NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

BEHAVIORAL ECONOMICS AND INSIDER THREATS: A CRITICAL REVIEW OF COMPREHENSIVE MITIGATION AND THE CASE FOR A NEW FRAMEWORK

by

David Siegmund

March 2025

Co-Advisors: Rudolph P. Darken
Thomas J. Mackin (contractor)

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2025	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE BEHAVIORAL ECONOMICS AND INSIDER THREATS: A CRITICAL REVIEW OF COMPREHENSIVE MITIGATION AND THE CASE FOR A NEW FRAMEWORK	**5. FUNDING NUMBERS**
6. AUTHOR(S) David Siegmund	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Distribution Statement A. Approved for public release: Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Adversarial insider threats are a persistent risk to critical infrastructure, particularly in aviation, where adversarial insider personnel (AIP) exploit systemic vulnerabilities to perpetrate high-impact crimes. The prevailing frames common for insider threat mitigation are most applicable to the adversarial life cycle and comprehensive insider threat mitigation programs. While this thesis takes an economic approach to assessing many significant facets of insider threat mitigations, it also evaluates the limitations of current mitigation strategies. It introduces a novel Decision Control Framework (DCF) that permits subjective yet methodological and precise socio-economic evaluation of organizational efforts to select and deploy insider threat countermeasures. This framework is informed by behavioral economics and psychological theories. In addition, this thesis presents three case studies of recent insider threat cases at airports as a proxy for more general critical infrastructures, explores the problematic current trends of insider threats within the U.S., and evaluates adversarial, conspiratorial, and airport systems through simple, sequential, and mechanistic economic games to enhance the understanding of agent decision-making and validate historical observations. This research ultimately illustrates vulnerabilities and provides strategic recommendations, emphasizing unpredictability and revealing the implications of invisible and unknowable security measures.

14. SUBJECT TERMS insider threat, Prospect Theory, Decision Theory, deterrence, adversarial mitigation, aviation, critical infrastructure, Game Theory, mechanism design	**15. NUMBER OF PAGES** 189
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

BEHAVIORAL ECONOMICS AND INSIDER THREATS: A CRITICAL REVIEW OF COMPREHENSIVE MITIGATION AND THE CASE FOR A NEW FRAMEWORK

David Siegmund
Transportation Security Specialist, Transportation Security Administration,
Department of Homeland Security
BA, Saint Leo University, 2016

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2025**

Approved by: Rudolph P. Darken
Co-Advisor

Thomas J. Mackin
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Adversarial insider threats are a persistent risk to critical infrastructure, particularly in aviation, where adversarial insider personnel (AIP) exploit systemic vulnerabilities to perpetrate high-impact crimes. The prevailing frames common for insider threat mitigation are most applicable to the adversarial life cycle and comprehensive insider threat mitigation programs. While this thesis takes an economic approach to assessing many significant facets of insider threat mitigations, it also evaluates the limitations of current mitigation strategies. It introduces a novel Decision Control Framework (DCF) that permits subjective yet methodological and precise socio-economic evaluation of organizational efforts to select and deploy insider threat countermeasures. This framework is informed by behavioral economics and psychological theories. In addition, this thesis presents three case studies of recent insider threat cases at airports as a proxy for more general critical infrastructures, explores the problematic current trends of insider threats within the U.S., and evaluates adversarial, conspiratorial, and airport systems through simple, sequential, and mechanistic economic games to enhance the understanding of agent decision-making and validate historical observations. This research ultimately illustrates vulnerabilities and provides strategic recommendations, emphasizing unpredictability and revealing the implications of invisible and unknowable security measures.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1

