

Springer Tracts in Civil Engineering

Mark G. Stewart
David V. Rosowsky *Editors*

Engineering for Extremes

Decision-Making in an Uncertain World



Springer

Mark G. Stewart · David V. Rosowsky
Editors

Engineering for Extremes

Decision-Making in an Uncertain World

Editors

Mark G. Stewart
Centre for Infrastructure Performance
and Reliability
The University of Newcastle
Newcastle, NSW, Australia

David V. Rosowsky
Kansas State University
Manhattan, KS, USA

ISSN 2366-259X

ISSN 2366-2603 (electronic)

Springer Tracts in Civil Engineering

ISBN 978-3-030-85017-3

ISBN 978-3-030-85018-0 (eBook)

<https://doi.org/10.1007/978-3-030-85018-0>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2022

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The community has always been worried by extreme weather events and for good reason. In the era before insurance, the personal and financial loss from a flood, storm, fire, hurricane, or earthquake could wreck livelihoods, destroy homes, shops and workplaces, and lead to widespread poverty and destitution that might take generations to recover from. While these devastating consequences are often avoided in the developed world, they remain a sad reality for much of the world.

It is therefore of no surprise that the civil engineering profession has its roots in improving the resilience of the community to extreme events. The desire to build a flood proof river crossing led to the revolutionary cast-iron Iron Bridge being built in Coalbrookdale in England in 1779 for what in its day was an impressive 30 m span. Within a century, civil engineering had advanced to the point where spans of 500 m or longer were possible—the Brooklyn Bridge linking the communities of Manhattan and Brooklyn in New York City being one notable example.

Despite this progress, significant challenges remain today. Buildings, bridges, roads, nuclear power plants, and other infrastructure essential to our economic and social well-being are at an increasing risk from terrorism, climate change, hurricanes, storms, floods, earthquakes, heat waves, fires, and other extreme events. The timing and severity of these extremes are highly uncertain and are characterised as low probability–high consequence events. Risk and cost–benefit analyses of protective measures aim to reduce the vulnerability of infrastructure and hence reduce the future impact of extreme events to reveal protective measures that are cost effective and those that are not. Relevant also are private and public policy imperatives in the decision-making process.

Extreme events and actions taken to reduce the vulnerability of infrastructure are sometimes based on worst-case thinking, probability and cost neglect, and risk aversion. This can result in a frightened public, costly policy outcomes, and wasteful expenditures.

The book will explain how risk and decision-making analytics can be applied to the wicked problem of protecting infrastructure and society from extreme events. There is increasing research that takes into account the risks associated with the timing and severity of extreme events in engineering to reduce the vulnerability or increasing the

resiliency of infrastructure—we refer to this as ‘*Engineering for Extremes*’. Engineering for extremes is defined as measures taken to reduce the vulnerability or increase the resiliency of built infrastructure to climate change, hurricanes, storms, floods, earthquakes, heat waves, fires, and malevolent and abnormal events that include terrorism, accidental explosion or fire, vehicle impact, and vehicle overload. This may include, for example, enhancement of design standards (higher design loads or flood levels), retrofitting or strengthening of existing structures, utilisation of new materials, and changes to inspection and maintenance regimes.

The book will introduce the key concepts needed to assess the economic and social well-being risks, costs, and benefits of infrastructure to extreme events. This will include hazard modelling (likelihood and severity), infrastructure vulnerability, resilience or exposure (likelihood and extent of damage), social and economic loss models, risk reduction from protective measures, and decision theory (cost–benefit and utility analyses). This will be followed by case studies authored by experts from Australia, USA, Canada, UK, Ireland, France, New Zealand, China, Japan, South Africa, and South America. These case studies will describe succinctly the practical aspects of risk assessment when deciding on the most cost-efficient measures to reduce infrastructure vulnerability to extreme events for housing, buildings, bridges, roads, tunnels, pipelines, and electricity infrastructure in the developed and developing worlds.

The editors have been colleagues and close friends for nearly 30 years. One introduced the other to a lifetime addiction to Dunkin Donuts and the other to the delights of an Aussie favourite—Tim Tams. This book became our COVID project. It was also an excuse to reach out to our friends and colleagues around the globe. Their response to our book proposal was warm and generous. All the more so as, we were all battling the personal trauma and professional disruptions wreaked by COVID-19. In these trying times, their support was something we will not easily forget.

So we are incredibly grateful to the authors of the chapters. The authors shared our enthusiasm for the book and, more importantly, devoted much time and energy to producing chapters that are at the forefront of the latest developments, are engaging to a non-specialist reader, and provide a focus on practical decision outcomes. The chapters reflect the expertise of the authors and the latest developments on engineering for extremes.

Finally, we appreciate the support from the folks at Springer in bringing this book to fruition.

Newcastle, Australia
Kansas, USA
May 2021

Mark G. Stewart
David V. Rosowsky

Contents

Part I Introduction

- 1 Extreme Events for Infrastructure: Uncertainty and Risk** 3
Mark G. Stewart and David V. Rosowsky

Part II Decision-Making

- 2 Risks and Compromises: Principled Compromises
in Managing Societal Risks of Extreme Events** 31
Paolo Gardoni and Colleen Murphy
- 3 Risk-Informed Approaches for Mitigating Impacts of Extreme
and Abnormal Events in the Built Environment** 45
Bruce R. Ellingwood

Part III Case Studies

- 4 Aviation Resilience to Terrorist Hijackings** 69
Mark G. Stewart and John Mueller
- 5 Challenges of Effective Blast Protection of Buildings** 93
Hong Hao and Xihong Zhang
- 6 Adaptation of Housing to Climate Change and Extreme
Windstorms** 119
Hao Qin and Mark G. Stewart
- 7 Risk-Based Management of Electric Power Distribution
Systems Subjected to Hurricane and Tornado Hazards** 143
Yue Li, Abdullahi M. Salman, Abdullah Braik, Sirrý Bjarnadóttir,
and Babak Salarieh
- 8 Hurricane Fragility Assessment of Power Transmission
Towers for a New Set of Performance-Based Limit States** 167
Yousef M. Darestani, Ashkan B. Jeddi, and Abdollah Shafieezadeh

9	Building Adaptation to Extreme Heatwaves	189
	Dileep Kumar, Morshed Alam, and Jay Sanjayan	
10	Improving Regional Infrastructure Resilience to Earthquakes, Storms and Tsunami	217
	David Elms, Ian McCahon, and Rob Dewhurst	
11	Earthquake-Tsunami Risk Assessment and Critical Multi-hazard Loss Scenarios: A Case Study in Japan Under the Nankai-Tonankai Mega-Thrust	235
	Katsuichiro Goda, Raffaele De Risi, Flavia De Luca, Ario Muhammad, Tomohiro Yasuda, and Nobuhito Mori	
12	Building Resilience in Changing Cryosphere Services	255
	Bo Su, Xiaoming Wang, Cunde Xiao, Jinglin Zhang, and Bin Ma	
13	Extreme Vehicles and Bridge Safety	271
	Colin Caprani and Mayer Melhem	
14	Fire Safety in Road Tunnels	293
	T. D. Gerard Canisius, Dimitris Diamantidis, and Suresh Kumar	
15	Cost-Benefit Analysis of Design for Progressive Collapse Under Accidental or Malevolent Extreme Events	313
	André Teófilo Beck, Lucas da Rosa Ribeiro, and Marcos Valdebenito	
16	Durability and Performance of Wind Turbines Under Climate Extremes	335
	Rui Teixeira, Alan O'Connor, and Dimitri V. Val	
17	Extreme Value Analysis for Offshore Pipeline Risk Estimation	355
	Robert E. Melchers	
18	Reliability Assessment of Corroded Pipelines Subjected to Seismic Activity	373
	Rafael Amaya-Gómez, Mauricio Sánchez-Silva, and Emilio Bastidas-Arteaga	
19	Climate Change Impact for Bridges Subject to Flooding	393
	Boulent Imam	
20	Bushfire and Climate Change Risks to Electricity Transmission Networks	413
	Chi-Hsiang Wang	
21	Provisions for Climate Change in Structural Design Standards	429
	Johan Retief and Celeste Viljoen	

Part IV Conclusions and Recommendations

22	Conclusions for Engineers and Policy Makers	449
	David V. Rosowsky and Mark G. Stewart	

About the Editors

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. Professor Stewart is an international leader in risk assessment, public policy decision-making, and protective infrastructure for extreme hazards. He is Author of *Probabilistic Risk Assessment of Engineering Systems* (Chapman & Hall 1997), *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security* (Oxford University Press 2011), *Chasing Ghosts: The Policing of Terrorism* (Oxford University Press 2016), *Are We Safe Enough? Measuring and Assessing Aviation Security* (Elsevier 2018), an edited book *Climate Adaptation Engineering: Risks and Economics for Infrastructure Decision-making* (Elsevier 2019), as well as more than 500 technical papers and reports. He has more than 30 years of experience in probabilistic risk and vulnerability assessment of infrastructure and security systems that are subject to man-made and natural hazards. He has attracted more than \$10 million in research funding. In the past decade, Stewart has led the way in risk-based assessment of terrorism and climate change impacts on engineering infrastructure with 25 keynotes at international conferences. He is Editor-in-Chief of *Structural Safety* and Fellow of the Australian Academy of Technology and Engineering.

