and 100% by August 2010). It provides that the EU "will use the same screening equipment, provide the same training to screeners, and impose the same security requirements on facilities where cargo is screened [30]."

Thus, recent developments appear to be moving air cargo (at least belly cargo) away from the former risk-based approach and toward the more prescriptive 100% approach applied to passenger and baggage screening. In other words, the discrepancy in policy regarding belly cargo and checked bags seems to being resolved by moving away from a truly risk-based approach. This may increase pressure from some quarters to apply similarly costly and non-risk-based approaches to all-cargo planes and later to other modes of shipping.

7. SUMMARY AND CONCLUSIONS

Defending target-rich free societies against terrorism is inherently difficult. On a macro level, it seems unlikely that terrorism can be eliminated in a permanent sense; the inherent asymmetries will likely make such societies attractive targets for one or another terrorist group indefinitely. We also know that terrorists learn from experience, and can change tactics and targets in response to defensive measures. Therefore, defensive measures must be dynamic and flexible, rather than static and predictable.

Most of today's aviation security policies and programs are responses to previous terrorist attacks, rather than more broadly based protections against a range of possible future threats. It seems likely that a number of such programs (e.g. air marshals and 100% EDS screening of checked baggage and belly cargo) would not pass a test of relative cost-effectiveness, such as the annual cost per life saved. Yet risk assessment, though much talked about as providing a sound basis for setting security priorities and allocating resources, seems to be very difficult to put into practice, despite its potential for getting significantly more value from whatever amount of resources is available in a country for aviation security.

In the United States, the largest resource allocation decisions have been made not by the designated security agency, the TSA, but by the US Congress, and enacted as legislation. These include the mandates for 100% EDS screening of checked baggage and 100% physical screening of belly cargo, the creation of TSA with the dual roles of aviation security regulator and airport screening provider, and a static "fortress wall" approach to airport screening. These decisions were not based on analysis by security experts, but rather by elected officials seeking to reassure the public that aviation is well-protected, regardless of cost or secondary effects.

The GAO's expert panel on strengthening the use of risk management principles was asked to identify the "key challenges" to doing so. The number one challenge (35% of panelists) was to "Educate the public about risks and engage in public discourse to reach consensus on an acceptable level of risk." Number two (19%) was to "Educate policymakers and establish a common lexicon for discussing risk", to counter-act political obstacles to risk-based resource allocation.

The goal of such efforts should be to wean legislators away from enacting mandates not based on risk analysis. Legislators should be encouraged to direct the national aviation security policymaker/regulator to address various problems, perhaps within some kinds of quantitative parameters (e.g. the US DOT's USD 3 million per life saved measure). Details of making actual policy and resource-allocation decisions should be left to the aviation security agency. That agency, in turn, should be flexible in tailoring policies to changing threats and different situations at individual airports, which vary enormously in type, size, configuration, etc.

No security policy should be pursued "at all costs", since resources are always limited. Likewise, all possible targets cannot be hardened to any appreciable degree, without bankrupting a country. While it seems likely that commercial aviation will remain a high-profile potential target, spending billions every year on static defenses at airports is almost certainly a poor use of resources. Whether any kind of effort can succeed in educating elected legislators and opinion leaders to these realities is the most difficult challenge.

REFERENCES

(1) Todd Sandler, Daniel G. Arce, and Walter Enders, *Terrorism: Copenhagen Consensus 2008 Challenge Paper*, Copenhagen, Copenhagen Consensus Center, 2008.

(2) Brian A. Jackson, *et al*., *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, RAND Corporation, 2007. (www.rand.org/pubs/monographs/2007/RAND-MG481.pdf)

(3) M.G. Stewart and J. Mueller, “Assessing the Risks, Costs, and Benefits of United States Aviation Security Measures”, Research Report No. 267.04.08, University of Newcastle (Australia), 2008. http://hdl.handle.net/1959.13/28097

(4) Clinton V. Oster and John H. Strong, “A Review of Transportation Security Administration Funding, 2001-2007”, *Journal of Transportation Security*, Volume 1, pp. 37-43, 2008.

(5) Jens Hainmuller and Jan Martin Lemnitzer, “Why Do Europeans Fly Safer? The Politics of Airport Security in Europe and the US”, *Terrorism and Political Violence*, Vol. 15, No. 4, Winter 2003, pp. 1-36.

(6) Robert W. Poole, Jr., “A Risk-Based Airport Security Policy”, Policy Study No. 308, Reason Foundation, May 2003. (www.reason.org/ps308.pdf)

(7) Regulation (EC) No. 300/2008 of the European Parliament and of the Council, of 11 March 2008 on Common rules in the Field of Civil Aviation Security [and repealing Regulation (EC) No 2320/2002].

(8) “Flight Plan: Managing the Risks in Aviation Security”, Review of the Canadian Air Transport Security Authority Act, Report of the Advisory Panel, 2006. (www.tc.gc.ca/tcss/CATSA/toc_e.htm)

(9) David Armstrong and Joseph Pereira, “Nation’s Airlines Adopt Aggressive Measures for Passenger Profiling”, *Wall Street Journal*, Oct. 23, 2001.

(10) Robert W. Poole, Jr., “Improving Airport Passenger Screening”, Policy Study No. 298, Appendix B, Reason Foundation, September 2002 (www.reason.org/ps298.pdf)

(11) Steven Brill, *After: How America Confronted the September 12 Era*, Simon & Schuster, 2003.

(12) “CATSA Act 5-Year Review: CAC Position Paper”, Canadian Airports Council, May 2, 2006.

(13) Robert W. Poole, Jr., “Airport Security: Time for a New Model”, Policy Study No. 340, Reason Foundation, January 2006. (www.reason.org/ps340.pdf)

(14) "Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference", Annex 17, Convention on International Civil Aviation, Eighth Edition, April 2006.

(15) "National Security in Canada: The 2001 Anti-Terrorism Initiative: Air Transportation Security, Maritime Security, and Emergency Preparedness", Auditor General of Canada, April 2005.

(16) Robert Poole telephone interview with Jim Facette, Canadian Airports Council, October 8, 2008.

(17) "Airports and Airlines Launch Joint Action to Tackle Aviation Security", Airports Council International Europe and Association of European Airlines, news release, October 10, 2006.

(18) Issue 6, Homeland Security, August 2007, www.homelandsecurityeu.com/currentissue/article.asp?art=271260&issue+219

(19) Email to Robert Poole from Vlad Olteanu of ACI Europe, October 28, 2008.

(20) "Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions", GAO-07-454, Government Accountability Office, August 2007.

(21) "Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security", GAO-08-904T, Government Accountability Office, June 25, 2008.

(22) "One-on-One: TSA Administrator Kip Hawley Preps His Final Initiatives", *Business Travel News*, October 20, 2008.

(23) Michael E. Levine and Richard Golaszewski, "E-ZPass for Aviation", *Airport Magazine*, November/December 2001.

(24) Catharine Foster, *et al.,* "Enhancing Aviation Security with the SWIFT System", H. John Heinz III School of Public Policy and Management, Carnegie Mellon University, May 18, 2003.

(25) Russell Shaver and Michael Kennedy, "The Benefits of Positive Passenger Profiling on Baggage Screening Requirements", DB-411-RC, Rand Corporation, September 2004. (www.rand.org/pubs/documented_briefings/2004/RAND_DB411.pdf)

(26) Ann Davis, Joseph Pereira, and William M. Bulkeley, "Security Concerns Bring Focus on Translating Body Language", *Wall Street Journal*, August 15, 2002.

(27) Robert W. Poole, Jr., "Can the Air Cargo Security Mandate Be Met?" *Airport Policy News*, No. 37, July/August 2008.

(28) Bart Elias, "CRS Report to Congress: Air Cargo Security", Congressional Research Service, updated July 30, 2007.

(29) Cathleen A. Berrick, "Aviation Security: Transportation Security Administration May Face Resource and Other Challenges in Developing a System to Screen All Cargo Transported on Passenger Aircraft", GAO-08-959T, July 15, 2008.

(30) Eileen Sullivan, “Officials: EU, US Agree on Air Cargo Screening, Associated Press, October 31, 2008.

(31) Robert Poole telephone interview with former ACI-NA official Charles Chambers, November 6, 2008.

(32) “AAAE and the Transportation Security Clearinghouse”, www.aaae.org/government/150_Transportation_Security_Policy/FactSheet_AAAE, accessed November 10, 2008.

(33) Robert Poole telephone interview with Carter Morris of the American Association of Airport Executives, November 10, 2008.

SECURITY AND RISK-BASED MODELS IN SHIPPING AND PORTS: REVIEW AND CRITICAL ANALYSIS

Khalid BICHOU

Centre for Transport Studies
University of London - Imperial College
London
United Kingdom

SUMMARY

London, December 2008

ABSTRACT

The primary aim of maritime security assessment models is to assess the level of security within and across the maritime network. When managing risk through legislation, regulatory assessment models are used to assess risk levels and examine the impact of policy options, usually in terms of the costs and benefits of a regulatory proposal. This paper reviews the development, application and adequacy of existing risk assessment and management models to maritime and port security. In particular, we examine the problematical issues of security perception, value and impact, and discuss the limitations of the current regulatory framework in providing an integrated and effective approach to risk assessment and management, including for supply chain security.

1. OVERVIEW OF THE NEW SECURITY REGIME IN SHIPPING AND PORTS

Since the terrorist attacks in the US in September 2001 and with the growing concern about the security of the international movement of goods and passengers, several frameworks have been introduced, either on a compulsory or voluntary basis, with a view to enhancing maritime and port security. Regulatory measures that have been multilaterally endorsed and implemented include the International Ship and Port Facility Security (ISPS) code, the IMO/ILO code of practice on security in ports, and the World Customs Organization's (WCO) "Framework of Standards to Secure and Facilitate Global Trade", also referred to as "SAFE Framework".

A second set of security initiatives has been introduced at various national levels, with the US-led initiatives being the most significant. The US measures started with common initiatives such as the Maritime Transportation Act (MTSA) of 2002, which involves both mandatory and voluntary ISPS provisions (DHS, 2003), and later introduced a range of layered security programmes which target specific types of maritime operations. Major programmes under this category include the Container Security Initiative (CSI), the 24-hour Advanced Manifest Rule (hereafter referred to as the 24-hour rule), the Customs and Trade Partnership against Terrorism (C-TPAT), the Operation Safe Commerce (OSC), the mega-port initiative, and the Secure Freight Initiative (SFA). Excepting the 24-hour rule, these programmes and others were subsequently codified into the US Safe Port Act. Other national programmes include Canada's and Mexico's own 24-hour rules and the Swedish Stair-sec programme.

Initiatives have also emerged from the European Commission (EC), in the guise of EC Regulation 725/2004 on enhancing ship and port facility security; Regulation 884/2005 laying down procedures for conducting Commission inspections in maritime security; and the Directive 2005/65/EC, extending security measures from the ship-port interface to the entire port facility. The Authorised Economic Operator (AEO), the status and accreditation of which were introduced in the EU Custom Security Programme implemented on 1 January 2008, is a scheme that deserves particular attention since it can be seen as the EU response to the US C-TAPAT programme. Outside the EU, regional initiatives worth mentioning include the US-Canada-Mexico Free and Secure Trade (FAST) initiative; ASEAN/Japan Maritime Transport Security; and Secure Trade in the APEC Region (STAR) for Asia Pacific. The Secured Export Partnership (SIP) is a bilateral customs security arrangement, designed to protect cargo exported from New Zealand to the USA against tampering, sabotage, smuggling of terrorists or terrorist-related goods, and other transnational crime, from the point of packing to delivery.