A. PROBLEM STATEMENT 1

B. THE DYNAMIC NATURE OF INSIDER THREATS 3

1. Insider Threat Motivations 3

2. Diverse Ideology and Social Pressures 7

3. Strained Labor Considerations 10

4. Inhibited Law Enforcement 12

5. Modern Airports 12

6. Increasing AIP Capability 14

C. RESEARCH QUESTIONS 15

D. RESEARCH DESIGN 15

II. LITERATURE REVIEW 19

A. CONCURRENCE REGARDING INSIDER THREAT MITIGATION STRATEGY 19

B. THE PROLIFERATION OF TACTICS 21

C. UNDERSTANDING RISK AND POLICY IMPLICATIONS 24

D. DECISION-MAKING: PSYCHOLOGY AND BEHAVIORAL ECONOMICS 28

1. Decision Control: Self and Social Control 28

2. Economic Decision-Making: Games, Rational Choice, and Prospects 31

E. CONCLUSION 41

III. INSIDER THREAT CASE STUDIES: THE PATHS ARE LEGION BEFORE THE INSIDER 43

A. WHEN TRUST IS THE PROBLEM 43

1. Case 1: Even Smuggling Is Bigger in Texas 43

2. Case 2: Just One Bag—Daallo Flight 159 46

3. Case 3: It's People—The Crew Are People 49

B. CASE STUDY SYNTHESIS 52

C. COUNTERFACTUAL ANALYSIS 54

1. Aviation Worker Screening at Access Points to Secured Areas 55

2. Increased Recurrent Vetting 57

3. Increased Intelligence Gathering and Investigation and Employee Monitoring 60

D. CONCLUSION....62

IV. WINNING THE BATTLE, LOSING THE EDGE—INSIDER THREAT MITIGATION IN AIRPORTS....65
A. MECHANISM DESIGN THEORY (MDT): SECURITY GAMES....66
B. AIRPORT SYSTEMS—THE GAME....67
1. Model Elaboration....70
2. Extending and Revising the Model....72
3. Incentivized Security....73
C. ADAPTED MDT—A SEQUENTIAL ADVERSARY-DEFENDER GAME....79
1. MDT Applied to Adversarial Gaming....79
2. Combining MDT and Attacker-Defender Games....80
D. A GAME OF WATER AND DANGEROUS DRUGS....82
1. Game 1....84
2. Game 2....95
E. CONCLUSION....98

V. CONSIDERATION OF BEHAVIORAL ECONOMICS AND PSYCHOLOGICAL THEORY....101
A. SELF AND SOCIAL CONTROL THEORIES—CRIMINOLOGY AND THE CRIMINAL....103
B. SOCIAL IDENTITY THEORY—THE RELATIONSHIP OF THE PERSON TO MANY WHOLES....106
C. RATIONAL CHOICE THEMES—IS THIS WORTH THE RISK?....110
D. PROSPECT THEORY—DEGREES OF RATIONALITY....115
E. A NOVEL DECISION CONTROL FRAMEWORK....119
F. CONCLUSION....130

VI. CONCLUSION....133
A. KEY FINDINGS AND SYNTHESIS....133
1. Insider Threat Dynamics....133
2. Strategic and Tactical Insights....134
3. Theoretical Contributions....135
B. RECOMMENDATIONS....136
1. Policy and Engagement....136
2. Implement Economic Incentives to Drive Security Investment....137

3. Operational Enhancements 137
C. LIMITATIONS AND AMBIGUITIES 138
D. FUTURE RESEARCH AND TECHNOLOGICAL INNOVATION 139
E. CLOSING REMARKS 141

LIST OF REFERENCES 143

INITIAL DISTRIBUTION LIST 163

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Insider Threat Motivations 5

Figure 2. True vs. Reported Headline Rates of Unemployment..... 10

Figure 3. Construction of Mass-Transit Linkages at Los Angeles International Airport Demonstrating Increasing System Complexity. 14

Figure 4. Airport Net Profit by Passengers Per Annum..... 76

Figure 5. ~38 Grams of Seized Fentanyl Prepared for Distribution Demonstrating Compact Size 88

Figure 6. DCF: Axial Organization of Theoretical Families..... 125

Figure 7. DCF Illustrated Influence of Countermeasure According to Valuation 129

Figure 8. DCF: Illustration of Focus Areas—Comprehensive Mitigation Evaluation..... 130

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Summary of Case Study Attributes 53

Table 2. Airport MDT Game 1 70

Table 3. Airport MDT Game 2 73

Table 4. Airport MDT Game 3 78

Table 5. Security Value Table 90

Table 6. Game 1—Attacker Defender 94

Table 7. Game 2—Increased Resources 97

Table 8. Countermeasures by Theoretical Family 124

Table 9. Countermeasure Evaluation 127

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AA	adversarial agent, games
AAAE	American Association of Airport Executives
ACI	Airports Council International (Inc.)
AIP	adversarial insider personnel
AR	augmented reality
ASAC	Aviation Security Advisory Council
CBA	Cost-benefit analysis
CBP	Customs and Border Protection (U.S.)
CCTV	closed-circuit television
CFR	Code of Federal Regulations (U.S.)
CIP	critical infrastructure protection
CISA	Cybersecurity and Infrastructure Security Agency
CPIR	Critical Pathway to Insider Risk
DCF	Decision Control Framework (proposed)
DFW	Dallas-Fort Worth International Airport
DHS	Department of Homeland Security
HSI	Homeland Security Investigations
ICAO	International Civil Aviation Organization
IED	improvised explosive device
ISIS	Islamic State of Iraq and the Levant – a transnational Salafi jihadist group and unrecognized quasi-state
JFK	John F. Kennedy International Airport
KCM	Known Crewmember (program)
MDT	Mechanism Design Theory
RAP	Record of Arrest and Prosecution (program)
RBF	risk-based frameworks
SA	security agent, games
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Card (program)
U.S.	United States of America
VSL	value of a statistical life

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The escalating challenge of insider threats, referred to herein as adversarial insider personnel (AIP) within critical infrastructure, where trusted personnel might exploit their legitimate access to cause harm, remains significant to critical infrastructure protection (CIP). This thesis explores this problem within the aviation industry, specifically at airports. This issue has led to substantial economic losses and billions spent annually on mitigation efforts. Traditional security measures, rooted in economic and utilitarian theories, often fail to address the unique characteristics of AIP, who possess insider knowledge and adaptability. Case studies and data show the increasing sophistication of such threats, with incidents involving smuggling, bypassing security measures, and collaboration with external actors. The problem is compounded by fragmented mitigation strategies, insufficient coordination among stakeholders, and resistance to implementing advanced security measures due to cost and operational constraints. These gaps underscore the need for multidisciplinary approaches, integrating behavioral economics, game theory, and psychological insights to develop adaptive and dynamic strategies for reducing insider threats in critical infrastructure environments.