David V. Rosowsky is Vice President for Research at Kansas State University where he also holds the title of Professor of Civil Engineering. Prior to joining K-State, he served for six years as Provost and Senior Vice President and Provost at University of Vermont. Prior to that, he served as Dean of Engineering at Rensselaer Polytechnic Institute and before that as Head of the Zachry Department of Civil Engineering at Texas A&M University where he also held the A.P. and Florence Wiley Chair in Civil Engineering. He also previously held Richardson Chair in Wood Engineering and Mechanics at Oregon State University and was Faculty Member at Clemson University. Since 1990, he has conducted research in the areas of structural reliability, performance of wood structural systems, design for natural hazards, stochastic modelling of structural and environmental loads, and probability-based codified design. His current research addresses three topics: (1) behaviour of the built

environment subject to natural hazards, most recently including the effects of climate change and adaptation, (2) modelling and analysis of load effects on buildings and other structures with particular emphasis on complex environmental phenomena, and (3) performance-based engineering for design, post-disaster condition assessment, and loss estimation studies. He has authored or co-authored more than 300 technical papers. A recognised expert in the field of structural reliability, he has been invited to present his research work around the world including invited lecturers in France, Italy, Switzerland, Canada, Japan, Australia, and New Zealand. He has supervised more than 20 masters and doctoral students. He is Recipient of the ASCE Walter L. Huber Research Prize, the T. K. Hseih Award from the Institution of Civil Engineers (UK), and the ASCE Norman Medal.

Chapter 4

Aviation Resilience to Terrorist Hijackings



Mark G. Stewart and John Mueller

Abstract Approximately \$50 billion is spent annually world-wide in the quest to deter or disrupt terrorist attacks to aviation, significant expenditures that have rarely been subject to systematic cost–benefit or risk analysis. This chapter applies that approach, assessing the risks, costs, and benefits of security measures designed to disrupt terrorist hijackings of airliners assuming terrorists arrive at the airport undeterred and undetected. Under those conditions, existing security measures reduce the risk of a terrorist success by over 88%. Another security measure could be added to the existing array: secondary flight deck barriers, lightweight devices that are easy to deploy and stow, installed between the passenger cabin and the cockpit door to block access to the flight deck whenever the cockpit door is opened in flight. These barriers are highly cost-effective and raise total risk reduction to over 96%. The benefit-to-cost ratio of the measure is high at 5.1, and it remains cost effective even if risk reduction is halved and costs are doubled. On the other hand the expensive Federal Air Marshal Service fails a cost–benefit analysis, whereas the Federal Flight Deck Officer program proves to be cost-effective.

Keywords Aviation security · Terrorism · Risk · Cost–benefit analysis · Transportation security administration · Risk reduction · Airline bombing

M. G. Stewart (✉)

Centre for Infrastructure Performance and Reliability, The University of Newcastle, Newcastle, Australia

e-mail: mark.stewart@newcastle.edu.au

J. Mueller

Mershon Center for International Security Studies, Department of Political Science, Ohio State University, 1501 Neil Avenue, Columbus, OH 43201, USA

Cato Institute, 1000 Massachusetts Avenue, Washington, DC, NW 20001, USA

4.1 Introduction

The attacks of September 11, 2001, by far the most destructive in history, highlighted the vulnerability of airliners and infrastructure to terrorism. The attack directly resulted in the deaths of nearly 3000 people. Following the widely-applied value of statistical life (VSL) approach, the best estimate for homeland security analysis is about \$8 million in 2020 dollars [1]. Using that leads to a direct loss of approximately \$25 billion arising from nearly 3000 fatalities. In addition 9/11 caused approximately \$35 billion in physical damage including rescue and clean-up costs. Indirect costs were even more substantial. Thus, the International Monetary Fund and others estimate that the 9/11 attacks cost the US economy up to 1% in lost GDP (\$200 billion in 2020 dollars) in that year alone. An upper bound estimate of the losses of 9/11, then, might exceed \$250 billion [2].

Thus, the protection of airliners seems to be particularly important because the downing of one does seem to carry with it the special dangers of a widespread and at least somewhat lingering impact on the airline industry, as well as on related ones such as tourism. Particularly in the few years after 2001, it was commonly said that if terrorists were able to down two or three more airliners, they would destroy the airline industry, and an attack on aviation is considered by some to be the “gold standard” for terrorists.

However, contrary to anticipations, there have been few terrorist attempts on airliners since 9/11 anywhere in the world, even though security measures in many places are considerably more lax than in the United States. Indeed, averaged over the past 44 years, the chance worldwide that an individual airline passenger will be killed by terrorists on an individual flight is 1 in 25 million, while for the post-9/11 period the odds are 1 in 110 million [3].

Approximately \$50 billion—about \$10 billion in the United States—is spent annually world-wide in the quest to deter or disrupt terrorist attacks to aviation [3]. But these significant expenditures have rarely been subject to systematic cost–benefit or risk analysis, and this lack of scrutiny may lead to risk-averse and costly counterterrorism policies.

This chapter assesses the degree to which security measures currently in place provide safety. In particular, it focuses on determining the likelihood under current conditions that a 9/11-like attempt by terrorists to hijack an airliner in the United States, commandeer it, and fly it into a pre-designated target could succeed. Another aim is to assess the cost-effectiveness of security measures by evaluating the risk reduction of each and its cost, as well as the losses from a successful terrorist attack, and the probability that there will be a terrorist attack.

Previous research has compared the costs and benefits of some aviation security measures, and recommended where savings can be made without unduly sacrificing risk reduction as in [2, 4]. This work was then considerably extended by applying utility theory to quantify levels of risk aversion finding that a very risk averse decision-maker is 48% likely to prefer to retain the expensive FAMS program even if the attack probability is as low as 1% per year—a very high level of risk aversion that

is exhibited by few, if any, other government agencies [5, 6]. Stewart and Mueller [7] then conducted a risk analysis that a terrorist organisation could down an airliner with a passenger-borne bomb or IED—an improvised explosive device. The cost–benefit assessment found that efficiencies in checkpoint screening are needed for this layer to be deemed cost-effective. A systems reliability analysis and a cost–benefit assessment of Advanced Imaging Technologies (AIT) full-body scanners found the technology to be a questionable expense [8]. Later studies have also assessed the risks and cost-effectiveness of Transportation Security Administration (TSA) PreCheck, airport policing, measures to protect airport terminals, and the counter-terrorism efforts of the Federal Bureau of Investigation [9–13].

There is other research that looks at the risks and efficiencies of aviation security.¹ Few of these studies, however, estimate absolute risk and risk reduction. A key component of assessing absolute risk is to include the probability of an attack in the calculations. A relative risk assessment, in contrast, is often conducted conditional on an attack occurring and then ranking risks based on the relative likelihood of threats.