A final set of security initiatives consists of primarily industry-led and voluntary programmes. Initiatives under this category include the Secured Export Partnership (SEP) programme; the ISO/PAS 28000: 2005 standard (specification for security management systems for the supply chain); the Business Anti-Smuggling Coalition (BASC) scheme; the Technology Asset Protection Association (TAPA) initiative; and a series of Partnership in Protection (PIP) arrangements. Although some of these programmes have not been fully implemented yet, it is believed that they will yield a more effective framework and a higher level of security assurance across and beyond the maritime network. For a detailed review and analysis of these initiatives and other port and maritime security measures, the reader is referred to Bichou *et al.* (2007a).

With such complexities in the current maritime security framework, much of the literature on the subject has focused on prescriptive details of the measures being put in place, as well as on their *ex-ante* costs of compliance. However, there has been little work on security-risk assessment and management models, be it at the physical or the supply-chain level. In this paper, we review the development, application and adequacy of existing risk assessment and management models to maritime and port security. In particular, we examine current approaches to security-risk assessment and establish the link between physical and supply-chain security. However, not all aspects relevant to security-risk analysis in shipping and ports are discussed in this paper, which limits the analysis to maritime reporting and precursor analysis, economic evaluation of regulatory measures and alternative approaches to risk assessment and performance.

2. CONVENTIONAL RISK ASSESSMENT IN SHIPPING AND PORTS

2.1. System's safety approach to risks and hazard analysis

The conventional approach to risk defines it as being the chance, in quantifiable terms, of an accident or adverse occurrence. It therefore combines a probabilistic measure of the occurrence of an event with a measure of the consequence, or impact, of that event. The process of risk assessment and management is generally based on three sets of sequenced and inter-related activities, as outlined below:

- The assessment of risk in terms of what can go wrong, the probability of it going wrong, and the possible consequences;
- The management of risk in terms of what can be done, the options and trade-offs available between the costs, benefits and risks; and
- The impact of risk management decisions and policies on future options and undertakings.

Performing each set of activity requires multi-perspective analysis and modelling of all conceivable sources and impacts of risks as well as viable options for decision making and management. The empiricist approach is to regard accidents as *random events* whose frequency is influenced by certain factors. Under this approach, the immediate cause of an accident is known in the system safety literature as a "hazardous event". A hazardous event has both causes and consequences. The sum of the consequences constitutes the size of the accident. Hazardous events range in frequency and severity from high-frequency, low-consequence events (e.g. road accident or machine failure), which tend to be routine and well reported, to low-frequency, high-consequence events (e.g. earthquake or terrorist attack), which tend to be rare but more complex.

Several analytical tools have been developed for hazard analysis (see Table 1). The choice of tool depends on (i) whether the causes or the consequences of a hazardous event are to be analysed, and (ii) whether the techniques used take into consideration or not the sequence of the causes or consequences.

Table 1. **Major hazard analysis tools**

	Consequence analysis	**Cause analysis**
Sequence dependent	Event Tree Analysis	Markov Process
Sequence independent	Failure Mode and Effects	Fault Tree Analysis

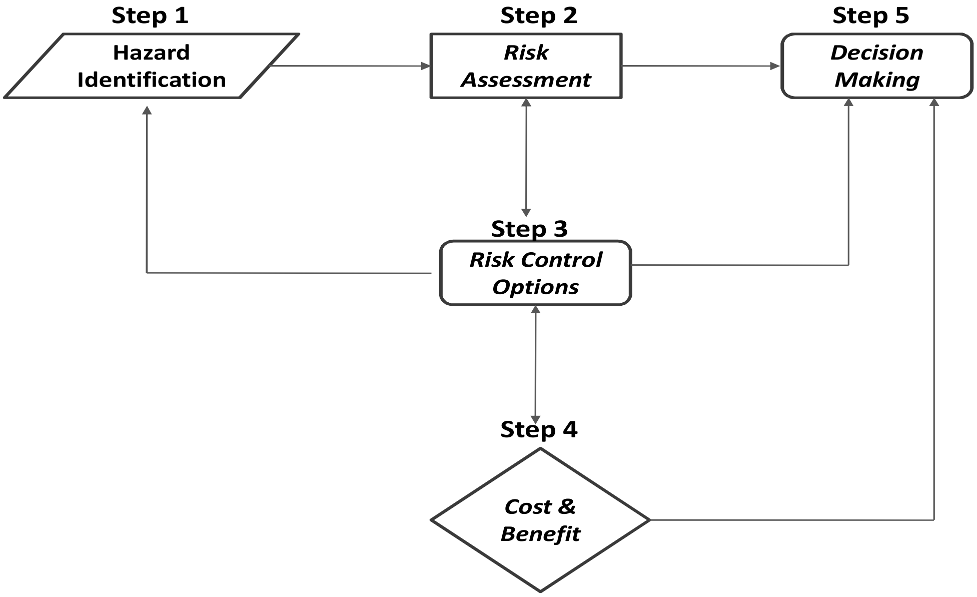
The causes of a hazardous event are usually represented by a fault tree, which is a logical process that examines all potential incidents leading up to a critical incident. A popular methodology that relates the occurrence and sequence of different types of incident is the fault tree analysis (FTA). Under the FTA, a mathematical model is fitted to past accident data in order to identify the most influential factors (top events) and estimate their effects on the accident rate. The model is then used to predict the likelihood of future accidents. The extent to which the tree is developed (from top to basic events) is usually governed by the availability of data with which to calculate the frequencies of the causes at the extremities of the tree, so that these may be assigned likelihoods. From these, the likelihood of the top event is deduced.

FTA has a number of limitations. For instance, the approach assumes that the causes are random and statistically independent but certain common causes can lead to correlations in event probabilities which violate the independence assumptions and could exaggerate the likelihood of an event fault. In a similar vein, missed or unrecorded causes may equally bias the calculated likelihood of a hazardous event. Another shortcoming of the fault tree analysis is the assumption that the sequence of causes is not relevant. Where the sequence does matter, Markov-chain techniques may be applied.

The consequences of a hazardous event may be analysed using an event tree. Event tree analysis (ETA) is a logical process that works the opposite way to FTA by focusing on events that could occur after a critical incident. Under ETA, a statistical analysis of past accidents is performed to estimate the consequences of each type of accident in order to predict risk and consequences of future accidents. The event tree approach implies that the events following the initial accident, if they occur, follow a particular sequence. Where a particular sequence is not implied, "Failure Modes and Effects" analysis may be used. This technique seeks to identify the different failure modes that could occur in a system and the effects that these failures would have on the system as a whole.

Most of the general tools described above have been successfully applied across many areas of maritime and port safety, with the Formal Safety Assessment (FSA) being the most standardized framework of risk analysis in regulated maritime systems. The FSA was first developed by the UK maritime and Coast Guard Agency (MCA) and later incorporated into the International Maritime Organisation (IMO) interim guidelines for safety assessment (IMO, 1997). The FSA methodology (see Figure 1) consists of a five-step process: hazards identification, risk assessment, risk management (alternative options), cost-benefit analysis and decision making (MCA, 1996).

Figure 1. **FSA Methodology**



Source: Adapted by the author from MCA, 1996.

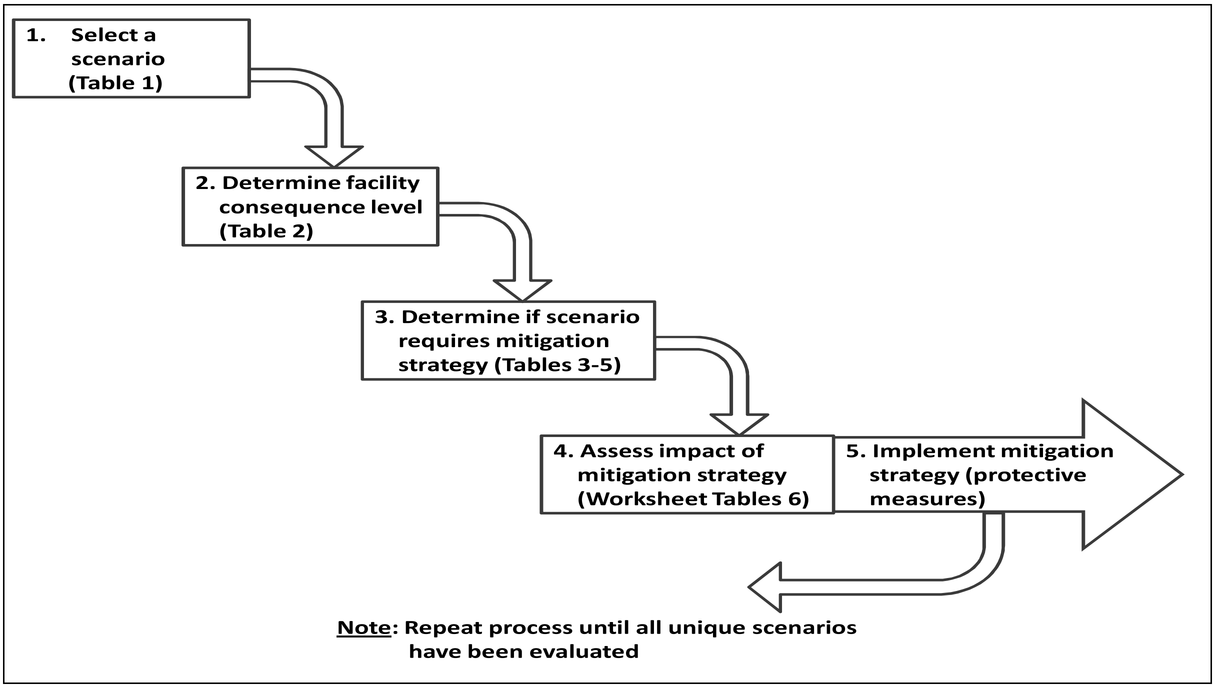
Despite the variety of analytical tools available, the FSA and other conventional risk assessment models involve a substantial element of subjective judgement for both the causes and the consequences. The assumption of randomness of the causes of hazardous events is particularly problematic for low-frequency, high-consequence events. The calculation of the consequences of an accident can also be subjective. Furthermore, any analytical tool for risk analysis requires that the boundaries, components and functioning of the system is well established; but this is not always evident in the context of shipping and port operations, given the combination of several elements related to vehicle, facility, cargo, equipment, communication and labour factors, as well as several environmental and exogenous factors.

2.2. The current risk approach to maritime security

A typical example of maritime security risk models based on system safety is the widely accepted Navigation Vessel Inspection Circular (NVIC) No. 11-02, "*Recommended Security Guidelines for*

Facilities", published by the US Coast Guard. Under this circular, the risk-based framework for security assessment and management is structured in terms of five steps (Figure 2).