Insider threats are among the most challenging risks to mitigate due to their inherent complexity. AIP leverage privileged access to bypass traditional security measures, exploiting procedural gaps and trusted status. This challenge is exacerbated by the increasing financial and operational costs associated with countering such threats. For instance, the 2022 Ponemon report estimates that organizations spend an average of $15 million annually on insider threat mitigation.[1] In aviation, critical infrastructure invests significantly in insider threat programs that seek to mitigate various aspects of insider threats and their life cycle, the importance of which has been the repeated call of existing

[1] Ponemon Institute, *Ponemon Insider Threats Global Report – 2022* (Traverse City, MI: Ponemon Institute, 2023), 4, https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-the-cost-of-insider-threats-ponemon-report.pdf.

research.[2] The aviation industry's reliance on trust, exemplified by systems such as unescorted access authority and the Known Crewmember (KCM) program, creates vulnerabilities that adversaries exploit. High-profile incidents, such as smuggling operations at Dallas/Fort Worth International Airport (DFW) and the bombing of Daallo Airlines Flight 159, highlight the limitations of static security measures and underscore the need for dynamic, adaptive countermeasures. This thesis attempts to answer the following research questions:

1. Primarily, to what extent can the principles of behavioral economics, classical economics, and other prominent psychological theories be applied to insider threat models and countermeasures, and what novel decision-making (or resource allocation) insights might such application offer?

2. Secondarily, and in relation to behavioral economics, when considering the perspectives of agents within critical infrastructure systems, what barriers and factors contribute to investment decisions and, as an extension, the formation of AIP mitigation strategies and the deployment of countermeasures at airports and other critical infrastructure?

3. Additionally, are common AIP countermeasures consistent with expectations derived from economic models and other significant psychological theories?

This research employs a multidisciplinary approach, integrating behavioral economics, game theory, and psychological theories to analyze the dynamics presented by the AIP problem. Key methodologies include:

[2] Mohd Nazer Apau, Muliati Sedek, and Rabiah Ahmad, "Inclination of Insider Threats' Mitigation and Implementation: Concurrence View from Malaysian Employees," in *Knowledge Management in Organizations*, ed. Lorna Uden, Branislav Hadzima, and I-Hsien Ting, vol. 877, Communications in Computer and Information Science (Springer International Publishing, 2018), 49, https://doi.org/10.1007/978-3-319-95204-8_29; Brian S. Bean, "Mitigating Insider Threats in the Domestic Aviation System: Policy Options for the Transportation Security Administration" (master's thesis, Naval Postgraduate School, 2017), 71, https://hdl.handle.net/10945/56861; Nick Catrantzos, "Insider Threat: Applying No Dark Corners Defenses" (master's thesis, Naval Postgraduate School, 2018), 63–64, https://hdl.handle.net/10945/4656.

- Case Study Analysis: High-profile incidents are examined to identify patterns in AIP behavior, vulnerabilities exploited, and the effectiveness of mitigation strategies.
- Counterfactual Analysis and Thought Experiment: Trends and insights from the case analysis are used to consider the value of various tactics and countermeasures qualitatively.
- Game Theory and Mechanism Design Theory (MDT): Used for both airport security investment decisions in competition with other airports and adversarial decision-making in reaction to the deployment decisions of security agents.
- Behavioral Economics and Psychological Frameworks: Self and Social Control Theory, Social Identity Theory, Rational Choice Theory, and Prospect Theory are applied to understand the cognitive and social drivers of adversarial behavior and develop a new frame through which AIP countermeasures may be evaluated.

The research reveals several important insights.

- Motivations: AIP are driven by diverse motivations, including financial gain, ideological conflict, personal grievances, psychological disturbances, and power dynamics. These motivations interact dynamically with the environment, enabling AIP to adapt to security measures.
- Adaptability: AIP learn and evolve in response to security protocols. For example, conspirators in the DFW smuggling operation used procedural knowledge and collaborative planning to subvert security measures.
- Visibility and Knowability: Current strategies rely heavily on static and visible security measures, such as physical screening and access controls to presumably deter and detect AIP. Insights from analysis of the cases, games and socio-economic frames indicate that the extent to which security measures can be observed and known inhibits the security value of tactics from an adversarial perspective. Additionally, existing recommendations for insider threat programs cannot dynamically assess the effect of this observation.

