Risk Preferences and Decision-Support for PreCheck

This project will develop a risk-based assessment of the Transportation Security Administration’s PreCheck program considering risk preferences, threat likelihood, consequences, and co-benefits in a probabilistic terrorism risk framework.

1. **Theme Area:** Economics

2. **Principal Investigator:** Mark G. Stewart

3. **Lead Institution:** Newcastle Innovation, The University of Newcastle, Australia.

4. **Co-Investigators:** John Mueller

5. **Research Transition Lead:** Mark G. Stewart

6. **Keywords:** risk, economic assessment, cost-benefit, aviation security.

7. **Brief Description:**
The project would evaluate the cost-effectiveness of TSA’s PreCheck program which seeks to lower screening costs and enhance passenger satisfaction by allowing for more careful evaluation of higher-risk passengers while reducing the evaluation of lower-risk passengers. The project will model the checkpoint efficiencies for both the PreCheck and the regular screening lanes. A system reliability model allows the rate of deterrence and disruption to be inferred for 9/11 type and IED terrorist threats to aircraft. It will also include considerations of risk aversion, a policy preference for many public policy decision makers; these will be incorporated into the analysis through utility theory. Monte-Carlo simulation analysis of terrorist deterrence and detection, risk reduction and losses allow for the effectiveness and confidence intervals of policy preferences to be calculated.

8. **Research Objectives**
To determine whether an important screening innovation can improve efficiencies without notably lowering security. Monte-Carlo simulation will be used to propagate uncertainties in calculations of net present value, expected utility, and probabilities of net benefit. A break-even analysis is useful when there is uncertainty about threat likelihood. In this case, a stochastic analysis enables us to determine how many threats would need to occur for a 50, 90, 95 or 99 percent surety that PreCheck is cost-effective. The expansion of PreCheck to beyond the United States will also be considered. The project will provide the rigor needed for evidence-based policy. The models developed for the proposed project will be generic - they can also assess the effectiveness of other layers of security.

9. **Research Transition Objectives**
There is a clear need for rational, objective, and transparent methods to assess and compare risks and decision-making preferences of the TSA and DHS. An evaluation of PreCheck will illustrate the utility of such an approach, and provide evidence for policy making.

10. **Interfaces to Current CREATE Projects**
We are unaware of specific CREATE projects that bear resemblance to this project.
11. Previous or current work relevant to the proposed project:
We have published one book, *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security* (Oxford University Press) and 19 peer-reviewed journal articles on risk and cost-benefit analysis of homeland security measures, most of them related to aviation security in the United States. We have also written a book evaluating counterterrorism policing and intelligence that will be published by Oxford University Press in 2015. Stewart holds a SECRET clearance from the Australian Defence Force, and has briefed the Australian Federal Police on aviation security risks. The PreCheck project builds upon this expertise and is a logical extension of this research.

12. Major Deliverables, Research Transition Products and Customers
The product will be user-friendly computer software where the user can enter deterrence and disruption rates, costs and losses, as well as percentile (surety) of a decision.

13. Technical Approach
Our approach (i) maps out a system of the multiple layers of aviation security, (ii) assesses the effectiveness of each layer to deter, disrupt, or prevent an attack, (iii) models interactions between each layer recognizing that security measures are not perfectly substitutional (i.e. independent of each other) requiring event probabilities for all layers of security to be treated as conditional probabilities, (iv) takes into account the risk profile of passengers, (v) characterizes detection rates, risk reduction and losses as probabilistic variables allowing confidence intervals of policy preferences to be calculated, and (vi) uses utility theory to quantify levels of risk aversion. The data requirements for this approach are tractable. Game theory and other advanced methods of matching adversaries with countermeasures is instructive, but requires many assumptions for input variables, and assumes much about the capabilities of terrorists to “play the game.” Our approach is a “first pass” on the problem. It can be highly instructive, and reveal inefficiencies and overlapping security layers. The main advantage is that it is transparent and fully understandable by decision-makers - they are not blinded by the science. Our experience with policy-makers bears this out, often with the comment “I’ve seen lots of presentations on risk management, but this is the first I can understand.”

We favor a risk-neutral approach to decision-making, but recognize that public policy decision-making for low probability - high consequence events is often characterized by risk-aversion (e.g., Cha and Ellingwood 2012). Utility theory can be used to factor risk aversion into the decision process, and this project will infer utility functions that represent the level of risk averseness of the Department of Homeland Security (e.g., Stewart et al. 2011, Stewart and Mueller 2013b).

A practical approach is a break even cost-benefit analysis that finds the minimum likelihood of a successful attack required for a 50-50 chance that the benefit of security measures to equal their cost (e.g., Stewart and Mueller 2013a). The threat likelihood, then, is the output of the cost-benefit analysis, and it is the prerogative of the decision-maker, based on expert advice about the anticipated threat likelihood, to decide whether or not a security measure is cost-effective. If the threat likelihood is known with confidence, the break-even approach can be recast another way by calculating the minimum risk reduction required for a security measure to be cost-effective. While this approach is not without challenges (Farrow and Shapiro 2009), break even cost-benefit analyses are increasingly being used for homeland security applications (e.g. Willis and LaTourette 2008).