Figure 2: **The NVIC risk assessment model**


1. Select a scenario (Table 1)
2. Determine facility consequence level (Table 2)
3. Determine if scenario requires mitigation strategy (Tables 3-5)
4. Assess impact of mitigation strategy (Worksheet Tables 6)
5. Implement mitigation strategy (protective measures)
Note: Repeat process until all unique scenarios have been evaluated

Step 1 of the risk-based assessment begins by selecting an attack scenario that consists of a potential threat to the vehicle (e.g. ship, truck), cargo/passengers, facility (e.g. port, equipment) and/or operation (e.g. cargo handling). In the context of the maritime security regulatory regime, such scenarios must be consistent with scenarios developed for formal assessment models, such as the ISPS provisions for ship security plan (SSP) or port-facility security plan (PFSP). Step 2 of the risk-based security assessment is to determine the appropriate consequence level for the type of activity on which the risk assessment is based. Step 3 refers to vulnerability assessment, with four factors considered for vulnerability scoring: availability, accessibility, organic security and facility hardness. In the context of the ISPS Code, the NVIC grading scenario-risk method (Table 2) may be assimilated to the ISPS provisions of maritime security (MARSEC) levels, ranging from (1) for minor to (3) for severe. An indication of vulnerability scores in the case of transportation and warehousing of bulk cargo is provided in Table 3. Step 4 deals with the mitigation of the risk. As shown in Table 4, this can be achieved by determining where the scenario falls, based on the consequence level and vulnerability assessment score.

Table 2. **NVIC national list of scenarios**

Typical types of scenario		Application example
Intrude and/or take control of the target and....	damage/destroy the target with explosives	Intruder plants explosives.
	damage/destroy the target through malicious operations/acts	Intruder takes control of a facility internationally open valves to release oil or hazardous materials that may then be ignited.
	create a hazardous or pollution incident without destroying the target	Intruder opens valves/vents to release oil or toxic materials or release toxic material brought along.
	take hostages/kill people	Goal of the intruder is to kill people.
Externally attack the facility by...	launching or shooting weapons from a distance	Shooting at a target using a rifle, missile, etc. To damage or destroy bulk storage tanks, dangerous cargo, etc.
Use the facility as means of transferring...	materials, contraband and/or cash into/out of the country	Facility is used as conduit for *transportation security incident*
	people into/out of the country	

Table 3. **Vulnerability scenarios and scores**

Score	Accessibility	Organic security
3	No deterrence (e.g. unrestricted access to facility and unrestricted internal movement)	No deterrence capability (e.g. no plan, no guard force, no emergency communication, outside law enforcement not available for timely prevention, no detection capability)
2	Fair deterrence (e.g. single substantial barrier, unrestricted access to within 100 yards of bulk storage tanks)	Fair deterrence capability (e.g. minimal security plan, some communications, security force of limited size relative to the facility, outside law enforcement with limited availability for timely prevention, limited detection systems)
1	Good deterrence (expected to deter attack, access restricted to within 500 yards of bulk storage tanks, multiple physical/geographical barriers)	Good deterrence capability expected to deter attack (e.g. detailed security plan, effective emergency communications, well-trained and equipped security personnel, multiple detection systems (camera, x-ray, etc.), timely outside law enforcement for prevention)

Table 4: **Vulnerability and consequence matrix**

	Total vulnerability score (Table 3)		
Consequence level (Table 2)	**2**	**3-4**	**5-6**
	Consider	Mitigate	Mitigate
	Document	Consider	Mitigate
	Document	Document	Consider

3. SHORTCOMINGS OF CONVENTIONAL MODELS FOR ANALYSING MARITIME AND PORT SECURITY RISK

The NVIC model and other conventional risk models follow a safety-risk approach; but the latter is based on the assumption of unintentional human and system behaviour to cause harm. This is not the case for security incidents stemming from terrorism or other malicious acts. Another major problem with assessing security threats is that much of the assessment process is intelligence-based, which does not always follow the scrutiny of statistical reasoning. Even with a sound intelligence risk approach, there are many uncertainties involved, such as in terms of higher levels of noise in background data. An additional instance of inadequacy of conventional risk models to maritime security is the lack of historical data, given the rarity of occurrence of large-scale terrorist incidents. Another important issue stems from the supply-chain dimension of the international shipping and port network, and the fact that data on the scope and levels of externalities are extremely difficult to extract and analyse. In either case, the security of the maritime network must be considered in both its physical and supply-chain dimensions, the latter evolving around disruptions and risk-driven uncertainties in the supply chain. In the following, we discuss two main drawbacks of the current regulatory framework in relation to the assessment and management of the security risk for ships and shipping operations, namely: the inconsistencies in the current maritime reporting system and the failure to consider the supply-chain dimension of security.

3.1 Reporting systems and maritime security

3.1.1 Security incidents and precursor analysis

A broad definition of precursors may involve any internal or external condition, event, sequence, or any combination of these that precedes and ultimately leads to adverse events. More focused definitions reduce the range of precursors to specific conditions or limit their scope to a specified level of accident outcome. For instance, the US Nuclear Regulatory Commission (NRC) defines a precursor as *"any event that exceeds a specified level of severity"* (NRC, 1978), while other organisations incorporate a wider range of severities. In either case, a quantitative threshold may be established for the conditional probability of an incident given a certain precursor, with events of lesser severity being considered either as non-precursors with no further analysis or as non-precursors that need categorisation and further investigation.

Following the events of 11 September 2001, several formalised programmes have been developed for observing, analysing and managing accident precursors, including comparison charts and reporting systems. In recent years, several organisations have designed and implemented reporting systems for security incidents/accidents, with the most recognisable reporting system being the colour alert system used by the US Department of Homeland Security (DHS). Relevant examples in maritime security include the International Maritime Organisation's (IMO) reporting system for ISPS compliance, International Maritime Bureau (IMB) reports of piracy accidents, and a number of voluntary reporting initiatives for maritime safety (BTS, 2002).

A major drawback resulting from the combination of warning thresholds and security event reporting is that the system may depict several flaws and errors. If vulnerabilities are defined too precisely or the threshold is set too high, several risk-significant events may not be reported. On the other hand, setting the threshold for reporting too low may overwhelm the system by depicting many false alarms, and ultimately a loss of trust in the system. Table 5 shows the types of error that may occur given these conflicting approaches. "Type I error" refers to a false negative and occurs in situations of missed signals when an accident occurs with no warning being issued. "Type II error" refers to a false positive whereby a false alert is issued, leading, for instance, to mass evacuation or a general disturbance of the system.

Table 5. **Errors resulting from the interplay between threshold settings and event reporting**

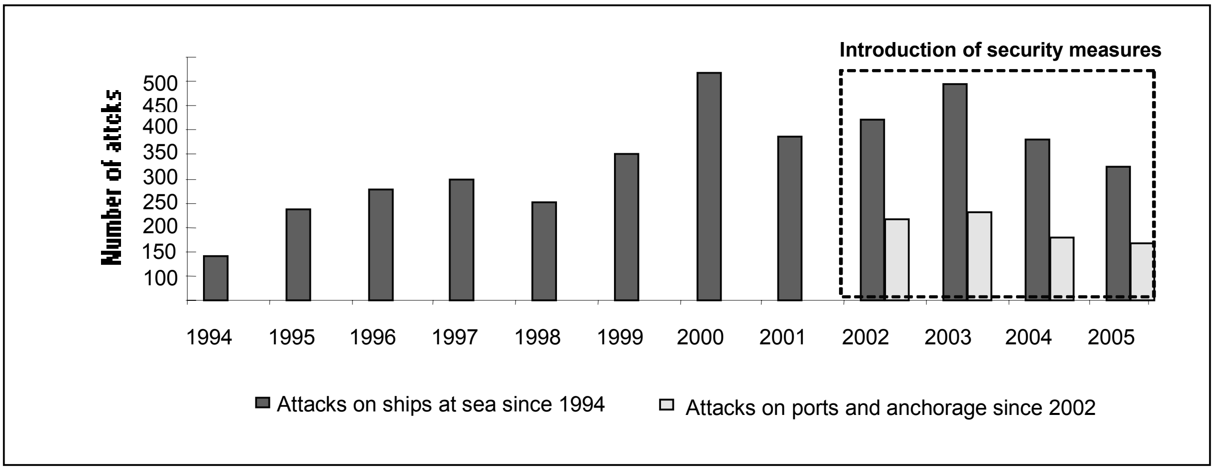
	Significant	**Not significant**
Event reported	True positive (Significant event)	False positive (Type II error)
Event not reported	False negative (Type I error)	True negative (Non-significant event)

Another issue arising from reporting security precursors under regulatory constraints relates to the fact that reported data remains in the hands of the regulator. This raises questions about (i) the reliability and validity of information, since fears of regulatory actions may discourage organisations from reporting precursor events, and (ii) the dissemination of reported information, given that the regulator may restrict access to data which is considered too sensitive to be shared. The argument here is that the purpose of reporting must emphasize organisational learning, along with a guarantee of privacy and immunity from penalties for those reporting the information.

A particular aspect of precursor analysis is the so-called "near miss", also referred to as the near hit, the close call, or simply the incident. A near miss is similar to an accident except that it does not necessarily result in injury or damage. It is a particular kind of precursor with elements that can be observed in isolation without the occurrence of an accident. The advantage of the concept is that organisations with little or no history of major incidents can establish systems for reporting and analysing near misses. This is because it has been found that near misses occur with greater frequency than the actual event (Bird and Germain, 1996). This argument is even made stronger with much of the literature on reported transport accidents confirming that near misses have usually preceded the actual incidents (Cullen, 2000; BEA, 2002).

In maritime security, implementing programmes of security assessment based on precursor analysis would have a number of benefits, for such aspects as identifying unknown failure modes and analysing the effectiveness of actions taken to reduce risk. Another opportunity derived from precursor analysis is the development of trends in reported data, which may be used for the purpose of risk management and mitigation; however, there is no formal categorisation between incident and accident reporting in shipping and ports. Furthermore, we are not aware of any formal precursor programme being implemented in the context of maritime security, except for on-going research into potential security hazards for liquid-bulk and specialised ships, such as LNG and LPG vessels. On the one hand, inherently secure designs against the threat of terrorism and other similar acts are yet to be developed, although improvements have been made in ship design for safer and sustainable transportation. On the other hand, existing reporting schemes of maritime security incidents show noticeable gaps in both content and methodology. This is the case, for instance, for piracy and armed robbery incidents, whereby available reports show general information with no sufficiently detailed data to display and analyse incident precursors (see Table 6); although the recent piracy incidents in the Gulf of Aden may trigger a radical change in piracy-incident reporting.