- Behavioral economics reveal that AIP often engage in risk-seeking behavior, driven by cognitive biases and heuristics. Prospect Theory explains how loss aversion and perceived gains influence adversarial decision-making. These insights suggest that traditional deterrence models assume rational behavior and may fail to account for the psychological factors driving insider activity.[3]
- Security Investment: Mechanism Design Theory (MDT) economic games highlight the strategic interactions between defenders and adversaries, revealing critical vulnerabilities in current security systems. MDT demonstrates that airports face conflicting incentives when investing in security measures, with economic and operational considerations often outweighing collective security benefits.
- The proposed Decision Control Framework (DCF) synthesizes insights from behavioral economics, game theory, and psychology to provide a structured approach for evaluating and selecting countermeasures. The framework emphasizes:
    - Unpredictability: Countermeasures should be dynamic and challenging for adversaries to adapt to or predict.
    - Layered Security: A multilayered approach reduces reliance on any single measure and increases the complexity of adversarial planning.
    - Cultural and Social Interventions: Enhancing organizational culture and social bonds can reduce the likelihood of adversarial behavior.
    - Visibility and Adaptation: Balancing visible and invisible countermeasures to deter AIP without revealing system vulnerabilities.

The threat posed by AIP is a complex, evolving challenge that demands a multidisciplinary response. This thesis highlights the limitations of current mitigation strategies and proposes the DCF to guide the development of adaptive, layered, and socially informed countermeasures. By integrating insights from behavioral economics, game

[3] Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision Under Risk," *Econometrica* 47, no. 2 (March 1979): 17–18, https://doi.org/10.2307/1914185.

theory, and psychology, this research provides a roadmap for enhancing the resilience of critical infrastructure against insider threats. The findings underscore the need for collaborative efforts among regulators, industry stakeholders, and researchers to address the systemic vulnerabilities exploited by AIP. Future research should focus on refining and validating theoretical models, evaluating innovative countermeasures, and fostering interdisciplinary collaboration to create a more secure aviation environment.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis represents the culmination of a challenging and deeply rewarding journey, and I am profoundly grateful to those who supported and guided me along the way. First and foremost, I wish to thank my beautiful and intelligent wife, Andi. Your insightful advice and unwavering encouragement, both about this thesis and throughout my participation in the CHDS master's program, were invaluable. The many discussions we shared helped shape my thoughts and deepen my understanding. I am endlessly grateful. To my children, Alice and Roland, thank you for your patience and understanding throughout what I know felt like a "lost year" devoted to this work. Your resilience and love were constant sources of motivation.

I sincerely thank Bob Scott for his support and for keeping the promise to provide the time and space necessary to complete this project. To the rest of my leadership team—Zach Landis, Robert Rottman, Jackie Bester, and Kevin Knott—your sponsorship and belief in the value of my participation in this program made this possible. Thank you for your understanding and encouragement. I am especially grateful to Dr. David Brannan and Dr. Anders Strindberg, whose commitment to challenging our preconceptions and prejudices profoundly influenced my perspective. Your willingness to share opened my understanding of the world and my place in it, leaving an indelible mark on my academic and professional growth. To my advisors, Dr. Thomas Mackin and Dr. Rudy Darken, I deeply appreciate your patience and guidance as we navigated the complex and often vexing challenges posed by the intersection of insider threats, critical infrastructure, and my obtuse thinking. Your expertise and support were essential to the success of this thesis. Finally, to all those whose names may not appear here but who contributed in ways large and small, particularly the CHDS cohorts 2302 and 2304, thank you. I am profoundly grateful for your encouragement, feedback, and belief in this endeavor. While this thesis looks nothing like I imagined it would have, neither am I the same as when I began. Thank you for your unselfish, sometimes unintentional, contributions.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Insider threats to aviation—individuals using legitimate authority and trusted access to cause harm—are evolving, more dangerous, difficult to mitigate using traditional security measures, and driving airports and the commercial aviation industry to spend billions of dollars annually.[1] The 2022 Ponemon "Costs of Insider Threats Global Report" is the industry standard for quantifying expenditure on insider threat mitigation and response and estimates that more than $15 million, on average, was spent per company in this effort.[2] Research by Carnegie Mellon's world-renowned insider threat program indicates such threats have continued to increase in frequency and damage.[3] Analysis focusing on lost productivity by Lowers and Associates, a prominent risk management firm, notes that business costs resulting from workplace violence alone, a subset of insider risk, found that $130 billion are being lost by businesses annually, quadrupling in fiscal impact over 30 years.[4] In the aviation industry, airports are preparing to add nearly a billion dollars of spending to physically screen a small percentage of airport workers daily, cutting into financial solvency and their distinct ability to provide competitive service.[5] Industry and regulators are expending significant resources to reduce the opportunities and impacts of adversarial insider personnel (AIP) while, so far, failing to control them.

---

[1] Triana McNeil, *Aviation Security: TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals*, GAO-20-275 (Washington, DC: Government Accountability Office, 2020), 11, https://www.gao.gov/assets/gao-20-275.pdf.

[2] Ponemon Institute, *Ponemon Insider Threats Global Report – 2022*, 4.

[3] Software Engineering Institute, *Common Sense Guide to Mitigating Insider Threats*, 7th ed. (Pittsburg, PA: Carnegie Mellon University, 2022), 4, https://insights.sei.cmu.edu/documents/5777/5692_CSG_Book_20-optimized.pdf.

[4] Lowers & Associates, "The Impact of Workplace Violence," Risk Management Blog, May 19, 2016, http://www.lowersriskgroup.com/blog/2016/05/19/infographic-impact-workplace-violence/.