A potential security measure is a *secondary flight deck barrier* (Installed Physical Secondary Barrier or IPSB). This is a lightweight device that is easy to deploy, installed between the passenger cabin and the cockpit door that blocks access to the flight deck whenever the reinforced door is opened in flight for rest breaks, meals, etc. (see Fig. 4.1). It will reduce the vulnerability of another 9/11 type attack. In 2018 the United States Congress reauthorized the Federal Aviation Administration (FAA) that included a mandate that the FAA issue a rule by 5 October 2019 to require the installation of secondary flight deck barriers on all new passenger aircraft. However, the FAA is now studying the requirement and has yet to issue a final rule on this legislation. Hence, the life saving and risk reducing potential of secondary flight deck barrier and its cost-effectiveness is assessed in this chapter.

The system reliability model used in this chapter is taken from our latest book [3]. However, this chapter extends that work by considering risks from hijacking that are not deterred in the first place. Some of the numerical estimates will differ from those listed in the book due to updated information and to feedback from the book [15].

Throughout, costs and benefits are taken as mean values—that is, as single-point or deterministic values. An advantage of this is that the calculations are straightforward. They can also be readily replicated and checked by others. However, this simplified approach ignores the uncertainties and variabilities in the parameter estimates—and uncertainties in the realm of terrorist intentions and predictions are large. Stewart and Mueller [6, 8] have used Monte Carlo simulation methods to propagate vulnerability, risk reduction, and loss uncertainties in the calculation of net benefits. However, results from a probabilistic analysis shows similar trends to those obtained from a deterministic analysis.

¹ For a full review of probabilistic terrorism risk assessment see Stewart and Mueller [16].

Fig. 4.1 Secondary Flight Deck Barrier (Installed Physical Secondary Barrier or IPSB) [14]



4.2 The Risk Framework

The standard definition of risk used by the Department of Homeland Security is:

$$(\text{Risk}) = (\text{Threat}) \times (\text{Vulnerability}) \times (\text{Consequence}) \quad (4.1)$$

Threat:

- A 9/11-like attempt by terrorists to hijack an airliner in the United States, commandeer it, and flying it into a pre-designated target.
- We assume that the terrorists arrive at the airport undeterred and undetected.

Vulnerability:

- Probability that the attack will be disrupted at the airport or on the airliner.

Consequences:

- Economic and human losses, direct, indirect and social, from a successful hijacking attack.

To determine the benefit-to-cost ratio for a security layer the *benefit* is calculated as:

Benefit of a security measure

$$\begin{aligned}
&= \text{probability of a successful attack} \\
&\times \text{losses sustained in the successful attack} \\
&\times \text{reduction in vulnerability (risk reduction)} \\
&\text{furnished by the security measure} \quad (4.2)
\end{aligned}$$

This *benefit* is then divided by the *cost* of the security measure to generate an easy to understand decision-making metric—the benefit-to-cost ratio (BCR).

4.3 Vulnerability and Reliability Analysis of the Existing Layers of Security Against a Hijacking

The TSA has arrayed 21 “Layers of Security” to “strengthen security through a layered approach” (see Fig. 4.2).

Rates of deterrence are more difficult to quantify than disruption rates because the former depends more on the motivation and adaptive capability of the terrorist. And deterrence rates also depend on the ability of a terrorist to game the system. Our approach is to consider those terrorists who arrive at the airport undeterred and undetected. In this case, the deterrence rates for all layers are set at zero, and disruption rates are set to zero for the first four layers on TSA’s list: intelligence, international partnerships, customs and border protection, and Joint Terrorism Task Force. Also ignored are several layers that play little or no role in a hijacking consideration: crew vetting, VIPR, canines, checked baggage, random employee screening, and bomb appraisal officers. In our analysis, we thus include ten of the TSA’s security layers and add two more for the post-hijacking stage.

The effectiveness at disrupting a terrorist effort is estimated for each of these 12 layers. Since there is little quantitative data on disruption rates, it is more tractable to assign words of estimative probability such as “probably not” and “chances about even” as in Table 4.1, and to translate them into probabilities.

Many of the disruption rates are taken from previous studies [3, 6, 8, 13, 16]. The results of this examination are summarised in Table 4.2 and the overall model of the system is shown in Fig. 4.3.

4.3.1 Pre-boarding Security Layers

1. *No-fly list and passenger pre-screening*
 2. *Behavior Detection Officers (BDOs)*
 3. *Travel document checkers*
 4. *Checkpoint screening with Transportation Security Officers (TSOs).*
- The disruption rates for the pre-boarding layers are mostly modest, with the most effective being the passenger screening at the TSA checkpoints.

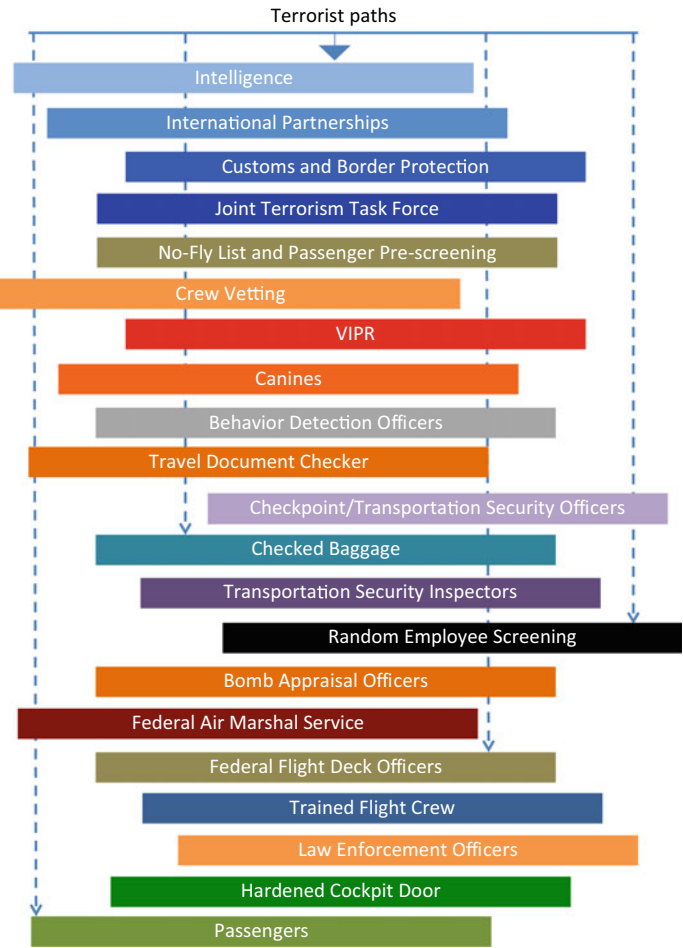


Fig. 4.2 TSA’s 21 Layers of security. *Source* Transportation Security Administration

Table 4.1 Words of estimative probability

Certain	100%
Almost certain	95%
Highly probable	85%
Probable	75%
Chances about even	50%
Less likely than not	40%
Probably not	25%
Highly improbable	15%
Almost certainly not	5%
Impossible	0%

Table 4.2 Disruption rates for existing aviation security measures, for a hijacking attack

	Disruption rate
Pre-boarding Security:	
1. No-fly list & passenger pre-screening	5%
2. Behavior Detection Officers	1%
3. Travel document checkers	5%
4. Checkpoint/TSOs	15%
In Flight Security:	
5. Passenger resistance	15%
6. Cabin crew resistance	15%
7. Law enforcement officer	1%
8. Federal Air Marshal Service (FAMS)	NA
Probability that air marshals are on-board: 20%	
9. Hardened cockpit door	
FAMS on board	75%
No FAMS on board	50%
10. Flight deck resistance and FFDOs	40%
11. Unable to fly airliner into target	5%
12. Anti-aircraft measures	15%