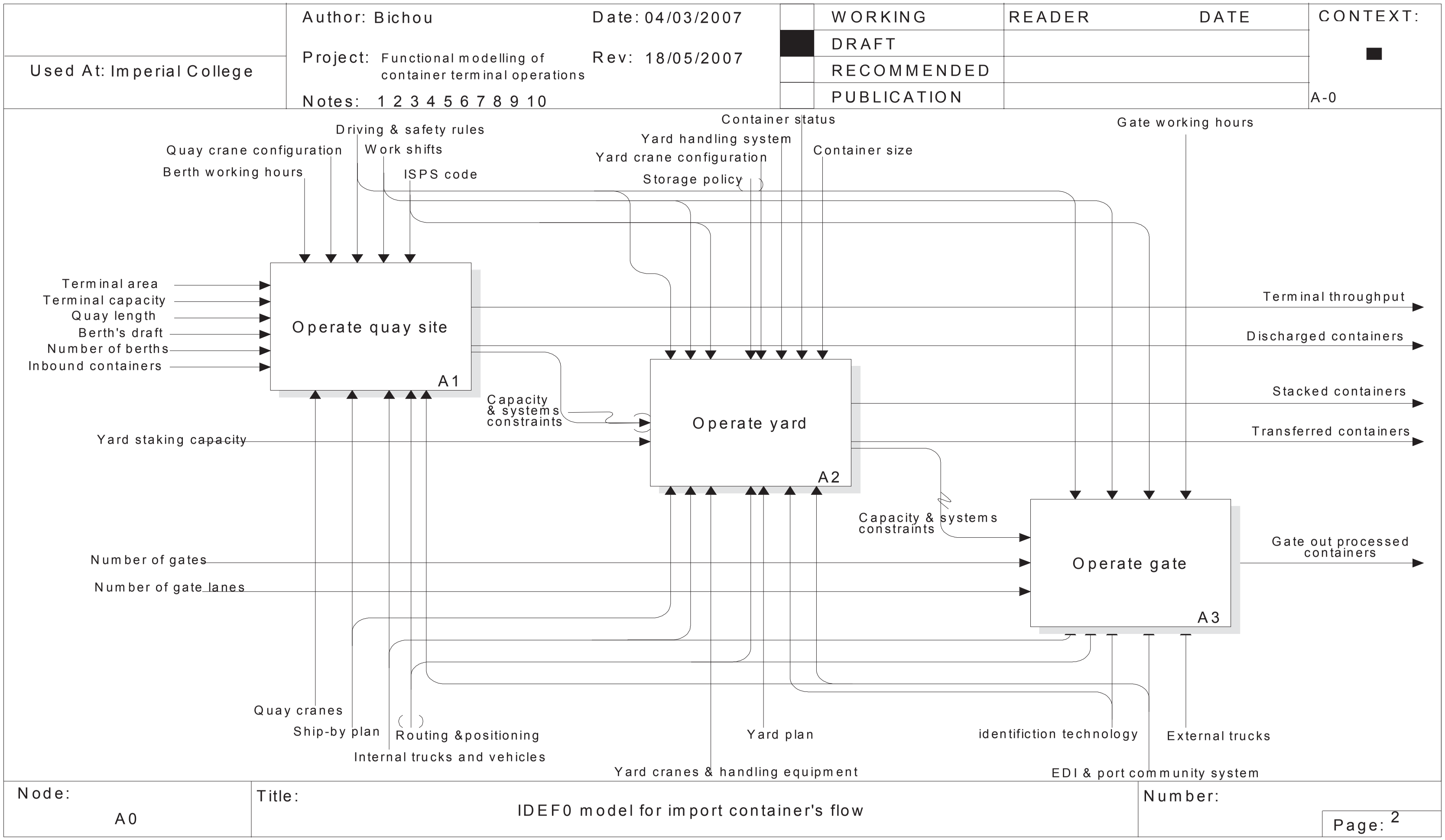
Table 6. **Reported actual and attempted piracy incidents on ships and ports, 1994-2005**



Source: Compiled by the author from IMB & IMO annual piracy reports.

Analysis of accident precursors can also be useful in conjunction with probabilistic risk analysis (PRA). PRA is a quantitative risk assessment method for estimating risk failure based on a system's process mapping and decomposition into components (Bier, 1993; Bedford and Cook, 2001). PRA has been used in a variety of applications including risk analysis in transportation systems. PRA can be combined with precursor analysis to quantify the probability of accidents given a certain precursor, thus helping in prioritising precursors for further analysis or corrective actions. The method can also be improved based on precursor data analysis, such as by checking on the validity of PRA model assumptions. An instance of modelling port operations for the purpose of PRA and accident precursor analysis is provided in Figure 3 below.

Figure 3: **A model of import container's flow for PRA and precursor analysis**



Source: Author.

3.1.2 Shipping security and reporting procedures

One of the major changes brought about by maritime and shipping security is that further documentation and screening for the cargo being transported by sea is now required. However, such requirements are not always consistent between regulations or countries. Anomalies in maritime reporting and documentation systems occur, for instance, when ships and their cargoes become exempt from regular customs inspections when sailing between ports of countries belonging to the same trading or economic block, such as the EU or NAFTA. In the EU, for example, Member States of the European Union enjoy the freedom of moving goods within the Community, which means that as long as consignments originate within the EU, there are no controls concerning their movement. The issue of the exemption of Authorised Regular Shipping Services from Customs Reporting Regimes gives rise to anomalies in the reporting of cargoes, as it is very likely that such vessels are not only carrying goods of EU origin but also consignments under Community Transit Customs control, or sometimes cargo originating from outside the EU. Unless that cargo is individually reported as being in separate containers or trailers, or the vessel itself is registered within the EU, the cargo may not be declared and its contents may be unclear. Vessels sailing in EU territorial waters may also be carrying consignments on a consolidated basis and for which there are only brief summary details referring to the consolidation, and not necessarily for each individual, grouped consignment.

To avoid such anomalies, countries such as the USA have introduced detailed documentation and reporting systems, e.g. through the 24-hour rule. However, because of the requirements of such levels of detail under the new security regulations, shipping lines and their agents may fail to produce the relevant documentation and related detailed cargo description in conformity with the 24-hour rule and other maritime security requirements. A sample of potential errors that might occur in the work processes while satisfying maritime security is provided in Table 7.

Even with detailed procedural regulations such as the 24-hour rule, full and accurate information regarding cargo movement and ownership throughout the supply chain may not be readily available to regulators or customs authorities. This is typically the case when using a combination of transport modes (multimodal transportation) and consolidation arrangements. For the latter, the description of Less-than-Container-Load (LCL) consignments in terms such as “Said to contain” or “Freight of All Kinds” (FAK) creates a vacuum in information transparency and accessibility as far as the carriage of goods on groupage consignment is concerned. A more radical example is that of a consignment described loosely as “cosmetic products”, which may range from aromatic oils through soaps to lipsticks and nail varnish. However, the consignment may also include items such as nail varnish remover, classed as a hazardous good because of its flammable nature. But since the overall groupage consignment description makes no mention of this, the specific commodity is overlooked, and no specific Dangerous Goods documentation issued for the nail varnish remover, despite the evident risk involved in the shipment of the consignment.

Table 7. **Potential errors from implementing the 24-hour rule**

Functional department	Potential errors
Marketing	Flagging the CSI cargo in business information system Booking data quality Booking confirmation to shipper CSI cut-off time
Administration (documentation and ICT)	Manifest data quality Transmission of timely manifest data to AMS Handling amendment Bill of Lading issuance to shipper Rating the shipment Billing the CSI fee and amendment fee
Operations	Ship/port planning Release of empty container Coordination with terminals and customers for cargo inspection

Source: Bichou *et al.*, 2007.

The nature of the international supply chain demands that information pertaining to cargoes is passed down the line from supplier to customer in order to ensure the smooth and efficient despatch and delivery of the consignment; and that all authorities and parties within the supply chain, especially from a transportation and national control perspective, are fully informed as to the nature and risk of the consignment in question. Even when no international frontier controls are involved, such as within the European Union, there is still a significant need for such flows of information, especially where combined forms of transport are involved. This issue will be examined further in the next section.

Another issue arising from the new requirement for detailed reporting stems from the on-going trend of increase in vessel size. For instance, the wide deployment of the new, Super Post-Panamax container vessels means that the cargo manifest for each vessel becomes larger, with the risk that the computer systems required to analyse the information therein require updating to cover the increased volume of information or may take some time to absorb all the information contained therein. Given the sheer volume of container information in each manifest, it is too cumbersome a task for the customs computer or the customs officer to analyse each cargo at the time the manifest is submitted, although containers are selected at random for scanning and examination at the port.

Last, but not least, the issue of container security poses a problem as there are yet no agreed international standards and regulations on the enforcement of container seals (mechanical and electronic) used in international transport movements. Container security consists of a complex system of interrelated activities in information and data capture, physical surveillance of the container, and inquiries into the various actors in the supply chain; but any standardization process must decide on the privacy of the parties involved and their willingness to share information between each other.

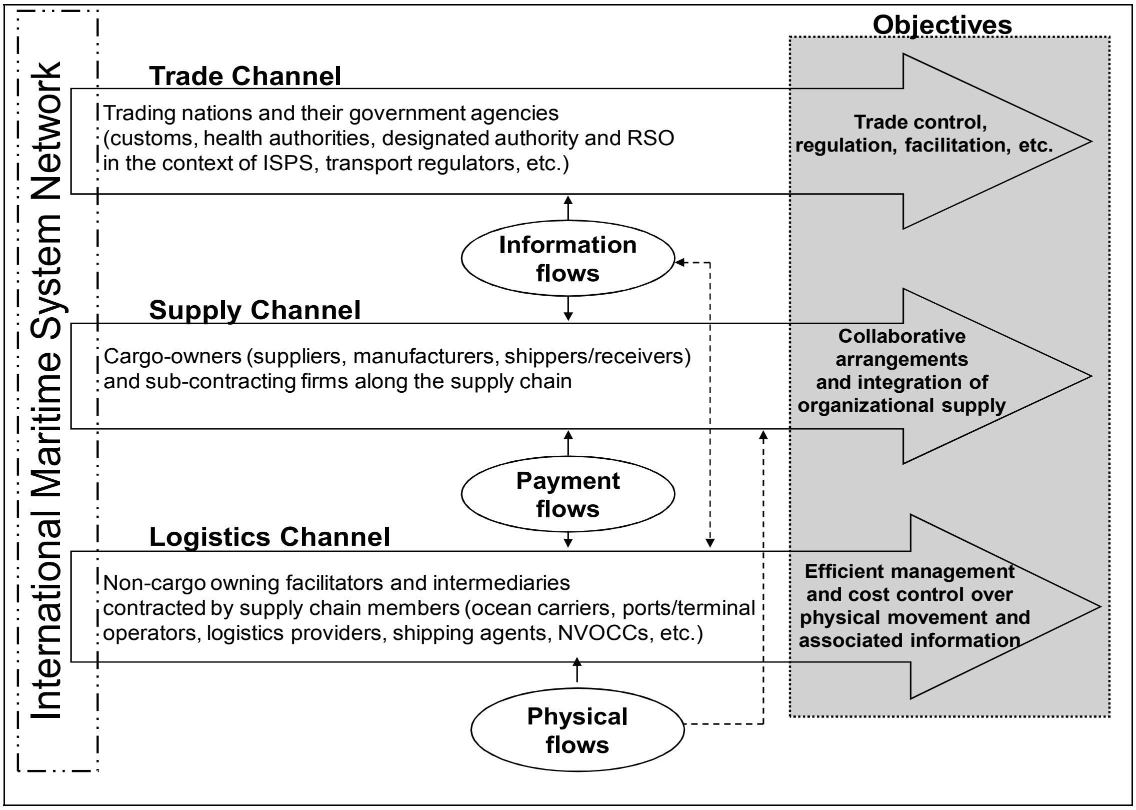
3.2. The supply chain risk dimension of maritime security

Since the introduction of the new security regime in shipping and ports, researchers and practitioners alike have questioned the wisdom of such a plethora of regulations. Others have justified the overlap of these programmes by the need to establish a multi-layer regulatory system in an effort to fill potential security gaps (Flynn, 2004; Willis and Ortiz, 2004). The concept of layered security is not entirely new to transport systems as it dates back to the 1970s. Prior to the introduction of new maritime security measures, the concept was also cited in 1997 in the context of aviation security (Gore Commission, 1997).