[5] Airports Council International, "ACI-NA Position on TSA's Aviation Worker Screening National Amendment" (Washington, DC: Airports Council International, August 2, 2023), https://airportscouncil.org/wp-content/uploads/2023/08/ACI-NA-USPC-Position-on-TSA-Aviation-Worker-Screening-Mandate.pdf.

The United States (U.S.) aviation industry struggles to mitigate the risk insiders pose. For example, despite modern insider risk mitigation efforts, employees at Dallas/Fort Worth International Airport (DFW) were caught smuggling guns and offering to smuggle explosives while bypassing existing security measures in 2018.[6] This struggle is also evident in the recent Aviation Security Advisory Committee's 28 aviation insider threat mitigation recommendations to the Transportation Security Administration (TSA).[7] Insider threats pose a grave threat to public trust and a risk to life at U.S. airports. Still, methods to effectively mitigate such risks remain contested by industry leaders, regulatory authorities, and researchers.[8] Given this risk and the lack of agreement associated with AIP, strategies should be continually assessed from valuable, multi-disciplinary perspectives.

Researchers, regulators, and businesses have struggled to design effective solutions. The National Safe Skies Alliance Program for Applied Research's report on *Insider Threat Mitigation at Airports* illustrates many options and tactics.[9] Many of these efforts, like vetting employees before and after granting trust or physically screening employees, are traditionally used to mitigate threats posed by external actors and are rooted in traditional economics theory.[10] Insiders are different: their authority empowers them to

---

[6] Harrison Roberts, "Airline Employee, Heading DFW Airport Drug-Smuggling Ring, Sentenced to 16 Years in Prison," KCBD, December 6, 2019, https://www.kcbd.com/2019/12/06/airline-employee-heading-dfw-airport-drug-smuggling-ring-sentenced-years-prison/; Alex Scroxton, "Calls for Clarity over Amazon Insider Breach," *ComputerWeekly*, October 27, 2020, https://www.computerweekly.com/news/252491142/Calls-for-clarity-over-Amazon-insider-breach; Vincent Manancourt, "'Millions of People's Data Is at Risk' — Amazon Insiders Sound Alarm over Security," Politico, February 24, 2021, https://www.politico.eu/article/data-at-risk-amazon-security-threat/.

[7] Steve Alterman, *Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control* (Washington, DC: Aviation Security Advisory Committee, 2015), https://www.tsa.gov/sites/default/files/asac-employee-screening-working-group-04-15.pdf. The ASAC was established in 1989 and made permanent in 2014. It consists of industry leaders affected by security regulations and serves to inform TSA Administrator decisions and strategy.

[8] Catrantzos, "Insider Threat," 65.

[9] Jessica Grizzle, *Insider Threat Mitigation at Airports* (Louisville, TN: National Safe Skies Alliance, Inc., 2021), v, https://www.sskies.org/images/uploads/subpage/PARAS_0026_InsiderThreatMitigation.FinalReport_.pdf.

[10] Catrantzos, "Insider Threat," 41; Taj Mathew, "Insider Threat: A Constant Problem with a Continuous Approach" (master's thesis, Naval Postgraduate School, 2023), 70, https://hdl.handle.net/10945/71985.

consider countermeasures with perfect knowledge and the advantage of attack initiative.[11] Current wisdom may also mislead policymakers by ignoring these aspects of insider perspectives and failing to account for themes sometimes absent from practical and rational choice models.[12] Employing behavioral economics concepts, as espoused by Prospect Theory, such as uncertainty, weighting biases, and loss aversion, while considering the adversarial perspective via psychological frameworks and attacker-defender game analysis may provide valuable new information, advance critical infrastructure protection, and guide future investments and strategic decisions toward options proven most effective.

B. THE DYNAMIC NATURE OF INSIDER THREATS

Insider threats are not static; they evolve in response to shifting economic, technological, social, and political landscapes. External threats often follow predictable patterns of intrusion and attack, whereas insider threats are deeply influenced by personal circumstances, workplace environments, and broader societal trends. Economic downturns, labor disputes, and organizational restructuring create stressors that will push otherwise trustworthy employees toward adversarial behavior. Social division, ideological radicalization, and social diversification further complicate the insider threat landscape, as individuals may be driven by grievances beyond the workplace. Moreover, the convergence of these factors creates a fluid threat environment where motivations can shift over time, contributing to new risks as old ones fade.

1. Insider Threat Motivations

Motivations compelling insiders to become adversarial can be categorized to better inform this analysis. Kirkpatrick provides an analysis of disgruntled employees as an important motivation for insider threat behavior but also discusses a number of other motivations such as personal gain via embezzlement and nationalist goals via espionage,

[11] Catrantzos, "Insider Threat," 63–64.

[12] Fariborz Farahmand and Eugene H. Spafford, "Understanding Insiders: An Analysis of Risk-Taking Behavior," *Information Systems Frontiers* 15, no. 1 (March 2013): 14, https://doi.org/10.1007/s10796-010-9265-x.

among others.[13] Cybersecurity and Infrastructure Security Agency (CISA) makes information on threat types available, which include potential motivations for insider threats such as "getting even" or "promoting a social objective".[14] From these examples, five distinct and useful categories for insider threat motivation can be distinctly observed: financial gain, power, ideology or nationalist loyalties, resentment and discontent, and emotional or psychological disturbance.