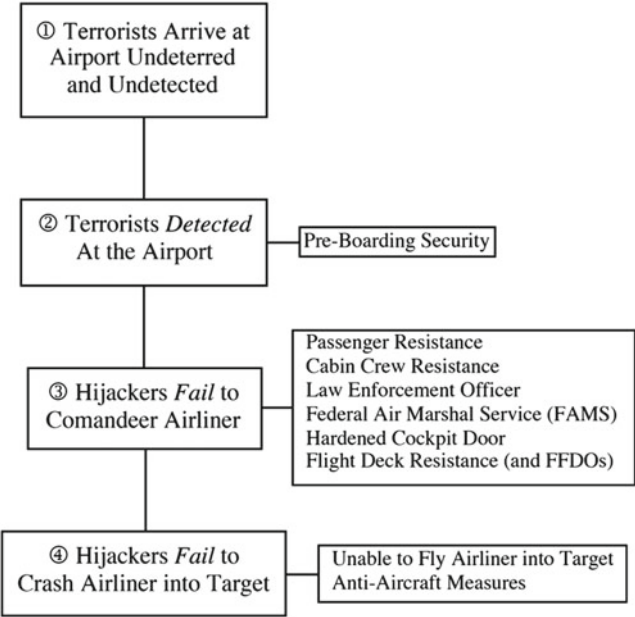


Fig. 4.3 System model of existing aviation security measures

4.3.2 *In-Flight Security Layers*

5 and 6. *Passenger and cabin crew resistance*

As pilot Patrick Smith points out, what the 9/11 attacks “actually exploited was a weakness in our mindset—a set of presumptions based on the decades-long track record of hijackings. In years past, a takeover meant hostage negotiations and standoffs; crews were trained in the concept of ‘passive resistance’” [17].

This policy was obviously shattered by the 2001 hijackings as was demonstrated on the fourth plane in which passengers and crew, having learned of what had happened on the three earlier flights, fought to overcome the hijackers and were successful in that they were able to prevent the terrorists from flying the plane into its intended target. That is, any terrorists seeking to actually commandeer the aircraft would face not only a considerable number of security measures designed to counter such a threat, but “a planeload of angry and frightened people ready to fight back” [17].

Nonetheless, there have been a number of airliner hijackings by passengers since 2001, although none of them took place in the United States and none have involved a concerted effort to commandeer the plane.

Bruce Schneier concludes that passenger resistance combined with secure cockpit doors is likely to be enough, by itself, to disrupt a hijacking attempt, while Smith suggests that crew and passenger resistance alone is likely to do the trick [17, 18].

Others disagree, Captain Tom Walsh rates it as “unlikely” that “passengers will come to the rescue of crew members and fighting back against attackers” [19]. Most reported incidents of fighting back have occurred when the terrorist was acting alone, not the coordinated resistance needed to overwhelm a team of hijackers spread throughout an aircraft—and a team of hijackers is what would be required for a 9/11 type of attack to be repeated. The time it takes for hijackers to take over an aircraft could be a matter of seconds, which could conceivably be less than passengers need to assess the situation, realize the dire threat, communicate with other passengers, and process other information needed for them to summon the courage to assault armed and dangerous terrorists. Moreover, there is little formal training of cabin crew in effective techniques to fight back.

With this in mind, we estimate that for the passenger resistance layer, the rate of disruption is 15% and that the rate of disruption for the cabin crew is also 15%.

7. *Law enforcement officers on board*

Law enforcement officers are on some flights for reasons other than countering terrorism, such as escorting prisoners or protecting VIPs. However, their numbers are small and their impact on security is also likely to be low. Largely because of the low likelihood of one being on an individual flight, we estimate that the layer reduces the risk of a successful hijacking by only 1%.

8. *The Federal Air Marshal Service (FAMS)*

There are now some 3000–4000 air marshals [20, 21]. It has been estimated that air marshals ride on less than 5% of flights in the United States [21]. Although these are deemed to be high-risk flights based on intelligence reports, it is unclear exactly how that risk has been determined—after all, since 9/11, no airline flight in the U.S. has had an active terrorist on board.

It might be argued that some crew and passengers may be reluctant to be the first to confront a hijacker if they believe an air marshal is on board, a hesitation that could conceivably give hijackers the time they need to execute their plans. On the positive side, air marshals may provide more flexibility than many other security measures because they can be deployed at short notice for emerging threats.

Although FAMS are on no more than 5% of flights, they are not placed randomly but rather on flights deemed to be ‘high risk.’ Consequently, and perhaps rather generously, we assume a high 20% effective coverage.

9. *Hardened cockpit door*

While the effectiveness of the hardened cockpit door in restricting cockpit access to a determined hijacker has sometimes been questioned [19], there is little doubt that they will have an impact on the likelihood that a hijacking will succeed.

We assume that the hardened cockpit door will be attacked during a time of its opening and closing—i.e., when it is most vulnerable. In this case, the odds that the attack will be disrupted by the door is “about even” or 50%. While there is a vulnerability, an attack would only succeed if the terrorist(s) could launch their attack at precisely the right moment to exploit what is a momentary vulnerability during a door transition. As the presence of air marshals near the cockpit door is likely to complicate a terrorist attempt, a door’s disruption rate increases in that case to 75%.

However, if attackers are somehow able to get into the flight deck, the doors could be used to protect them. Something like this happened in deliberate crashes on a Germanwings flight in 2015 and on a LAM Mozambique Airlines flight in 2013—neither of them terrorist events.

10. *Flight Deck Resistance Enhanced by the Federal Flight Deck Officer (FFDO) Program*

An invasion of the cockpit by terrorists determined to take over the controls would, in the aftermath of 9/11, be met with determined resistance by the flight crew.

The cockpit is a small place and, unlike any hijackers, the flight crew knows every square inch of it. In addition, they have, of necessity, access to tools, some of which can be used as weapons of defence like screwdrivers, hammers, chisels, hatchets, and they are likely to know exactly where each of these is. Added to this are less lethal defensive measures. For example, there was an attempt in 1994 to hijack and crash a FEDEX cargo flight by an employee of the company flying as a passenger. Even though both pilots and the flight engineer suffered head blows from a hammer

during a violent struggle in the cockpit, they successfully restrained the hijacker and landed the aircraft safely [22].

As an enhancement, TSA instituted the Federal Flight Deck Officer (FFDO) program in which flight crew members are trained and armed with firearms to be able to defend the cockpit from intruders. This program, not FAMS, provides the “last line of defense” against a hijacking, and it has dramatically increased in size since its inception in 2003 [23]. It is estimated that up to 20% of pilots in the United States are FFDOs [21]. (Data on the number of FFDOs is classified). It seems reasonable to assume that if FFDOs are present on the flight deck, they are likely to be as effective as any air marshals who happen to be on board.

If FFDOs are in the cockpit, we suggest they are likely to be highly effective in foiling a hijacking. If the probability that FFDOs are on a plane is 15–20%, we estimate that the FFDO program, when combined with flight deck resistance more generally, reduces the risk of a successful hijacking by 40%—i.e., their ability to foil a hijacking is “less likely than not”.

4.3.3 *Post-Hijacking Security Layers*

11. *Terrorists are unable to fly the airliner into the target*

Piloting a large commercial airliner is difficult and so perhaps is the challenge confronting a hijacker trying to steer an airliner to a pre-designated target on the ground. Assuming that a hijacker has the time, resources, and ability to learn to pilot large aircraft, the odds of successfully striking a ground target will be high, as evidenced by the attacks on the World Trade Center and Pentagon. Of course, if an aircraft misses its intended target when it crashes into the ground, it can still do damage, though probably not as much as might be imagined.

We estimate that the difficulty for terrorists to fly the airliner into their intended target or to inadvertently hit a mass casualty target reduces the risk of a successful hijacking by 5%.

12. *Anti-aircraft measures*

If a pilot is able to transmit to air controllers that the plane is under a violent hijacking attempt (or if passengers or cabin crew members can use their phones to warn authorities), anti-aircraft measures might immediately be deployed to shoot down or ground the captured airliner before it can reach an intended target.

Despite these efforts, Associated Press report that “U.S. military officials have concluded it would be very difficult to intercept a hijacked plane within a certain radius of major cities like Washington unless fighter jets were already airborne”. Surface-to-air missiles have been deployed around Washington DC, but these are a “measure of last resort for protecting a limited number of key locations against an aerial attack” [21]. The 9/11 hijackers were able to disable the aircraft’s transponders,

making the detection of the aircraft the more difficult, but not impossible as the aircraft were still tracked by ground-based radar [21].

We estimate that the anti-aircraft layer reduces the risk of a successful hijacking by 15%.