To illustrate the application of the layered approach to maritime and supply-chain security, we develop a conceptual construct of the structure and functioning of the international maritime network. The system is portrayed in terms of three chains or channels (logistics, trade and supply) and three flows (payment, information and physical). A chain or channel is a pathway tracing the movement of a cargo shipment across a "typology" of multi-institutional and cross-functional alignments; while flows are the derived interactions or transactions between various "functional institutions" within each channel. The logistics channel consists primarily of third-party specialists (ports, carriers, freight forwarders, 3PLs, 4PLs, etc.) which do not own the cargo but facilitate its efficient progress of movement, for example, through transportation, cargo handling, storage and warehousing. Both the trade and supply channels are associated with the ownership of goods moving through the system, with the difference that the trade channel is normally perceived to be at the level of trade or national ownership (e.g. the oil trade, containerised trade, US-Canada trade, intra-EU trade) and the supply channel at the level of the firm (e.g. Toyota and Wal-Mart supply chains, respectively). For each channel, one flow or a combination of physical, information and payment flows is taking place.

Figure 4 depicts the interactions between channels and flows in a typical international maritime network.

Figure 4. **Channel typologies and components of the maritime network**

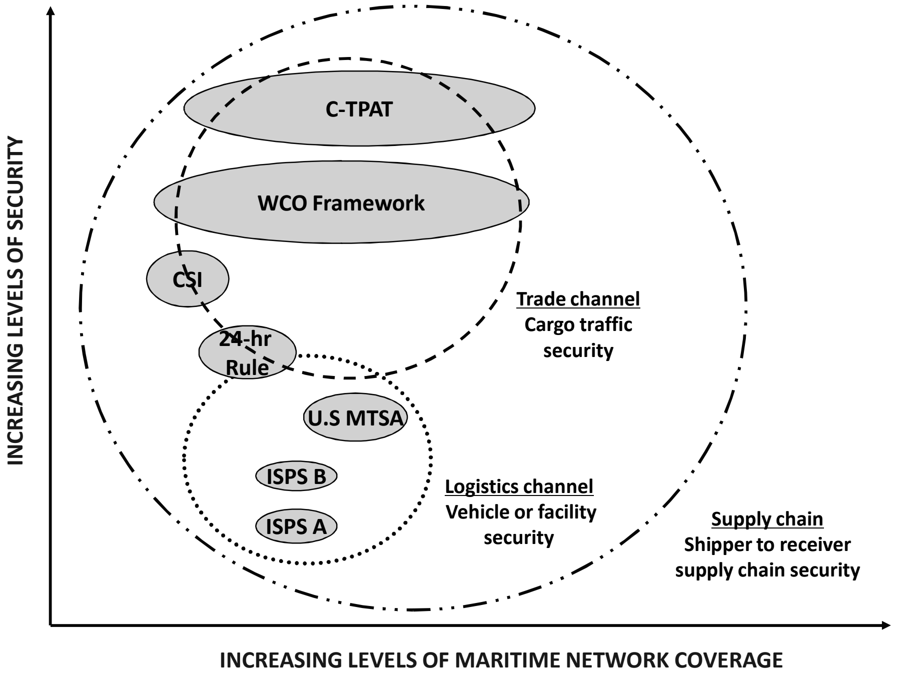

International Maritime System Network
Objectives
Trade Channel
Trading nations and their government agencies (customs, health authorities, designated authority and RSO in the context of ISPS, transport regulators, etc.)
Trade control, regulation, facilitation, etc.
Information flows
Supply Channel
Cargo-owners (suppliers, manufacturers, shippers/receivers) and sub-contracting firms along the supply chain
Collaborative arrangements and integration of organizational supply
Payment flows
Logistics Channel
Non-cargo owning facilitators and intermediaries contracted by supply chain members (ocean carriers, ports/terminal operators, logistics providers, shipping agents, NVOCCs, etc.)
Efficient management and cost control over physical movement and associated information
Physical flows

Source: Bichou, 2007b.

As a justification for the need for a layered framework to port and maritime security, consider a typical global movement of a containerised cargo, which is estimated to involve as many as 25 parties and a compound number of flow-configurations within and across the supply-chain network. Because of the increased trend of outsourcing and contract logistics, the role and scope of control exercised by members of the supply channel (mainly manufacturers, shippers and receivers) would only be limited to overseeing the management of direct interactions between them rather than the details of logistical arrangements. Arrangements such as cargo consolidation and break bulk, multi-modal combinations, transhipment and reverse logistics are typically performed by third parties including ports and other intermediaries. In a similar vein, the trade channel stakeholders (regulators, customs, health authorities, etc.) may be able to scrutinise and monitor the logistical segment within their own national territory, but would have little or no control over arrangements taking place in a foreign country, including at transit and transhipment locations. Thus, the combination of intersecting functional and institutional arrangements across the supply chain makes it almost impossible for a single actor within a single channel to effectively trace and monitor every cargo movement and operation across different channels. This largely explains the use of a multi-channel layered approach to monitor the security of maritime and port operations, for instance through regulations such as the CSI and the 24-hour rule.

Figure 5 depicts the hierarchy of regulatory programmes by level of security and supply-chain coverage. The levels relative to each programme are hypothetical but typical.

Figure 5. **Hierarchy of security measures by level of security and network coverage**


C-TPAT
WCO Framework
CSI
24-hr Rule
U.S MTSA
ISPS B
ISPS A
Trade channel
Cargo traffic security
Logistics channel
Vehicle or facility security
Supply chain
Shipper to receiver supply chain security
INCREASING LEVELS OF SECURITY
INCREASING LEVELS OF MARITIME NETWORK COVERAGE

Source: Bichou, 2005.

One can argue, however, that the layered approach, as being currently implemented, has not yet materialised into an integrated and comprehensive system capable of overcoming existing and potential security gaps. For instance, the emphasis on goods and passenger movements has diverted attention away from non-physical movements, such as financial and information flows. The latter involve the use of a range of communications systems, including radar systems and electronic data interchange (EDI); but no agreed procedure on ensuring the security of such systems, as well as on related data security in the context of maritime operations, has been incorporated into the current maritime security framework. Other security gaps include the exclusion from the current regulatory regime of fishing vessels, pleasure crafts and yachts, and other commercial ships of less than 500 GT. There is also a lack of harmonization between the new security regime and other maritime environmental and safety programmes, such as the STCW Convention and the ISM and IMDG codes.

Another aspect of interest when examining maritime network security is the interplay between supply- chain security and supply-chain risk, the latter being closely related to uncertainties stemming from specific supply-chain configurations. Juttiner *et al.* (2003) review the literature on supply-chain risk management and categorise sources of supply-chain risk into three major groups:

- Environmental risk sources, corresponding to uncertainties associated with external sources such as terrorism or environmental risks;
- Organisational risk sources, relating to internal uncertainties within the supply chain, for instance strikes or production failures; and
- Network-related risk sources, referring to uncertainties arising from the interactions between organisations in the supply chain.

The current maritime security framework strongly emphasizes environmental and organisational risk sources, but there is less focus on network-related vulnerabilities. However, excluding or minimising network-related risk sources may overlook the capacity of the system to either absorb or amplify the impact of events arising from environmental or organisational sources. Examples of network-related risk drivers in maritime security include uncertainties caused by contracting with non-compliant (non-certified) supply-chain partners. A recent study involving 20 top US firms has shown that there is a tendency among American shippers towards trading off lowest bidders with known suppliers (MIT/CTS Interim Report, 2003). There have been similar examples across the shipping and port industry, for instance, shipping lines changing their ports of call because of the existence or absence of a regulatory programme.

4. ECONOMIC EVALUATION AND APPRAISAL OF MARITIME SECURITY MEASURES

In view of the new security regime, maritime operators have had to implement security measures in order to comply with security initiatives, and the route to compliance frequently requires investment in security equipment, procedures and the recruitment and training of security personnel. In addition to the cost of compliance, port operators and users alike may incur extra costs stemming from the implementation of new procedural security and the provisions for detailed reporting, further inspections and other operational requirements. Therefore, the literature on the cost impacts of maritime security may be classified into two main categories: compliance costs and procedural and operational costs.

4.1. Compliance cost of port security

4.1.1 Ex-ante assessment

Even before the entry into force of the new security regulations, several studies have attempted to assess the compliance cost of port security, particularly for formal security regulations such as the ISPS code. *Ex-ante* assessments of the compliance cost of maritime and port security are largely based on data and methods from national regulatory risk assessment models, such as the US National Risk Assessment Tool (N-RAT) and the UK Risk Assessment Exercise (RAE). These are ad hoc programmes undertaken by governmental agencies in order to assess the costs and benefits of new regulatory initiatives. For instance, the US Coast Guard (USCG) has estimated the ISPS compliance cost for US ports to reach USD 1.1 billion for the first year and USD 656 million for each year up to 2012. Based on these estimates, the Organisation for Economic Co-operation and Development (OECD, 2003) has produced a comprehensive report on the global economic impacts of maritime security measures. A summary of aggregate, *ex-ante* estimates for ISPS cost compliance is provided in Table 8. Regarding non-ISPS initiatives, a study funded by the European Commission (EC) suggests that voluntary security programmes, based on a participation level of 30% of European Union (EU) operators, would cost port and terminal operators in the EU around €5 million just for audit expenses (DNV Consulting, 2005).

Table 8. **Summary of ISPS ex-ante cost estimates as computed by various regulatory risk assessment impacts**

Source of estimates	Cost items	Scope	Initial Costs*	Annual Costs*	Total cost* over 10 years (2003-13) @ 7% DFC
USCG	Total ISPS US ports	226 port authorities, of which 5000 facilities are computed (from Fairplay) (ISPS Parts A & B MARSEC Level 1)	1125	656	5399
	Total ISPS US-SOLAS and non-SOLAS vessels subject to the regulation	3500 US-flag vessels, as well as domestic and foreign non-SOLAS vessels (i.e. operating in US waters) (ISPS Parts A & B MARSEC Level 1)	218	176	1368
	Automated Identification System		30	1	50
	Maritime Area (contracting government)	47 COTP US zones	120 (+106 for 2004)	46	477
	OSC facility (offshore installations)	40 US OCS Facilities under US jurisdiction	3	5	37
	US cost for ISPS implementation	**(ISPS parts A and B)**	**115**	**884**	**7331**
	Aggregate Cost of elevating MARSEC level from 1 to 2	Based on a twice MARSEC level 2 per annum, each for 21 days	16 per day		
UK	Total ISPS UK port facilities	430 facilities (ISPS Part A MARSEC Level 1)	26	2.5	
	Total ISPS UK-flagged ships and company related costs	620 UK-flag vessels (ISPS Parts A, MARSEC Level 1) (Calculations based on an exchange rate of UK= £1.6 USD	7.4	5.2	
OECD	AIS	Based on 43 291 international commercial fleet of more than 1 000 GT (Passenger and cruise vessels not included), MARESC Level 1, ISPS Part A only	649.3	Undetermined	
	Other vessel measures		115.11	14.6	
	Ship operating companies		1163.89	715.4	
	Total ships & shipping companies		**1279**	**730**	
	PFSA, PFSA, PFSP	2 180 port authorities worldwide, of which 6,500 facilities are computed (from Fairplay) (ISPS Part A only MARSEC Level 1)	390.8	336.6	
	Total ISPS ports		Undetermined	Undetermined	
	Global cost for ISPS implementation	(MARESC level 1, ISPS part A only)	Undetermined	Undetermined	
Australian Government	Total costs for Australia	70 Australian flag ships and 70 ports, of which 300 port facilities	240 AUD	74 AUD	
Shipowners' association	Total costs for vessels	47 Australian vessels	29655 AUD		

*: All cost figures are expressed in 2003 USD million, except for Australia where costs are expressed in 2002 AUD million.