Adversaries motivated by financial gain may attempt to enrich themselves, enhance their career prospects, or acquire money to pay debts. They will likely be opportunistic given their access to systems, materials, and spaces. Using Kirkpatrick's analysis, threat actors interested in acquiring or preserving power may use insider access to propel their career or influence small group politics; for instance, sabotaging the employer's supply chain may ensure competitors are more successful, whereas nationalist and ideological motivations may manifest as the theft of information or even seek to damage their host organization. Further, ideological motivation may compel an adversary to take more significant risks and engage in more elaborate plots.

Resentment and discontent often result from an insider's experience with an employer and usually manifest as simple defiance of policies. As a result, this motivation may serve to magnify existing intent to cause harm as opportunities present. Unlike other motivating factors, individuals affected by emotional and psychological disturbances, including those induced by drugs and medical conditions, may act without rational motivation, and tend toward violence.[15] These categories, illustrated in Figure 1 with exemplar objectives, are useful to understanding the impact of insider threat mitigation measures, and assessing an insider threat program and strategy against the multitude of potential threats.

---

[13] Shelley Kirkpatrick, "Refining Insider Threat Profiles," *Security Magazine* 45, no. 9 (September 2008): 57–63.

[14] Cybersecurity and Infrastructure Security Agency, "Defining Insider Threats," America's Cyber Defense Agency, accessed October 30, 2023, https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats.

[15] Molly Anman et al., *Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks* (Washington, DC: U.S. Department of Justice, 2017), 88.

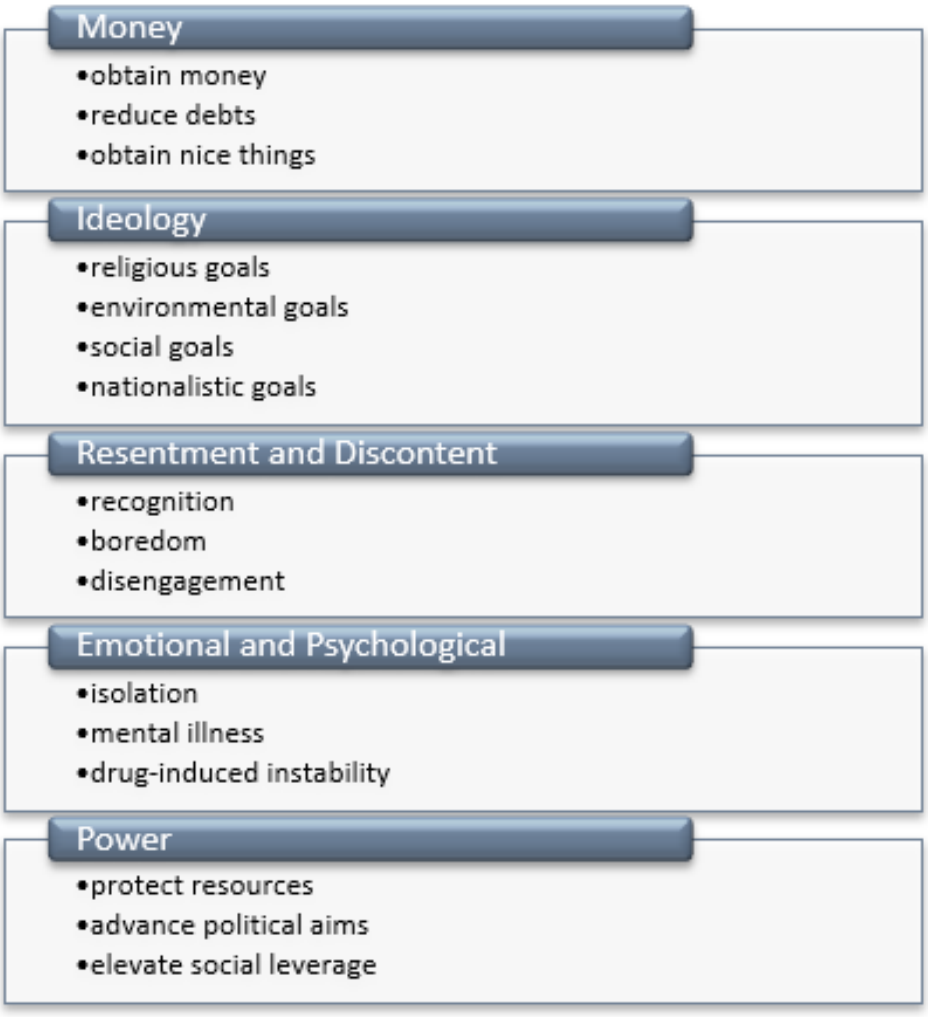

Figure 1. Insider Threat Motivations[16]