4.4 Adding a Security Layer: Installed Physical Secondary Barriers

An additional security measure to disrupt airline hijackers is a *secondary flight deck barrier* (Installed Physical Secondary Barrier or IPSB). The installation of this security barrier has been supported by the Airline Pilots Association (ALPA) because, “the reinforced flight deck door, together with supplementary crew procedures, does not provide a complete solution for securing the flight deck” [24].

One analysis examines a hijacking scenario positing “a team of highly trained, armed, athletic individuals” who might, in a matter of seconds, be able to take over the flight deck during a door transition. Under those circumstances, passengers and crew would scarcely have time to assess the situation, realize the dire threat, communicate with other passengers, and process the information needed for them to summon the courage to fight back. Accordingly, it concludes that “passengers are not considered a predictably reliable option for preventing an attempted violent or sudden breach of the flight deck,” and it completely excludes “the possibility of passenger intervention as a mitigating measure” from its consideration. Although flight attendants receive little or no training in the use of force, many airlines have instituted procedures during door transition, such as galley trolleys to block access to the flight deck. The study found, however, that this did “not produce satisfactory results” [25].

An IPSB could deal with this concern. Further security is provided by the fact that a cabin crew member is generally required to be at the scene when the secondary barrier is put into place, something that adds a complication for would-be hijackers.

The cost of an IPSB for a new aircraft has been estimated to be less than \$10,000 [21], with some estimates as low as \$3500 [26]. However, more recent cost data obtained by the Aviation Rulemaking Advisory Committee [27] suggest that the production cost is significantly higher at \$35,000 per aircraft. Added to this are design, testing and certification costs (\$9 million one-time), flight attendant and pilot training costs (60 min initial, 30 min recurrent), maintenance (up to \$700), supply chain/spares (\$10,000 per unit), added fuel burn due to additional weight of an IPSB, and time out of service (delay cost is \$4800 per hour). FAA [27] does not provide a definitive total cost estimate. However, as a starting point we assume that the one-off costs over the life of the aircraft are approximately \$45,000. Since there are approximately 6000 commercial aircraft in the United States, and if we take the \$45,000 estimate, this equates to \$270 million. If we annualize this cost over the 25 year design life of an aircraft with a 7% discount rate, this equates to a cost of \$23.2 million per year for the entire U.S. commercial airline fleet. If we then add

in annual costs (training, maintenance, etc.) of approximately \$2500 per aircraft per year, this equates to a cost of \$15 million per year. Total cost is then rounded up to \$40 million per year for the entire U.S. commercial airline fleet.

The IPSB layer (excluding the effects of a hardened cockpit door or FAMS) will have a high disruption rate if deployed properly. However, this may not always be the case, so we consider an IPSB to be “probably” effective leading to a disruption rate of 75%. If the IPSB is foiled, the hardened cockpit door is still a potential obstacle to a hijacking. The disruption rate for the door is reduced from 75 to 65% if an air marshal is on a flight, which is further reduced to 40% in the absence of FAMS. In this case, the failure of one layer of security (IPSB) affects the effectiveness of another layer (hardened cockpit door). Similarly, the presence of an IPSB may mean that the flight crew are less careful during door transitions, so if the IPSB is foiled by a hijacker, there is less opportunity for flight or cabin crew to close the hardened cockpit door in time, hence we assume a reduced rate of disruption for the hardened cockpit door. The risk reduction from an IPSB, hardened cockpit door and FAMS is calculated as 86%, and in the absence of an IPSB the risk reduction drops to 55%.

Thus, we add IPSB to the existing array of security measures as listed in Table 4.2, estimating its disruption rate to be 75%. And we add a further consideration: If IPSB fails, the risk reduction rate for hardened cockpit doors declines to 65% if FAMS is on board and to 40% if it is not.

4.5 Calculations of Reduction in Vulnerability

We apply a reliability analysis to the system. The probability that a hijacking attempt will be disrupted (that is, the degree to which the risk of a hijacking attack has been reduced by the security layers) is

$$R_{hijacking} = 1 - \left\{ \begin{array}{l} [1 - Pr(\text{disrupted by pre - boarding measures})] \\ \times [1 - Pr(\text{disrupted by in - flight measures})] \\ \times [1 - Pr(\text{unable to fly airliner into target})] \\ \times [1 - Pr(\text{disrupted by anti - aircraft measures})] \end{array} \right\} \quad (4.3)$$

where the term $Pr()$ represents a probability, such that, for example, $Pr(\text{disrupted by pre-boarding measures})$ is the probability that pre-boarding security measures will disrupt, foil or prevent a terrorist attack.

The elements behind the probabilities shown in Eq. (4.3) are arrayed in full detail in Appendix A. An example shows the benefits of multiple layers of security: if each of the four probabilities in Eq. (4.3) is 25%, the risk reduction (or reduction in vulnerability) is a high $R = 68.4\%$ (this is equal to $1 - (1 - 0.25)^4$). If other layers

of security are added to the array, this risk reduction will increase, but the additional risk reduction of each layer will become progressively smaller.

Applying the data from Table 4.2, the probability that a hijacking attempt by a well-organised and undeterred terrorist organisation will be disrupted by existing security measures is 88.2%. This represents the existing level of protection. This suggests that, because of existing security measures, even a well planned and executed terrorist hijacking attempt has perhaps at best one chance in ten of being successful. If the rates of deterrence are estimated using a similar procedure and then added in for all layers, vulnerability is reduced by over 99%. A similar analysis for bombing attacks reveals an overall risk reduction of over 98% (for more details see [3]).

That the risk is low is borne out by the data—there have been no successful terrorist attacks on US airliners since 2001, and, as noted earlier, a statistical analysis of the Global Terrorism Database shows that the probability that an airline passenger will be killed in a single flight in a terrorist attack world-wide is 1 in 110 million for the years since 2001 [3].

Table 4.3 shows that if IPSBs are installed on all aircraft, the probability that a hijacking attempt will be disrupted increases to 96.4%—i.e., the additional risk reduction furnished by IPSBs is $96.4 - 88.2 = 8.2\%$.² This is an impressive reduction in vulnerability from a security measure that will only cost about \$40 million per year.

The analysis does not directly include one important impediment to a successful hijacking attack: the general incompetence and poor tradecraft of most terrorists, particularly in complicated plots [10, 28–32]. As Brian Jenkins [33] puts it, “their numbers remain small, their determination limp, and their competence poor.” Some of the disruption rates presented in the analysis do in part take terrorist inadequacies into account in that a high rate of disruption implies less than perfect terrorist competence and tradecraft.

Table 4.3 Risk reductions in the United States

	Reduction in vulnerability (%)
Existing security layers	88.2
Existing security layers with the addition of IPSBs	96.4
Reduction in risk due to IPSBs	8.2

² Note that some results are rounded so as not to imply a precision higher than the precision of input detection rates and costs.

4.5.1 Substitution Effects and Adaptive Behaviour by Terrorists

As noted, the analysis has assumed that disruption rates are statistically independent. This assumption may not hold in every instance [6, 16]. Thus, security measures may not be perfectly substitutional: removing one layer of security may alter the systems model and/or detection rates of other layers of security. For example, if passengers or crew know there is an air marshal aboard, they may be less willing to jump a would-be hijacker. However, for the most part it seems correct to assume that the layers are statistically independent. Checkpoint screening effectiveness, for example, is not influenced by whether FAMS are on-board. Canines do not care whether there is an air marshal aboard. Do TSOs work less hard because there are BDOs around?

If it is believed that complete independence may not be strictly correct for some layers, the sensitivity analysis suggests that disruption rates can be doubled or halved with little effect on overall risk reduction. This high level of robustness strongly suggests that substitution and/or independence issues wouldn't make much difference even insofar as they may be valid.