Legend:

AIS: Automated Information System, AUD: Australian Dollar, COTP: Captain of the Port, DFC: Discount Factor, GT: Gross tons, MARSEC: Maritime Security Level, OSC: Outer Continental Shelf, PFSA: Port Facility Security Assessment, PFSO: Port Facility Security Officer, PFSP: Port Facility Security Plan, SOLAS: The IMO International Convention on the Safety of Life at Sea

Source: Bichou, 2005b.

4.1.2 Ex-post assessment

Following the entry into force and implementation of the new security measures, a number of *ex post* assessments of the cost of compliance have been undertaken. In so doing, researchers have used a variety of approaches, ranging from survey inquiries and economic impact studies to financial appraisal and insurance risk modelling:

- Among the plethora of survey inquiries on the subject, it is worth mentioning the United Nations' Conference on Trade and Development (UNCTAD) global survey on initial and annual costs of ISPS compliance. The survey results suggest that for each ton or TEU handled, the average cost for ISPS compliance would amount to USD 0.08 and USD 3.6 respectively, of which USD 0.03 and USD 2 in terms of annual (recurrent) costs, respectively (UNCTAD, 2007). However, a recent survey by the World Bank found that the average ISPS compliance costs amount to USD 0.22 per ton and USD 4.95 per TEU handled (Kruk and Donner, 2008). Such contradictory findings may be explained by the variety of methods used to calculate the ISPS costs (unit versus average, initial versus running, etc.), but can also stem from the different interpretations of the Code across world ports and terminals (Bichou, 2004; Bosk, 2006). While the ISPS Code provides general provisions on security requirements in ports, it does not prescribe detailed and uniform instructions on how to comply with them, for instance, in terms of the exact instructions on the type and height of fences required for each port or terminal facility.

- Another problem with survey inquiries occurs when the findings of a case-specific survey are generalised to all stakeholders and/or security programmes. For instance, Thibault *et al.* (2006) found that small ocean carriers generally enjoy lesser initial compliance costs but incur higher recurrent costs because of the difficulty to spread fixed costs across a small business base. However, Brooks and Button (2006) found that the costs of enhanced maritime and supply-chain security only accounts for 1% or less of shippers' total costs. Even when survey inquiries investigate a single security programme, their results may show inconsistent cost figures, either over time or between participants. For example, when first enrolments in the C-TPAT programme began in 2004, the industry widely quoted Hasbo's figures of USD 200 000 initial costs and USD 113 000 annual operating costs as being the benchmark for C-TPAT average compliance cost for a multinational firm (Googley, 2004). However, in a recent survey of 1 756 C-TAPAT certified participants, Diop *et al.* (2007) report that C-TPAT implementation and operating costs only amount to USD 38 471 and USD 69 000, respectively. Furthermore, according to the same survey, 33% of respondents said that the benefits of C-TPAT participation outweighed the costs, while an additional 25% found that the CTPAT costs and benefits were about the same. Other surveys on the subject also provide contradictory results – see Lloyd's List (2003) and BDP (2004).

- As with survey inquiries, economic impact studies on the cost of port and maritime security also depict inconsistent results. For example, Damas (2001) estimated that the new security measures introduced in the awake of the 9/11 terrorist attacks would cost the US economy as much as USD 151 billion annually, of which USD 65 billion just for logistical changes to supply chains. However, a study undertaken by the International Monetary Fund in the same year has estimated the increase in business costs due to higher security costs to be around USD 1.6 billion per year, with an extra financing burden of carrying 10% higher inventories at USD 7.5 billion per year (IMF, 2001). Such discrepancies are also observable in studies seeking to quantify the economic and supply-chain cost of port security incidents and other similar disruptions such as industrial action and natural disasters. For instance, Martin Associates (2001) estimated that the cost to the US economy of the West-Coast port lockout in 2001 to reach USD 1.94 billion a day, based on a 10-day shutdown of port facilities. However, by the time the labour dispute was resolved, Anderson (2002) priced the total economic cost at around USD 1.7 billion, based on a longer shutdown period of 12 days.

- Other researchers have looked at the knock-on effect of the US port closure on other dependent economies and foreign ports. For example, Saywell and Borsuk (2002) estimated the loss from this disruption be as high as 1.1% of the combined GDP of Hong Kong, Singapore and Malaysia. In a similar vein, Booz Allen Hamilton (2002) ran a port security war game simulation to assess the impacts of a terrorist incident in a US port followed by a nation-wide port and border-crossing closure for eight days. With an estimated cost to the US economy of USD 50 billion, their simulation showed results inconsistent with those of previous studies. Pritchard (2002) and Zuckerman (2002) suggest even lower costs than those reported above.

- Cost assessment of regulatory initiatives may also be undertaken through financial and insurance risk modelling. For the former, *ex-post* costs are typically assessed by analysing market response to risk-return performance, for instance by translating security provisions into port investments and analysing their *ex-post* impact using models and techniques of financial appraisal and risk analysis. For the latter, researchers typically use premium-price analysis, whereby security costs and benefits are added to or subtracted from the price of port and shipping services, referring *inter alia* to the variations in freight rates and insurance premiums. For instance, Richardson (2004) reports that insurance premiums trebled for ships calling at Yemeni ports after the 2002 terrorist attack on the oil tanker *Limburg* off the Yemeni coast, which has also forced many ships to cut Yemen from their schedules or divert to ports in neighbouring states.

- Trade facilitation studies can also be used to analyse the *ex-post* impacts of security, such as by measuring the time factor (delay or speed-up) brought by security measures. Nevertheless, despite the rich literature on the interface between trade facilitation and economic development (Hummels, 2001; Wilson *et al.*, 2003), few studies have investigated the role of the new security regime as either a barrier or an incentive to trade (Raven, 2001). For instance, the OECD (2002) reports that post-9/11 trade security measures would have cost from 1% to 3% of North American trade flows, corresponding to a cost of between USD 60 billion and USD 180 billion in 2001 figures. Another estimate places the global costs for trade of post-9/11 tighter security at about USD 75 billion per year (Walkenhorst and Dihel, 2002).

- Another way to analyse the cost benefit of a regulatory change is to contrast transfer costs against efficiency costs. The former refer to the costs incurred and recovered by market players through transferring them to final customers (e.g. from ports to ocean carriers or from ocean carriers to shippers), while the latter represent net losses and benefits in consumer and producer surpluses. Compiled cost figures from industry and press reports suggest an average security charge of USD 6 per shipped container, and up to USD 40 per bill of lading for the 24-hour rule. Note that this approach is not without bias, including the common practice of cost spin-off and exponential computations of security expenses. In a highly disintegrated and fragmented maritime and logistics industry, there is no guarantee that additional security charges accurately reflect the true incremental costs incurred by each operator, including ports. Standard practices in the industry suggest that market players try to generate extra profits by transferring costs to each other (Evers and Johnson, 2000; Fung *et al.*, 2003), and there is already evidence of similar practices in the recovering of security costs by the port industry (see Table 9).

Table 9. **Sample of container ports' security charges**

Port or terminal			Security fee USD ($)/TEU
Europe	Belgian ports		10.98
	France and Denmark		6.1
	Dutch ports		10.37
	Italian ports		9.76
	Latvian ports		7.32
	Norwegian ports		2.44
	Spanish ports		6.1
	Irish ports		8.54
	Swedish ports (Gothenburg)		2.6
	UK ports	Felixstowe, Harwich and Thames port	19 for import and 10 for export
		Tilbury	12.7
USA	Charleston, Houston and Miami		5
	Gulf seaports marine terminal conference		2
Others	Shenzhen (China)		6.25

Source: Compiled by the Author from various trade journals.

4.2. Procedural and operational impacts

The increasing interest in the procedural and operational impacts of security has been fed largely by the continuing debate between those who anticipate productivity losses because of operational redundancies and those who advocate higher operational efficiency due to better procedural arrangements:

– On the one hand, many argue that the procedural requirements of the new security regime act against operational and logistical efficiency. Proponents of this standpoint list a number of potential inefficiencies, ranging from direct operational redundancies, such as lengthy procedures and further inspections, to derived supply chain disruptions, as in terms of longer lead times, higher inventory levels and less reliable demand and supply scenarios. The 24-hour rule provides a typical example of procedural requirements with potentially negative impacts on operational and logistics efficiencies. For example, the requirements of the 24-hour rule will result in ocean carriers declining any late shipment bookings but also bearing, under customary arrangements, the cost of at least one extra day of container idle time at ports. The latter may be extended to three days or more for carriers and forwarders that are not electronically hooked into the US CBP Automated Manifest System (AMS). Shippers and receivers alike will then have to adjust their production, distribution and inventory management processes accordingly. Ports will also bear the commercial and cost impacts of the 24-hour rule, including potential congestion problems and possible delays in both ships' departures and arrivals. Additional costs to shippers may also stem from the extra time and resources needed for carriers to compile and record detailed data information. In fact, shipping lines have already started transferring the cost of the 24-hour rule data filing and processing requirements to shippers and cargo owners who now have to pay an extra USD 40 levying charge per bill of lading (Lloyd's List, 2003), plus any additional indirect costs from advanced cut-off times and changes in production and distribution processes. Ocean carriers and NVOCCs may also be faced with a violation fine of USD 5 000 for the first time and USD 10 000 thereafter if they submit missing or inaccurate data to CBP. A detailed review of the 24-hour requirements, costs and benefits is provided by Bichou *et al.* (2007a).

– On the other hand, proponents of new security measures argue that their implementation is not only necessary but can also be commercially rewarding. The main argument put forward is that measures such as the CSI, the 24-hour rule and the C-TPAT fundamentally shift the focus from inspection to prevention, the benefit of which offsets and ultimately outweighs the initial and recurrent costs of implementation. Detailed data recording, electronic reporting and other procedural requirements brought about by the new security regulations would allow for pre-screening and deliberate targeting of "suspect" containers, which is proven as more cost-effective and less time-consuming than the traditional approach of random physical inspections. In addition to the benefits of access certification and fast-lane treatment, compliant participants would also benefit from reduced insurance costs, penalties and risk exposure. Other advantages that go beyond the intended security benefits include the protection of legitimate commerce, the exposure of revenue evasion, reduced risk of cargo theft and pilferage, real-time sharing of shipping and port intelligence, advanced cargo processing procedures and improved lead-time predictability and supply-chain visibility.

Nevertheless, both arguments are rarely supported by empirical analysis and much of the analytical research on procedural security impacts uses modelling techniques to predict the operational costs and benefits of security. Lee and Whang (2005) have developed a mathematical model to assess the benefits of reduced lead times and inspection levels in the context of Smart and Secure Trade-lanes (SST). White (2002) also used mathematical modelling by developing a min-depth heuristic to minimise the number of container moves in the case of CSI. Using simulation, Babione *et al.* (2003) examined the impacts of selected security initiatives on import and export container traffic at the port of Seattle. Rabadi *et al.* (2007) used a discrete event simulation model to investigate the impact of security incidents on the recovery cycle for the US container terminal of Virginia. Other simulators have been specifically designed to run pre-defined disruption scenarios and predict their impacts on port efficiency. For example, the national infrastructure simulation and analysis centre (NISAC) has developed two port simulators, an operations simulator to evaluate the short-term operational impacts, and an economic simulator to assess long-term economic impacts (NISAC, 2005).