However, a break-even analysis assumes a risk-neutral approach to decision-making. A Monte-Carlo
simulation analysis enables us to also determine how many threats would need to occur for a 90, 95 or 99 percent surety that PreCheck is cost-effective. In other words, a cautious decision-maker may prefer a policy option that has a small likelihood of a net loss. For example, a policy option that ensures that there is 90% surety that benefits exceed the cost would be preferred over a break-even (50-50) policy option. This allows the risk preferences of the decision-maker to be explicitly considered in the decision analysis.

The novel aspect of this project is its attempt to quantify the risk reduction of each of the TSA layers of aviation security and then to assess whether PreCheck reduces risk enough to justify its costs. Given that PreCheck will result in reduced screening costs of $100 million in FY2015, PreCheck might be justified even if risks increase somewhat.

The first step is to develop a systems representation of all levels of aviation security that deal with hijacking and Improvised Explosive Device (IED) threats to aircraft. This will involve combinations of series and parallel systems with feedback loops and interdependencies such as common cause security breaches. Scenario analyses then reveal the human and technological factors that affect the effectiveness of each security measure by their ability to deter or disrupt an attack. The mapping of the aviation security system sets out the framework for the rest of the project. And this is the stage of the project where meetings with TSA and CREATE will be most beneficial to ensure that system representation is realistic and captures the key interactions and interdependencies - this is particularly important when modeling the effectiveness of PreCheck and regular screening as these security measures are not perfectly substitutional. Due to time and travel constraints for this project, specific discussions with TSA PreCheck officials have not been possible at this point. However, the principal investigators have attended many meetings and discussions with airport and airline security managers and officials in the US, Canada, Australia, and Europe. We are aware of many of the issues, and PI Stewart has been involved as an expert consultant to the IATA Checkpoint of the Future (or Smart Security), and the Australian Government Office of the Inspector of Transport Security. The PIs will be attending the First CREATE and TSA Conference on Improving Transportation Security Capabilities: The Next 10 Years at USC on 20-21 July 2015. We would hope that would be an excellent opportunity to engage with TSA on the PreCheck project.

The selection of event probabilities for all layers of security are treated as conditional probabilities, and will include separate estimates for deterrence and disruption rates. Deterrence and disruption rates are uncertain and will be modeled as random variables. The triangular distribution is well suited to probabilistic characterization of these variables. In this case, low, mid and high estimates of deterrence and disruption rates characterize the shape of the triangular distribution (see Table 1). Words of estimative probability are supplied in Table 1 (adapted from Fletcher 2011), and they will then applied to security measures.
At P can be a negative value (cost saving), which of course has a high successful attack. An interesting feature of this framework is that for PreCheck the value if C isn’t in place, Pr(T) is the likelihood a successful terrorist attack and/or the losses sustained in such an attack, C is the cost associated with security measures that lead to a risk reduction as well as opportunity costs, and L is the loss from a successful attack. For illustrative purposes, three loss attributes are considered: L1, L2 and L3 represent low, medium and high consequences, respectively. A simplified event tree of events that lead to losses L_i is given by Figure 1.

The losses from a successful attack on aircraft can be estimated based on statistical analysis of past attacks. For example, losses from a 9/11-type attack where an aircraft is commandeered and crashed into a building may range from $10 billion (Pentagon attack) to over $200 billion (all four attacks). On the other hand, an IED attack where an aircraft is downed by a bomb may result in lower losses than a 9/11-type attack. These losses can be represented probabilistically.

Utility theory provides a means of evaluating the risk preferences of the interested parties under choice uncertainty. The attribute (x) under consideration is monetized costs of security measures and disruption rates (and their uncertainties) through the system representation. The result is the mean utility for cost x expressed as a utility function, u(x) is the utility for cost x expressed as a utility function, the probability or likelihood of attack Pr(T) is the likelihood a successful terrorist attack will take place if the security measure were not in place, Pr(L|T) is the conditional probability of a loss given occurrence of the threat, the reduction in risk (ΔR) is the degree to which security measures reduce the likelihood of a successful terrorist attack and/or the losses sustained in such an attack, C is the cost associated with security measures that lead to a risk reduction as well as opportunity costs, and L is the loss from a successful attack. An interesting feature of this framework is that for PreCheck the value if C can be a negative value (cost saving), which of course has a high utility.
The objective of the decision-making process is to maximize the expected utility, and so an option is preferable if it has a higher utility. Utility is highest ($u=1.0$) when costs and losses are zero, and lowest ($u=0$) when costs are a maximum. A linear utility function is appropriate for decision-makers in governments or large companies that can afford to sustain a loss ($C$) on a 50-50 chance of making a substantial profit ($A$). However, this would not be true among individuals making decisions involving monetary values that are large in relation to their working capital. These decision-makers would only take a gamble if the risk of large loss is small. Such a decision-maker is "risk-averse" and his/her preferences are manifested in a concave utility function. In other words, the individual is prepared to settle for a guaranteed expected loss rather than accept a risk (avoid the gamble) of an even larger loss. Figure 2 shows risk neutral and risk averse utility functions.