It is also important to recognise that some terrorists may exhibit adaptive behaviour. Jackson and LaTourrette [34] have developed a set of adaptation strategies: substitute target or location, substitute tactic or attack mode, hide from or deceive defence, avoid defence at the target, attack defence directly, and absorb defence effects. Adaptive behaviour is inherently difficult to model in a risk analysis, but scenario-based analyses can be enlightening by considering changes such behaviour might make in rates of disruption. Duping someone into unwittingly boarding an aircraft with a bomb concealed in their carry-on luggage is one way to avoid detection from intelligence services, no-fly lists, JTTF, FBI or police. However, Stewart and Mueller [3] show that the overall risk reduction for a passenger-borne bombing declines by about 5% for this scenario. The insider threat is another example of adaptive behaviour. Overall, the results suggest that it is difficult to imagine a scenario in which an adaptive terrorist working with an organisation is likely to be able to dramatically alter the odds of pulling off a passenger-borne bombing or hijacking attack.

4.5.2 Comparisons with Other Countries

The aviation security layers in Europe, Canada, and Australia are very similar to those in the United States. Although the nomenclature may vary, the intent remains the same. For example, the JTTF is unique to the United States, but the concept of coordination between security services, police, airports, and airlines is not.

However, many European Union countries have fewer air marshals on flights, or even none at all, and they do not require the removal of shoes at the screening checkpoint. The sensitivity analysis in the American case shows that, if the likelihood

that air marshals are on board is reduced from 20 to 5%, the overall risk reductions are essentially unchanged. Thus, risk reductions estimated for the United States are most likely to apply as well to other Western countries, including Australia.

It is often argued that Israel has the most effective aviation security. All passengers are interviewed by Israeli security officials, air marshals are on every flight, secondary barriers to the cockpit (or double doors) are fitted to all aircraft, and each is equipped with anti-missile defences [21]. When Richard Reid, the December 2001 shoe bomber, flew on El Al in the summer of 2001, Israeli security “didn’t like the look of him, so they checked everything in his bags, and everything he was wearing, and then put an armed sky marshal in the seat right next to him” [35]. While Reid was not carrying a bomb at the time, it could be argued that Israeli authorities were perceptive enough to recognise a potential threat and deal with it appropriately. In 1986, a six months pregnant Irish woman was interviewed by Israeli security officials at London’s Heathrow Airport before her planned El Al flight to Tel Aviv. The interview was “inconclusive,” so officials searched her bags, discovering a bomb hidden in the lining of her luggage [22]. The bag had been given to her by her Jordanian fiancé. This, and other examples, may attest to the effectiveness of the interview process—there has been no successful attack on an El Al airliner in nearly 50 years, which is, as [21] observes, “a somewhat remarkable feat given terrorist animosities toward Israel.”

The Israeli approach comes at a considerable cost, however. TSA Administrator John Pistole estimates that Israel spends “about 10 times as much as we spend here in the U.S. per passenger” [36]. To duplicate the Israeli approach in the United States would roughly require boosting U.S. government and private spending on aviation security from its current level of \$10 billion per year to \$100 billion per year. It is highly doubtful that such a spending increase is a worthwhile investment if it reduces risk only by an additional 3–5%. The laws of diminishing returns applies—the first dollars spent on counterterrorism measures are likely to be more worthwhile than the last ones.

4.5.3 Security Measures in Place in the US Before 2001

A key value of our reliability model of the overall system of aviation security is that risk reductions can be estimated when some layers of security are removed or have reduced effectiveness. This allows for an evaluation that compares aviation security measures for the 1973–2001 period with those currently in place.

To establish a match, we make the following adjustments to the model:

- Since the ability to trace weapons at the checkpoint was lower because detection technologies were less advanced, we reduce disruption rates for this layer by half.
- We reduce disruption rates for resistance by passengers and crew to zero percent because the crew were instructed to cooperate with hijackers before 9/11, not to fight back.

- We halve the proportion of flights that air marshals are on from 20 to 10%. The U.S. Customs Air Security Officers Program (or sky marshals as they were then called) comprised nearly 1800 recruits when established in 1970, but the program was discontinued in 1974, only to be re-established in the mid-1980s [21]. There were only 33 air marshals in 2001, which was rapidly expanded to several thousand soon after [37].
- Hardened cockpit doors were only introduced in 2003, so this layer can be removed from the analysis entirely.
- However, we assume that, if air marshals are on board, their ability to foil a hijacking attempt is a high 50%.
- Since anti-aircraft measures would have a much lower chance of success before the shocking events of 9/11, we reduce the probability for disruption to 5% for this layer.
- Travel document checkers, Behavior Detection Officers, and the FFDO program were introduced after 2001, so these layers can be removed from the analysis entirely.

With these revised measures in place, the risk reduction is lowered: from 88.2 to 23.5%. The odds of a successful hijacking attack before 9/11 thus become quite high.

We can also evaluate aviation security in the United States prior to 1973 when it was minimal. In-flight measures might include law enforcement officers, and anti-aircraft measures and ability to fly the airliner. With these revised measures in place, overall risk reduction for hijackings is lowered again: from 23.5% (as established for the 1973–2001 period) to 10.6%. The odds of a successful hijacking before 1973 become quite high—the likelihood that a terrorist who arrives at the airport undeterred and undetected will be successful is a high 90%. Under these conditions hijackings are easier to accomplish, something that, sadly, is borne out by the historical record for this period.

4.6 Benefit-to-Cost Ratio for IPSBS

To determine the benefit-to-cost ratio for IPSBs the *benefit* is calculated as:

$$\begin{aligned}
 & \textit{Benefit of IPSBs} \\
 &= \textit{probability of a successful attack} \\
 &\times \textit{losses sustained in the successful attack} \\
 &\times \textit{reduction in vulnerability (risk reduction) furnished by IPSBs}
 \end{aligned}
 \tag{4.4}$$

An easy to understand decision-making metric—the benefit-to-cost ratio (BCR)—is simply the benefit divided by the cost. If the ratio exceeds one, the benefits exceed

the cost and the measure is cost-effective. The most cost-effective measures are those with high risk reduction, low cost, or a combination of the two.

Losses sustained in a successful attack

A loss of \$10 billion for the 9/11 attack on the Pentagon gives a reasonable lower bound, and \$100 billion per airliner for the World Trade Center attack on 9/11 represents an upper bound.

In our analysis, mean losses for a hijacking is taken as \$50 billion.

Probability of an otherwise successful terrorist attack

No terrorist hijackings or bombing attacks have been disrupted at U.S. airports for several decades.

An attempt was made to hijack and crash a FEDEX cargo flight from Memphis to San Jose in 1994 by an employee of the company flying as a passenger; after a violent struggle in the cockpit in which all three flight crew were seriously injured, he was restrained and the aircraft landed safely [22].

If we count the 9/11 attacks as a single attack and the failed FEDEX attack, there have been two hijacking attacks over the last 26 years (1994–2019) in the United States.

The likelihood of a hijacking attack, then, is two divided by 26 years which is 7.7% which we conservatively round down to 5% or one attack every 20 years.

Cost of the security measure

The cost of IPSBs to be installed in new aircraft is \$40 million per year for the entire U.S. commercial airline fleet.

Applying these numbers, the benefit-to-cost ratio (BCR) for IPSBs assuming a risk reduction of 8.2% is 5.1—i.e., \$1 of cost buys \$5.10 of benefit. If public safety is paramount the decision-maker may wish to ensure that decisions are risk averse. In this case, the BCR would increase if a Disproportionate Factor is applied to life-safety benefits [38] or if risk-averse utility function are utilised [6].

The results of this model are robust. Table 4.4 shows that changing the disruption rates in Table 4.2, often very substantially, alters risk reduction mostly by no more than $\pm 7\%$. For example, if the rate of disruption for IPSB is halved to 37.5%, the risk reduction provided by IPSBs declines from 8.2 to 2.8%—with a BCR of 1.7 where \$1 of cost returns nearly \$2 in benefit. Doubling the rates of disruption for passengers, cabin crew and flight deck crew reduces risk reduction of IPSBs to 1.9%, with a BCR of 1.2. Even if there were only one terrorist hijacking attack in a hundred years (annual attack probability of 1%) and the terrorists arrived at the airport undeterred and undetected, secondary barriers would still be cost-effective.

Therefore, at just about all reasonable combinations of security measure effectiveness, costs and attack likelihood, the IPSB is an effective and cost-efficient security measure.