Motivation may overlap in definition and manifest simultaneously in individuals and groups. As Kirkpatrick's article indicates, different motivations will favor particular pathways, be sensitive to distinct countermeasures, and be causal to target selection. For example, AIP motivated by personal enrichment may choose to steal from passengers or employers. Motivated by personal enrichment, such AIP will likely prioritize surveillance avoidance and secrecy to continue their activities and avoid punishment. Conversely, AIP motivated by newly discovered ideological conflict with any domestic authority may use

16 Adapted from Kirkpatrick, "Refining Insider Threat Profiles," 57–63.

any opportunity to cause harm, including the circumvention or nullification of traditional security features such as screening.[17] An ideologically motivated AIP may also be less deterred by physical security measures or getting caught after-the-fact.[18] Finally, insider threats posed by disengaged employees may also take a more passive form such as negligent behavior and defiance of policy with observed tendencies to embarrass the organization.[19] Considering the motivation of an insider threat is important as it permits researchers to understand the intensity and tactics such threats may use to cause crime, violence, and operational disruptions.

Business and regulatory actions and reactions to issues surrounding the problem of insider threats demonstrate a complex and sometimes competitive environment. For instance, Airports Council International recently displayed prescient concerns in its response to the TSA's 2023 requirement of modest improvements to aviation worker screening at airports.[20] The realities of proper governance, including protecting civil rights and liberties and preserving cooperation between regulatory authorities and private stakeholders, including concerns about profit, liability, and market competition, are intractable and often provide the outer bounds for realistic action. Consider that the TSA has spent billions on enhancing the passenger screening checkpoint: to fund the security of the nation's transportation systems, $6.46 billion was appropriated for the TSA in fiscal year 2022.[21] This is an impressive figure and does not represent the whole U.S. commitment to domestic aviation security. Airports spend much more to ensure only

---

[17] Adam Humphrey, "Do Innovative Thinkers Pose an Increased Insider Threat?: A Preliminary Analysis" (master's thesis, Monterey, CA, Naval Postgraduate School, 2019), 41, https://calhoun.nps.edu/bitstream/handle/10945/62735/19Jun_Humphrey_Adam.pdf.

[18] Farahmand and Spafford, "Understanding Insiders," 7.

[19] Kirkpatrick, "Refining Insider Threat Profiles," 58.

[20] Airports Council International, "ACI-NA Position on TSA's Aviation Worker Screening National Amendment." ACI is a group that focuses on representing the collective interests of airports internationally. ACI-NA is the North American chapter. They also establish and leverage deep relationships with regulatory authorities. It should also be noted that most airports in the United States are publicly owned and operated enterprises that are generally exempt from federal taxation but are nonetheless motivated by generating revenue and are self-sustaining. .

[21] Alejandro Mayorkas, *DHS Agency Financial Report FY2022* (Washington, DC: Department of Homeland Security, 2022), 154, https://www.dhs.gov/sites/default/files/2022-11/dhs_agency_financial_report_fy2022.pdf.

aviation workers have access to security-restricted areas given regulatory requirements and often implement measures above the requirements. As security measures are enhanced at passenger screening checkpoints and the perimeter of the airport, keeping the "bad guys" out will shift motivated threat actors elsewhere. Sufficiently motivated adversaries have sought any means of bypassing security, as indicated by numerous smuggling operations in airport security-restricted areas. These small examples of action and perspective drive a complex system within which insider threat ideation and mitigation occur.

Insider incidents have continued to increase both in frequency and damage.[22] However, recent international conflict, changing labor-relations contexts, concerns with law enforcement, and the modernization and diversification of airport business models may exacerbate the issue. AIP are human beings subject to the motivations and challenges of everyday life. Therefore, security professionals may look to macro trends regarding economic and social stability to speculate and forecast security challenges, particularly those caused by AIP.

2. Diverse Ideology and Social Pressures

The U.S. is becoming more diverse, and as it does, it is more vulnerable to action by disenfranchised groups and individuals within it. The U.S. has always been a melting pot; however, over the last two decades, it has accelerated its trajectory toward increasing diversity. According to the U.S. Census Bureau, the U.S. is expected to grow more from international migration than from natural population growth through 2060.[23] According to this information, some foreign-born groups, such as those from Africa and Asia, are expected to double in size over this period.[24] Predicting shifts in diversity is a difficult task, but census information indicates the country is entering an uncharted period during which the percentage of foreign-born residents will have never been higher. While

[22] Ponemon Institute, *Ponemon Insider Threats Global Report – 2022*, 4.

[23] Jonathan Vespa, Armstrong, David, and Medina, Lauren, "Demographic Turning Points for the United States: Population Projections for 2020 to 2060" (U.S. Census Bureau, March 2018), 2.

[24] Christine Tamir, "Key Findings about Black Immigrants in the U.S.," Pew Research Center, January 27, 2022, https://www.pewresearch.org/short-reads/2022/01/27/key-findings-about-black-immigrants-in-the-u-s/; Vespa, Armstrong, David, and Medina, Lauren, "Demographic Turning Points for the United States: Population Projections for 2020 to 2060," 7.

immigration does not in itself portend greater division, it has been observed globally and domestically, more acutely, that the political landscape has been trending toward fractionalization with increasing extremist tendencies.[25] Given these facts, it is astonishing that violent, ideologically and politically motivated incidents such as the Waco Siege Incident of 1993 and the Oklahoma City Bombing of 1994 have not continued to permeate society or erode the domestic sense of security.