Expected utilities are calculated for the PreCheck policy option and for existing measures (business as usual without PreCheck) $E_{BAU}[u]$. A security measure is the preferred policy option if its expected utility exceeds $E_{NO}[u]$. A break-even analysis reveals the minimum attack likelihood for PreCheck to have a 50-50 chance of being the preferred policy option for risk neutral and various levels of risk-averseness utility functions. The Monte-Carlo simulation analysis also allows the minimum attack probability for PreCheck to have a 90%, 95% or 99% be the preferred policy option - this means that the decision-maker has more surety that PreCheck is the preferred option. The analyses will be subject to a full sensitivity analysis.

The decision analysis will serve to illustrate some important aspects of risk preferences for public decision-making. We expect the findings to be robust to changes in parameter values. If public policy makers are to make decisions that might not be supported by a quantitative decision analysis, their degree of risk averseness needs to be quantified and compared with other public policy decisions. This would make the trade-offs more transparent, and highlight the degree to which risk aversion is excessive or justified.
14. Major Milestones, Deliverables and Dates
July – September 2015:
- Meet with TSA to discuss experiences with PreCheck, how resources are deployed to regular screening lanes, and judgments on improvements of effectiveness. Discuss policy options.
- Develop a systems model of all layers of aviation security and their interactions.

October – December 2015:
- Survey select TSA staff to elicit their low, mid and high estimates of deterrent and disruption rates for layers of aviation security.
- Write Preliminary Report of Progress for first 6 months of the project.

January – March 2016:
- Combine survey results for statistically robust deterrent and disruption rates.
- Evaluate PreCheck cost savings and the co-benefits of improved passenger experience.
- Develop a range of utility functions to represent risk preferences of TSA decision-makers.

April – June 2016
- Use systems reliability techniques to compute risk reductions from PreCheck.
- Apply Monte-Carlo simulation risk and cost-benefit analyses, assessing attack probabilities for various levels of surety that the decision is cost-effective.
- Conduct sensitivity analyses.
- Write Final Report.

15. References

17. Brief Bios

Mark G. Stewart is Professor of Civil Engineering and Director of the Centre for Infrastructure Performance and Reliability at The University of Newcastle in Australia, ARC Australian Professorial Fellow, and Senior Fellow, Mershon Center for International Security Studies, Ohio State University.

He is the co-author of *Probabilistic Risk Assessment of Engineering Systems* (Chapman & Hall, 1997) and *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security* (Oxford University Press, 2011), as well as more than 350 technical papers and reports. He has more than 25 years of experience in probabilistic risk and vulnerability assessment of infrastructure and security systems. Stewart has received over $4 million in Australian Research Council (ARC) support in the past 12 years. He has received extensive ARC support to develop probabilistic risk-modelling techniques for infrastructure subject to military and terrorist explosive blasts and cost-benefit assessments of counter-terrorism protective measures for critical infrastructure. In 2011, he received a five-year Australian Professorial Fellowship from the ARC to continue and to extend that work. Mark works closely with the Australian Defence Force, and has a SECRET security clearance.

John Mueller is the Woody Hayes Senior Research Scientist at the Mershon Center for International Security Studies of Ohio State University. He is also adjunct professor of Political Science at Ohio State and a Cato Senior Fellow at the Cato Institute in Washington, DC.

Among his books are *War, Presidents and Public Opinion, Retreat from Doomsday: The Obsolescence of Major War, Atomic Obsession: Nuclear Alarmism from Hiroshima to Al Qaeda, Overblown, War and Ideas: Selected Essays, Terrorism Since 9/11: The American Cases, Capitalism, Democracy, and Ralph's Pretty Good Grocery, The Remnants of War*, and, with Mark Stewart, *Terrorism, Security, and Money*. He has published well over 100 articles in scholarly journals as well as many editorial page columns and articles, is a member of the American Academy of Arts and Sciences, has been a John Simon Guggenheim Fellow, and has received grants from the National Science Foundation and the National Endowment for the Humanities. He has also received several teaching prizes, and in 2009 received the International Studies Association's Susan Strange Award that “recognizes a person whose singular intellect, assertiveness, and insight most challenge conventional wisdom and intellectual and organizational complacency in the international studies community.” In 2010, he received Ohio State University's Distinguished Scholar Award.