Table 4.4 Sensitivity analysis of risk reductions

	Reduction in vulnerability due to IPSBs (risk reduction) (%)	Benefit-to-cost ratio BCR
Addition of secondary flight deck barriers or IPSBs	8.2	5.1
Rate of disruption for hardened cockpit door reduced by 50%	15.4	9.6
Rate of disruption flight deck resistance reduced by 50%	11.0	6.8
Rate of disruption by passengers and cabin crew reduced to 5%	10.3	6.4
Rates of disruption for anti-aircraft measures is 0%	9.7	6.0
Rate of disruption by passengers reduced from 15 to 5%	9.2	5.7
Rate of disruption for checkpoint screening reduced by 50%	9.0	5.6
Probability of air marshals on flight reduced from 20 to 5%	9.0	5.6
Rate of disruption for checkpoint screening increased by 50%	7.5	4.7
Passenger and cabin crew resistance increased by 50%	6.8	4.3
Rate of disruption for hardened cockpit door increased by 25%	5.5	3.4
Rate of disruption flight deck resistance increased by 50%	5.5	3.4
IPSB installed in 50% of aircraft	4.1	2.6
Rate of disruption for IPSB reduced by 50%	2.8	1.7
Doubling the rates of disruption for passengers, cabin and flight crew	1.9	1.2
Rate of disruption for IPSB reduced from 75 to 25%	1.0	0.62
IPSB cost halved to \$20 million per year	—	10.2
IPSB cost doubled to \$80 million per year	—	2.6
Attack probability reduced to 2.5% per year	—	2.6
Attack probability reduced to 1% per year (1 attack every 100 years)	—	1.0
Loss from successful attack doubled to \$100 billion	—	10.2
Loss from successful attack halved to \$25 billion	—	2.6
Loss from successful attack reduced to \$10 billion	—	1.0

Assumes that the probability that terrorist are undeterred and undetected is 5% per year.
The losses sustained in a successful terrorist hijacking attack are assumed to be \$50 billion.

Table 4.5 Cost-Effectiveness of FAMS, FFDOs and IPSBs

	Reduction invulnerability (risk reduction) (%)	Cost (millions)	Benefit-to-cost ratio BCR
FAMS	1.2	\$1000	0.03
FFDOs	4.0	\$20	5.0
IPSBs	8.2	\$40	5.1

4.7 Benefit-to-Cost Ratio for FFDOS and FAMS

Table 4.5 shows that the FFDOS program passes a cost–benefit assessment for terrorist attacks.³ However, we also find that the FAMS, at a combined cost of about \$1 billion per year, fails to be cost-effective by a considerable margin. Terrorists would need to arrive at an airport in the United States, undeterred and undetected at least two times per year for FAMS to be cost-effective.

Stewart and Mueller [3, 7, 15] provide more details and discussion about these and other security measures and their cost effectiveness.

4.8 Discussion

This approach should not be seen as all or nothing. What is important is to determine what levels of expenditure and risk reduction furnish the greatest benefit and when the law of diminishing returns kicks in. Security measures that are at once effective and relatively inexpensive are generally the first to be implemented (e.g., hardened cockpit doors and FFDOSs), and thus the first dollars spent on counterterrorism measures are often more likely to be worthwhile—that is, to be cost-effective—than are the last. This may even be the case for the expansion of FAMS which began right after 9/11. Quickly boosting the number of air marshals was sensible given understandable fears that there might soon be more hijacking attempts and it might as well have helped assuage the public’s fears about flying a bit. However, the continued expansion of the program thereafter is likely to have done far less good per dollar expended.

The analysis provides a snapshot of risk reductions and cost-effectiveness under present conditions. Of course, terrorists may adapt their threats in reaction to new security measures, security measures may lose effectiveness with time, evolving threats may lead to the potential for higher losses, and so forth. Nevertheless, it does not seem that the competence of terrorists and the destruction they inflict are on the rise, and 9/11 is increasingly standing out as an aberration, not a harbinger—indeed, scarcely any terrorist attack anywhere in the world has managed to do even one-tenth as much total damage. Also, it is difficult to imagine a scenario in which an adaptive terrorist would be able to dramatically alter the odds of pulling off a hijacking or passenger-borne bombing attack. It might be added that the layer of security we find to be particularly cost-ineffective—FAMS—is unlikely to be any more effective when dealing with insider and other threats, and so our conclusions are likely to hold true for those conditions as well. Reducing the budget for this expensive security measure and transferring some of the savings into more cost-effective security measures could maintain current security levels while substantially reducing the cost to taxpayers and the airlines.

³ Assumes that in the absence of FFDOSs, the disruption rate for flight deck resistance drops from 40 to 20%.

It should be stressed as well that our calculations are for terrorists who arrive at the airport undeterred and undetected by other security measures. Since security measures surely do deter and some provide pre-flight detection, the overall impact of existing security measures in preventing hijackings is likely much higher than our analysis would suggest.

The systems model provides a starting point for aviation risk analysis and helps to begin to flesh out some other concerns including the data requirements that become more challenging as the systems model increases in detail and complexity. A more detailed and comprehensive study may be required to fully model the interactions and interdependencies between different threats in aviation security. Nonetheless, the analysis provides a basis for assessing the influence and sensitivity of policy options on risk reduction.

We recognise that risk and cost–benefit considerations should not be the sole criterion for public decision making. Nonetheless, they provide important insights into how security measures may (or may not) perform, their effect on vulnerability and risk reduction, and their cost-effectiveness. They can reveal wasteful expenditures and allow limited funds to be directed to where the most benefit can be attained.

Finally, Western airlines or passengers have comprised about 50% of the victims of successful terrorist attacks worldwide in the past 48 years, but zero percent during the 20 years after 9/11. With the heightened awareness and enhancements in security and expenditures, particularly since 9/11, Western airlines and airports are quite resilient to terrorists attacks [32]—a person would need to fly once per day for 30,000 years before being involved in a terrorist attack.

4.9 Conclusions

In this analysis, we have assessed the full array of security measures designed to protect an airliner from being hijacked, and we have used that to evaluate the risk reduction supplied by each security measure. The analysis is presented in a fully transparent manner: readers who wish to challenge or vary the analysis and assumptions are provided with the information, data, and framework with which to do so. This analysis finds that existing layers of aviation security reduce the risk of a successful hijacking attack by undeterred and undetected terrorists to be near 90%. Secondary flight deck barriers reduce the remaining vulnerability quite considerably to over 95%. This level of risk reduction is very robust: security remains high even when the parameters that make it up are varied considerably. Their relatively low cost and high risk reduction lead to very high benefit-to-cost ratios. Hence, there is little doubt that secondary flight deck barriers are an effective and cost-efficient security measure.

Acknowledgements The support of the Australian Research Council grant DP160100855 is acknowledged.

Appendix A: Reliability Analysis of Aviation Security

Existing Security Measures

The probability that an attack is disrupted, foiled or prevented by pre-boarding security measures assuming that the terrorists have arrived at the airport undeterred and undetected is:

$$\Pr\left(\begin{array}{c} \text{disrupted by} \\ \text{pre - boarding measures} \end{array}\right) = 1 - \left\{ \begin{array}{l} [1 - \Pr(\text{disrupted by no fly list \& passenger pre-screening})] \\ \times [1 - \Pr(\text{disrupted by Behavior Detection Officers})] \\ \times [1 - \Pr(\text{disrupted by travel document checkers})] \\ \times [1 - \Pr(\text{disrupted by checkpoint/TSOs})] \end{array} \right\} \quad (4.5)$$

In the absence of a secondary barrier, the probability that an attack is disrupted or prevented by in-flight security measures is

$$\Pr\left(\begin{array}{c} \text{disrupted by} \\ \text{in-flight} \\ \text{measures} \end{array}\right) = 1 - \left\{ \begin{array}{l} [1 - \Pr(\text{foiled by passengers})] \\ \times [1 - \Pr(\text{foiled by cabin crew})] \\ \times [1 - \Pr(\text{foiled by Law Enforcement Officer})] \\ \times [1 - \Pr(\text{foiled by hardened cockpit door})] \\ \times [1 - \Pr(\text{foiled by flight deck resistance and FFDOs})] \end{array} \right\} \quad (4.6)$$

where

$$\Pr\left(\begin{array}{c} \text{foiled by} \\ \text{hardened} \\ \text{cockpit door} \end{array}\right) = \left\{ \begin{array}{l} \Pr(\text{FAMS on flight}) \\ \times \Pr(\text{foiled hardened cockpit door if FAMS on flight}) \\ + \Pr(\text{no FAMS on flight}) \\ \times \Pr(\text{foiled hardened cockpit door if no FAMS on flight}) \end{array} \right\} \quad (4.7)$$