4.3. CBA and maritime security

In evaluating the costs and benefits for optimal regulatory decisions, cost-benefit analysis (CBA) is regarded as a fairly objective method of making assessments. Cost-efficiency analysis (CEA) is an alternative method to CBA, usually applied when the output is fixed and the economic benefits cannot be expressed in monetary terms. CBA and CEA are widely used to assess the efficiency of various measures and alternatives, such as in terms of a new regulatory regime or a new investment (e.g. in infrastructure or technology). In the context of maritime regulation, CBA is a key component of the FSA methodology and other formal assessment procedures.

However, in a typical CBA or CEA model the results of implementing a regulation can be entirely different from one stakeholder (firm, nation-state, etc.) to another. The concept of externality is very difficult to apprehend in the context of malicious incidents. According to the definition of externality, costs arising from accidents are external when one person or entity causes harm to another person, or a third party, involved in the accident without providing appropriate compensation. Risk decisions regarding the introduction of regulatory measures involve multiple stakeholders who influence decisions through a complex set of legal and deliberative processes. Whether this is beneficial to the whole community or not is very debatable, given the differences between stakeholders' values and perspectives. In a typically fragmented maritime industry, this focus raises the important question: who will bear the cost of, or gain the benefits from, compliance with statutory measures?

To correct CBA/CEA deficiencies, particularly with regard to cost sharing and distribution, Stakeholder Analysis (SHA) was introduced in the early 1980s. SHA is designed to identify the key players (stakeholders) of a project or a regulation, and assess their interests and power differentials for the purpose of project formulation and impact analysis. Several procedures have been proposed for SHA implementation, with the World Bank's four-step formula (stakeholders identification, stakeholders interests, power and influence inter-relationships, and strategy formulation) being the most recognised and widely used. It must be noted, however, that there is no clear-cut predominance of one method over another, and quite often not all the conditions for the implementation of a complete regulatory assessment exercise are met.

An important element in any valuation method of new regulatory decisions is the cost of preventing principal losses in security incidents, a key component of which stems from human casualties, that is fatalities and injuries. However, since the value of these losses is not observable in market transactions, most economists believe that these valuations should be based on the preferences of those who benefit from security measures and who also pay for them, either directly or through taxation. In the context of casualty prevention, these preferences are often measured using the "willingness to pay" (WTP) approach, i.e. the amount people, or society, are willing to pay to reduce the risk of death or injury before the events. There are two major, empirical approaches to estimating WTP values for risk reductions, namely, the revealed preference method (RPM) and the stated preference method (SPM). RPM involves identifying situations where people (or society) do actually trade off money against risk, such as when they may buy safety (or security) measures or when they may take more or less risky jobs for more or less wages. SPM, on the other hand, involves asking people more or less directly about their hypothetical willingness to pay for safety/security measures that give them specified reductions in risk in specified contexts. The WTP approach has been extensively used in the context of road safety, but little literature exists on the use of the methodology in the context of shipping safety, let alone in the context of maritime and port security. The problem with the WTP approach in the latter context is that it is difficult to assume that people or society are capable of estimating the risks they face from terrorism (RPM) or that they are willing to answer questions about trading-off their security, or safety, against a given amount of money (SPM).

CONCLUSION

This paper is intended to serve as a conceptual piece that draws from the interplay between engineering and supply-chain approaches to risk in the context of recent maritime security regulations. It is hoped that cross-disciplinary analysis of the perception and impact of the security risk will stimulate thinking on appropriate tools and analytical frameworks for enhancing port and maritime security. In so doing, it may be possible to develop new approaches to security assessment and management, including such aspects as supply-chain security.

The framework and methods reviewed in this paper could serve as a roadmap for academics, practitioners and other maritime interests to formulate risk assessment and management standards and procedures in line with the new security threats. In particular, new and relevant approaches can be developed to assess the reliability of maritime security in the context of complex network theory (Bichou, 2005; Angeloudis *et al.*, 2006; Bell *et al*., 2008). Equally, further research can build on this to investigate the mechanisms and implications of security measures on port and shipping operations, including such aspects as the impacts of security on operational and supply-chain efficiency (Bichou, 2008a) and the assessment of risk and returns from security investments (Menachof and Talas, 2008; Bichou, 2008b).

BIBLIOGRAPHY

Accorsi, R., G. Apostolakis, E. Zio (1999), Prioritising stakeholder concerns in environmental risk management, *Journal of Risk Research*, 2 (1), 11-29.

Angeloudis, P., K. Bichou, M.G.H. Bell and D. Fisk (2007), Security and reliability of the liner container-shipping network: analysis of robustness using a complex network framework, In: Bichou, K., M.G.H. Bell and A. Evans (2007), *Risk Management in Port Operations, Logistics and Supply Chain Security*, Informa: London.

Babione, R., C.K. Kim, E. Rhone and E. Sanjaya (2003), *Post 9/11 Security Cost Impact on Port of Seattle Import/Export Container Traffic*, University of Washington: GTTL 502 Spring Session.

Bedford, T. and R. Cooke (2001), *Probabilistic Risk Analysis: Foundations and Methods*, Cambridge University Press.

Bell, M.G., U. Kanturska and J.D. Schmocker (2008), Attacker-defender models and road network vulnerability, *Philos Transact A Math Phys Eng Sci,* 366, 1893-1906.

Bichou, K., M.G.H. Bell and A. Evans (2007a), Risk Management in Port Operations, Logistics and Supply Chain Security, Informa: London.

Bichou K, Lai K.H., Lun Y.H. Venus and Cheng T.C. Edwin, 2007b, A quality management framework for liner shipping companies to implement the 24-hour advance vessel manifest rule, *Transportation Journal*, 46(1), 5-21

Bichou, K. and A. Evans (2007c), Maritime Security and Regulatory Risk-Based Models: Review and Critical Analysis,. in: Bichou, K., M.G.H. Bell and A. Evans (2007), *Risk Management in Port Operations, Logistics and Supply Chain Security*, Informa: London.

Bichou, K. (2008b), Security of Ships and Shipping Operations, in: Talley, 2008 (eds.), *Ship Piracy and Security*, Informa, 73-88.

Bichou, K. and R. Gray (2005), A critical review of conventional terminology for classifying seaports, *Transportation Research A*, 39, 75-92.

Bichou, K. (2004), The ISPS code and the cost of port compliance: an initial logistics and supply chain framework for port security assessment and management, *Maritime Economics and Logistics,* 6 (4), 322-348.

Bichou, K. (2005), *Maritime Security: Framework, Methods and Applications*. Report to UNCTAD, Geneva: UNCTAD, June.

Bier, V.M. (1993), Statistical methods for the use of accident precursor data in estimating the frequency of rare events, *Reliability Engineering and System Safety*, 42, 267-280.

Bird, F.E. and G.L. Germain (1996), *Practical Loss Control Leadership*, Det Norske Veritas: Alberta.

Brooks, M.R. and K.J. Button (2005), Market Structures and Shipping Security, *Proceedings of the 2005 Conference of the International Association of Maritime Economists*, Limasol: Cyprus, June.

Bureau d'Enquêtes et d'Analyse pour la Sécurité de l'Aviation Civile (BEA) (2002), *Rapport sur l'Accident de Air France Concorde F-BTSC ayant lieu le 25 Juillet 2000 à la Patte d'Oie,* Paris: Ministère de l'Equipement, du Transport et du Logement.

Bureau of Transportation Statistics (BTS) (2002), Project 6 Overview: Develop Better Data on Accident Precursors or Leading Indicators, *Safety Numbers Conference Compendium*, Washington DC: BTS.

Cullen, W.D. (2000), *The Ladbroke Grove Rail Inquiry*, Norwich: Her Majesty's Stationery Office.

Damas, P. (2001), Supply chains at war, *American Shipper*, November, 17-18.

Darren, P. (2004), Smart and safe borders: the logistics of inbound cargo security, *International Journal of Logistics Management*, (15) 2, 65-75.

De Kay *et al*. (2002), Risk-based decision analysis in support of precautionary policies, *Journal of Risk Research*, 5 (4), 391-417.

Diop, A., D. Hartman and D. Rexrode (2007), *C-TPAT Partners Cost/Benefit Survey*, CBP: Washington, DC.

Erkut, E. and A. Ingolfsson (2000), Catastrophe avoidance models for hazardous materials route planning, *Transportation Science*, 43 (2), 165-179.

European Conference of Ministers of Transport (ECMT) (2004), *Container Transport Security across Modes*, OECD: Paris.

Evers, P.T. and C.J. Johnson (2000), Performance perceptions, satisfaction, and intention: the intermodal shipper's perspective, *Transportation Journal*, 40 (2): Winter.

Flynn, S. (2004), America the Vulnerable: How our Government is Failing to Protect Us from Terrorism, NY: Harper-Collins Publishing.

Fung, M.K., L.K. Cheng and L.D. Qiu (2003), The impact of terminal handling charges on overall shipping charges: an empirical study. *Transportation Research Part A,* 37 (8): 703-716.

Gooley, T.B. (2004), C-TPAT: Separating hype from reality, *Logistics Management*, August 1.

Grencser, M., J. Weinberg and D. Vincent (2003), *Port Security War Game: Implications for US Supply Chains*, Booz Aallen Hamilton.

Guasch, J.L. (2000), New Port Policies in Latin America and the Caribbean, New Press.

Helferich, O.K. and R.L. Cook (2002), *Location and Networks: Theory and Algorithms*, MIT Press.

Hummels, J. (2001), Time as a trade barrier, Mimeo: Purdue University, 1-40.

International Maritime Bureau, On-line www.icc-ccs.org

International Monetary Fund (IMF) (2001), World Economic Outlook: The Global Economy after September 11, http://www.imf.org/external/pubs/ft/weo/2001/03, accessed December 2005.

Joseph, G.W. and G.W. Courtier (1993), Essential management to support effective disaster planning, *International Journal of Information Management*, 13 (5), 315-325.

Juttner, U., U.H. Peck and M. Christopher (2003), Supply Chain Risk Management: Outlining an Agenda for Future Research, *International Journal of Logistics: Research and Applications*, 6 (4), 197-210.

Kruk, B. and M.L. Donner (2008), Review of Cost of Compliance with the New International Freight Transport Security Requirements, *World Bank Transport Papers,* TP 16: 1-58, February.

Lake, E.J., W.L. Robinson and L.M. Seghetti (2004), *Border and Transportation Security: The Complexity of the Challenge*, Washington, DC: CRS Report RL23839.

Lee, H.L. and S. Whang (2005), Higher supply chain security with lower cost: lessons from total quality management, *International Journal of Production Economics*, 96 (3), 289-300.

Menachof, D. and R. Talas (2009), The Efficient Trade-Off between Security and Cost for Sea Ports: a Conceptual Model, *International Journal of Risk Assessment and Management*, Forthcoming.

Organisation for Economic Co-operation and Development (OECD) (2002), The Impact of the Terrorist Attacks of 11 September 2001 on International Trading and Transport Activities, Working Party of the Trade Committee, OECD: Paris [TD/TC/WP(2002)9/FINAL].

Organisation for Economic Co-operation and Development (OECD) (2003), *Security in Maritime Transport: Risk Factors and Economic Impact*, Maritime Transport Committee, Paris: OECD.

Phimister, J.A., V.M. Bier and H.C. Kunreuther (eds.) (2004), *Accident Precursor Analysis and Management: Reducing Technological Risk through Diligence*, National Academy of Engineering, Washington, DC: The National Academies Press.

Rabadi, G., C.A. Pinto, W. Talley and J.P. Arnaout (2007), Port recovery from security incidents: a simulation approach, in: Bichou, K., M.G.H. Bell and A. Evans (2007), *Risk Management in Port Operations, Logistics and Supply Chain Security*, Informa: London, 83-94.

Richardson, M. (2004), Growing vulnerability of Seaports from Terror Attacks, to protect ports while allowing global flow of trade is a new challenge, *Viewpoint,* Institute of South East Asian Studies, also available on-line at: www.**iseas.edu**.sg

Russell, D.M. and J.P. Saldana (2003), Five tenets of security-aware logistics and supply chain operation, *Transportation Journal*, 42, 4, 44-54.

Stavins, R.N. (ed.), *Economics of the Environment*, 4th Edition, Norton & Co: New York NY. pp. 378-393.

The Gore Commission (1997), *Report to the White House on Aviation Safety and Security*, also available on-line http://www.fas.org/irp/threat/212fin~1.html

The MIT/CTS Interim Report, 2003, *Supply Chain Response to Terrorism: Creating Resilient and Secure Supply Chains*. Also available on-line at: http://web.mit.edu/scresponse/repository/SC_Resp_Report_Interim_Final_8803.pdf

The US Federal Register (2003), *N-RAT Assessment Exercise*, 204 (68), 60464-6046.

The US Nuclear Regulatory Commission (US NRC) (1978), *Risk Assessment Review Group Report*, NUREG/CR-400, NRC: Washington, DC.

The World Bank Group (2001), *Stakeholder Analysis*, also available on-line under social development/social assessment: http://www.worldbank.org/social

UNCTAD (2004), Container Security: Major Initiatives and Related International Developments, Report by the UNCTAD Secretariat, Geneva: UNCTAD.

UNCTAD (2007), Maritime Security: ISPS Implementation, Costs and Related Financing, Report by the UNCTAD Secretariat, Geneva: UNCTAD.

Walkenhorst, P. and N. Dihel (2002), *Trade Impacts of the Terrorist Attacks of 11 September 2001: A Quantitative Assessment*, Workshop on the Economic Consequences of Global Terrorism, DIW/German Institute for Economic Research: Berlin.

Wilson, J., C. Mann and T. Otsuki (2003), Trade Facilitation and Economic Development: Measuring the Impact, *The World Bank Economic Review*, 17, 367-389.

Willis, H.H. and D. Ortiz (2004), *Evaluating the Security of the Global Containerised Supply Chain*, RAND Technical Report series.

LIST OF PARTICIPANTS

Prof. Andrew EVANS **Chairman**
Transport Risk Management
University of London
618, Skempton Building
Imperial College London
LONDON SW7 2AZ
United Kingdom

Dr. Khalid BICHOU **Rapporteur**
Imperial College London
Centre for Transport Studies
618, Skempton Building
LONDON SW7 2BU
United Kingdom

Prof. André DE PALMA **Rapporteur**
Ecole Normale Supérieure de Cachan
61 avenue du Président Wilson
F-94235 CACHAN CEDEX
France

Prof. Peter GORDON **Rapporteur**
University of Southern California
School of Policy Planning & Development
Ralph & Goldy Lewis Hall 321
LOS ANGELES
CA 90089-0626
USA

Dr. Robert POOLE **Rapporteur**
Director of Transportation Studies
Reason Foundation
3415 S Sepulveda Blvd # 400
CA 90034 LOS ANGELES
USA

Dr. Torkel BJORNSKAU
Chief Political Scientist
Institute of Transport Economics
Gaustadalleen 21
NO-0349 OSLO
Norway

Mr. Andrew COOK
Head of Land Transport Security Policy Development
TRANSEC
Department for Transport
105 Victoria Street
GB-LONDON SW1E 6DT
United Kingdom

Dr. Andrew GRAINGER
Director
Trade Facilitation Consulting Limited
30 Jemmett Close
GB-KINGSTON UPON THAMES
Surrey KT2 7AJ
United Kingdom

Dr. Juha HINTSA
Senior Researcher
Supply Chain Security and Customs Risk Management
Cross-Border Research Association
c/o BMT, Ave. d'Echallent 74
CH-1004 LAUSANNE
Switzerland

Dr. Brian JACKSON
Associate Director
Homeland Security Program
RAND Corporation
1200 South Hayes Street
ARLINGTON, VA 22202
USA

Mr. Carl KOOPMANS
Netherlands Institute for Transport Policy Analysis (KiM)
Ministry of Transport, Public Works and Water Management
P O Box 20901
NL-2500 EX LA HAYE
The Netherlands

Prof. Dr.-Ing. Juergen KRIEGER
Director
Head of Division Bridges and Structural Engineering
Federal Highway Research Institute
Bruederstrasse 53
D-51427 BERGISCH GLADBACH
Germany

Mr. Chang-Yong LEE
Assistant Director
Port Management Division
Logistics Policy Bureau
Ministry of Land, Transport and Maritime Affairs
1 Joongang-Dong, Gwacheon
KR-427-712 GYEONNGGI-DO
Korea

Dr. Jung-Yoon LEE
Associate Research Fellow
Department of Logistics & Air Transport Research
Korean Transport Institute (KOTI)
2311 Daewha-Dong, Ilsan-Gu
KOYANG CITY
KOR-411 701 Kyunngi-Do
Korea

Dr. David LEVINSON
RP Braun/CTS Chair in Transportation Engineering
Associate Professor
Department of Civil Engineering
University of Minnesota
500 Pillsbury Dr SE
MINNEAPOLIS, MN 55455
USA

Mr. Alex MACFARLANE
Economic Adviser
Department for Transport
4/14 Great Minster House
76 Marsham Street
GB-LONDON SW1P 4DR
United Kingdom

Dr. Susan MARTONOSI
Assistant Professor of Mathematics
Harvey Mudd College
301 Platt Blvd
Claremont, CA 91711
USA

Prof. Daniel MIRZA
Professor of Economics
Université François-Rabelais, Tours
Faculté de Droit, d'Économie et des Sciences Sociales
50 avenue Jean Portalis - BP 0607
F-37206 TOURS Cedex 03
France

Dr. Andrew MORRAL
Director of Homeland Security
RAND Corporation
1200 South Hayes Street
ARLINGTON, Va. 22202-5050
USA

Mr. Serge PAHAUT
Research Collaborator
Université Libre de Bruxelles (CP 238)
Bd. du Triomphe
B-1050 BRUSSELS
Belgium

Prof. Barry E. PRENTICE
Professor, Supply Chain Management
Transport Institute
I.H. Asper School of Business
University of Manitoba
Winnipeg, MB R3T 5V4
Canada

Dr. Mark B. SALTER
Associate Professor
School of Political Studies
University of Ottawa
55 Laurier Avenue
OTTAWA ON K1N 6N5
Canada

Dr. Risto TALAS
Faculty of Management
Cass Business School
106 Bunhill Row
GB-London EC1Y 8TZ
United Kingdom

Dr. Nicolas TREICH
Toulouse School of Economics (TSE)
LERNA-INRA
21 all. de Brienne
Aile J.-J. Laffont
F-31042 TOULOUSE
France

Monsieur Rene VAN BEVER
Directeur général
Service public fédéral Mobilité et Transports
Secrétariat et Services logistiques
City Atrium
Rue du Progrès 56
B–1210 BRUSSELS
Belgium

Professor David WIDDOWSON
Chief Executive Officer
Centre for Customs & Excise Studies
University of Canberra
CANBERRA
Australia

ITF SECRETARIAT

Mr. Jack SHORT
Secretary General, ITF/
Director of Joint ITF/OECD Transport Research Centre

JOINT TRANSPORT RESEARCH CENTRE:

Mr. Stephen PERKINS
Head of Centre

Dr. Kurt VAN DENDER
Chief Economist

Mrs. Julie PAILLIEZ
Assistant

Ms. Françoise ROULLET
Assistant

ALSO AVAILABLE

Transport Infrastructure Charges and Capacity Choice : Self-financing Road Maintenance and Construction. Series ECMT – Round Table 135 (2007)
(74 2007 02 1 P) ISBN 978-92-821-0108-7

Estimation and Evaluation of Transport Costs. Series ECMT – Round Table 136 (2007)
(74 2007 06 1 P) ISBN 978-92-821-0151-3

Transport, Urban Form and Economic Growth. Series ECMT – Round Table 137 (2007)
(74 2007 07 1 P) ISBN 978-92-821-0164-3

Biofuels: Linking Support to Performance. Series ITF – Round Table 138 (2008)
(75 2008 02 1 P) ISBN 978-92-82-10179-7

Oil Dependence: Is Transport Running out at Affordable Fuel? Series ITF – Round Table 139 (2008)
(74 2008 03 1 P) ISBN 978-92-82-10121-6

The wider Economic Benefits of Transport: Macro-, Meso- and Micro-Economic Transport Planning and Investment Tools. Series ITF – Round Table 140 (2008)
(74 2008 04 1 P) ISBN 978-92-821-0160-5

17th International Symposium on Transport Economics and Policy: Benefiting from Globalisation – Transport Sector Contribution and Policy Challenges (2008)
(74 2008 01 1 P) ISBN 978-92-821-0168-1

Privatisation and Regulation of Urban Transit Systems. Series ITF – Round Table 141 (2008)
(74 2008 06 1 P) ISBN 978-92-821-0199-5

The Cost and Effectiveness of Policies to Reduce Vehicle Emissions. Series ITF – Round Table 142 (2008)
(74 2009 01 1 P) ISBN 978-92-821-0212-1

Port Competition and Hinterland Connections. Series ITF – Round Table 143 (2009)
(74 2009 02 1 P) ISBN 978-92-821-0224-4

To register for information by email about new OECD publications: www.oecd.org/OECDdirect
For orders on line: www.oecd.org/bookshop
For further information about ITF: www.internationaltransportforum.org

OECD PUBLISHING, 2, rue André-Pascal, 75775 PARIS CEDEX 16
PRINTED IN FRANCE
(74 2009 03 1 P) ISBN 978-92-821-0231-2 – No. 56805 2009

144

TERRORISM AND INTERNATIONAL TRANSPORT: TOWARDS RISK-BASED SECURITY POLICY

Security is critical to transport systems as they are often appealing targets for terrorist attacks. The significant costs of potential damage make effective security policies a key concern for transport decision makers. This *Round Table* examines the contribution economic analysis can make to improving security.

The analysis covers the impact of uncertainty in assessing security policies and on the cost effectiveness of security measures in aviation and maritime shipping. Much can be criticised in current policies, which are often seen as unduly expensive and inadequately assessed. This *Round Table* identifies methods for quantifying the benefits of security measures and assessing their effectiveness, and examines techniques to allocate resources to targeting the highest risks. Applying these techniques would achieve better levels of security with current resources.

www.internationaltransportforum.org

OECD*publishing*
www.oecd.org/publishing

(74 2009 03 1 P1) ISBN 978-92-821-0231-2

9 789282 102312