Addition of Installed Physical Secondary Barriers (IPSBs)

The probability that in-flight security measures will disrupt an attack, and now including the effect of IPSBs, is a modified version of Eq. (4.6):

$$\Pr\left(\begin{array}{c} \text{disrupted by} \\ \text{in-flight} \\ \text{measures} \end{array}\right) = 1 - \left\{ \begin{array}{l} [1 - \Pr(\text{foiled by passengers})] \\ \times [1 - \Pr(\text{foiled by cabin crew})] \\ \times [1 - \Pr(\text{foiled by Law Enforcement Officer})] \\ \times [1 - \Pr(\text{foiled by IPSB})] \\ \times [1 - \Pr(\text{foiled by hardened cockpit if IPSB fails})] \\ \times [1 - \Pr(\text{foiled by flight deck resistance and FFDOs})] \end{array} \right\} \quad (4.8)$$

where

$\Pr(\text{foiled by hardened cockpit door if IPSB fails})$

$$= \left[\begin{array}{l} \Pr\left(\begin{array}{c} \text{FAMS} \\ \text{on flight} \end{array}\right) \times \Pr\left(\begin{array}{c} \text{foiled hardened cockpit door} \\ \text{if IPSB fails and FAMS on flight} \end{array}\right) \\ + \left(1 - \Pr\left(\begin{array}{c} \text{FAMS} \\ \text{on flight} \end{array}\right)\right) \times \left(\begin{array}{c} \text{failed hardened cockpit door} \\ \text{if IPSB fails and no FAMS on flight} \end{array}\right) \end{array} \right] \quad (4.9)$$

where $\Pr(\text{foiled by IPSB})$ is the probability that the IPSB is deployed and will function as intended and delay a hijacker sufficiently to allow the cockpit door to be closed.

References

1. Robinson LA, Hammitt JK, Aldy JE, Krupnick A, Baxter J (2010) Valuing the risk of death from terrorist attacks. *J Homel Secur Emerg Manage* 7(1):Article 14
2. Mueller J, Stewart MG (2011) Terror, security, and money: balancing the risks, benefits, and costs of homeland security. Oxford University Press, New York
3. Stewart MG, Mueller J (2018) Are we safe enough? measuring and assessing aviation security. Elsevier, New York
4. Stewart MG, Mueller J (2008) A risk and cost-benefit assessment of U.S. Aviation security measures. *J Transp Secur* 1(3):143–159
5. Stewart MG, Ellingwood BR, Mueller J (2011) Homeland security: a case study in risk aversion for public decision-making. *Int J Risk Assess Manage* 15(5/6):367–386
6. Stewart MG, Mueller J (2013) Aviation security, risk assessment, and risk aversion for public decisionmaking. *J Policy Anal Manage* 32(3):615–633
7. Stewart MG, Mueller J (2018) Risk and economic assessment of U.S aviation security for passenger-borne bomb attacks. *J Transp Secur* 11:117–136
8. Stewart MG, Mueller J (2011) Cost-Benefit analysis of advanced imaging technology fully body scanners for airline passenger security screening. *J Homel Secur Emergency Manage* 8(1):Article 30
9. Mueller J, Stewart MG (2014) Evaluating counterterrorism spending. *J Econ Perspect* 28(3):237–248
10. Mueller J, Stewart MG (2016) Chasing ghosts: the policing of terrorism. Oxford University Press, Oxford and New York
11. Stewart MG, Mueller J (2014) Risk and cost-benefit analysis of police counter-terrorism operations at Australian airports. *J Policing, Intell Counter Terrorism* 9(2):98–116

12. Stewart MG, Mueller J (2014) Cost-Benefit analysis of airport security: are airports too safe? *J Air Transp Manag* 35(March):19–28
13. Stewart MG, Mueller J (2017) Risk and economic assessment of expedited passenger screening and TSA PreCheck. *J Transp Secur* 10(1):1–22
14. ALPA (2020) Take action to secure the flight deck. <http://www.alpa.org/advocacy/cta/secondary-barriers>
15. Stewart MG, Mueller J (2019) Security risk and cost-benefit assessment of secondary flight deck barriers. Research Report No. 285.11.2019, Centre for Infrastructure Performance and Reliability, The University of Newcastle, NSW, Australia
16. Stewart MG, Mueller J (2013) Terrorism risks and cost-benefit analysis of aviation security. *Risk Anal* 33(5):893–908
17. Smith P (2007) The airport security follies. *nytimes.com*, December 28
18. Schneier B (2003) *Beyond Fear: Thinking sensibly about security in an uncertain world*. Copernicus, New York
19. Walsh T (2016) 15 Years Since 9/11: why are we still vulnerable to this type of attack? *Aviation Security International* June, 29–30
20. Black N, Devine C, Griffin D (2015) Sleep-deprived, medicated, suicidal and armed: federal air marshals in disarray. *CNN Invest*, August 14
21. Elias B (2010) *Airport and aviation security*. CRC Press, Boca Raton, FL
22. Baum P (2016) *Violence in the skies: a history of aircraft hijacking and bombing*. Summerdale Publishers, Chichester, U.K.
23. Moak L (2011) Letter to house subcommittee on transportation security, president of airline pilots association international, July 12, 2011
24. ALPA (2013) Secondary flight deck barriers and flight deck access procedures: a call for action. White paper, Airline Pilots Association International, Washington, DC, July
25. RTCA (2011) Aircraft secondary barriers and alternative flight deck security procedures, final report. Radio Technical Commission for Aeronautics, Special Committee 221, RTCA DO-329, Washington, D.C., September 28
26. Brennan C (2016) 15 years after 9/11, a pilot's widow still seeks aviation security. *The Inquirer*, September 12
27. FAA (2020) Recommendation report to aviation rulemaking advisory committee for implementation of section 336 of P.L. 115–254. Flightdeck Secondary Barrier Working Group, Federal Aviation Administration, Washington, D.C., February 27
28. Aaronson T (2013) *The terror factory*. Ig Publishing, Brooklyn, NY
29. Kenney M (2010) 'Dumb' yet Deadly: local knowledge and poor tradecraft among Islamist Militants in Britain and Spain. *Stud Conflict and Terrorism* 33(10):911–932
30. Mueller J (2020) Terrorism Since 9/11: The American Cases. Mershon Center, Ohio State University, Columbus, OH. <http://politicalscience.osu.edu/faculty/jmueller/SINCE.pdf>
31. Mueller J, Stewart MG (2012) The terrorism delusion: America's overwrought response to september 11. *Int Secur* 37(1):81–110
32. Stewart MG, Mueller J (2020) Terrorism risks chasing ghosts, and infrastructure resilience. *Sustain Resilient Infrastruct* 5(1–2):78–89
33. Jenkins BM (2011) *Stray dogs and virtual armies: radicalization and recruitment to Jihadist Terrorism in the United States Since 9/11*. RAND Corporation, Santa Monica, CA
34. Jackson BA, LaTourette T (2015) Assessing the effectiveness of layered security for protecting the aviation system against adaptive adversaries. *J Air Transp Manag* 35(March):26–33
35. Kohn D (2002) The safest airline: a security example set by Israel's El Al. *60 Minutes*, CBS, January 15
36. Balakrishnan A (2016) Would you pay more for extra airport security? *CNBC*, March 24
37. Meckler L, Carey S (2007) Sky patrol: U.S. Air Marshal service navigates turbulent times. *The Wall Street J*, February 9
38. Grant MJ, Stewart MG (2019) Postal IEDs and risk assessment of work health and safety considerations for postal workers. *Int J Risk Assess Manage* 22(2):152–169