Diverse populations and political perspectives can drive conflict and press individuals into action. Increasingly diverse populations in the United Kingdom (U.K.) have become more critical of mainstream government policy and more vulnerable to issues of inequity and marginalization.[26] Social scientists Husband and Alam observed in their research a rising tide of *difference politics* chipping away at unity in the U.K. and conclude there is a delicately balanced relationship between cohesion and violence of many forms.[27] Social cohesion, a quality that supports resilience and suppresses violence, is under strain. The U.K.'s experience is repeating throughout the West. During the weeks following the October 7, 2023, attack by Hamas, U.S.' allies have experienced a wave of opportunistic violence, including bomb threats and stabbings.[28] On October 17, 2023, a lone shooter, enabled by several others, killed two individuals and wounded another: the shooter is reported to have been inspired by Islamic State of Iraq and the Levant (ISIS) propaganda and the Hamas attack.[29] The actions of the U.S. and its interests abroad help to shape global sentiment and the world's reaction.

---

[25] World Economic Forum, *Global Risks Report 2023* (Zurich: World Economic Forum, 2024), 24–37, https://www.weforum.org/reports/globalrisks-report-2023/; Michael McMasters, "Societal Polarization: An Evolving Threat to U.S. Homeland Security" (master's thesis, Naval Postgraduate School, 2023), 22, https://hdl.handle.net/10945/72572.

[26] Charles Husband and Yunis Alam, *Social Cohesion and Counter-Terrorism: A Policy Contradiction?* (Portland, OR: Policy Press, 2011), 202–4.

[27] Husband and Alam, 100.

[28] Philip Fong, "Police Open Fire at Paris Train Station on Woman Making 'Threats,'" *Digital Journal*, October 31, 2023, sec. World, https://www.digitaljournal.com/world/police-open-fire-at-paris-train-station-on-woman-making-threats/article.

[29] "Brussels Shooting: Man Arrested on Suspicion of Supplying Gun to Assailant in Deadly Attack," Yahoo News, October 26, 2023, https://news.yahoo.com/brussels-shooting-man-arrested-suspicion-182722591.html; George Wright, "Brussels Shooting: 'Europe Shaken' after Two Swedes Shot Dead," BBC News, October 16, 2023, https://www.bbc.com/news/world-europe-67129117.

Domestic issues will also contribute to insider threat ideation. Since 2018, there have been numerous examples of activity that has been deemed insurrectionist by some and political violence by others, contentiously, such as the violent attacks on the federal courthouse in Portland, Oregon, and the breach of the United States Capital Building, both in 2020.[30] Even the politically charged, deeply divided discourse on such issues tips a hand toward destabilized social structures through the early part of this decade. Even without inspiration from the foreign stage, the domestic conflict between political parties and ideological extremists has resulted in violent clashes exceeding the bounds of protest and easily demonstrates the collective potential for future domestic terrorism, violence, and true insurrection. Violence is an attractive option in any political environment wherein there are fundamental disagreements, minority groups seeking power, and the degradation of quality public discourse.[31] Should democratic institutions and authority begin to fail, violence will become an increasingly attractive option to some groups and people.[32] Trusted and decorated individuals in the U.S. have demonstrated the capacity for violence recently. In 2025, two significant and relatively sophisticated plots of political violence, one in New Orleans and one in Las Vegas, were perpetrated in part to communicate political change through violence.[33] An increase in anti-American, pro-ISIS, or anti-Israeli sentiment at home is a portent of ideological and nationalistic threat ideation. Individuals in the U.S. are primed for radical action, especially given the increasingly diverse population and the U.S.' ever-present influence on world events. There is little reason to believe that the broad community of critical infrastructure employees is in some special way immune to the motivations that led to these recent attacks: trusted insiders are not immune from this trend of violence.

---

[30] Michael S. Brown Jr, "Tell Me How This Begins: Insurgency in the United States" (master's thesis, Naval Postgraduate School, 03/23), 40, https://hdl.handle.net/10945/72065.

[31] McMasters, "Societal Polarization: An Evolving Threat to U.S. Homeland Security," 13–15.

[32] Bruce Hoffman, *Inside Terrorism*, 3rd ed. (New York: Columbia University Press, 2017), 481.

[33] Jack Brook, Stephen Smith, and Sara Cline, "FBI Says Driver behind New Year's Truck Attack Visited New Orleans Twice before," PBS News – Nation, January 5, 2025, https://www.pbs.org/newshour/nation/fbi-says-driver-behind-new-years-truck-attack-visited-new-orleans-twice-before; Steve Beynon, "Green Beret in Las Vegas Bombing and New Orleans Attacker Had Brief Overlap in Military Careers," Military, January 6, 2025, https://www.military.com/daily-news/2025/01/06/green-beret-las-vegas-bombing-and-new-orleans-attacker-had-brief-overlap-military-careers.html.

3. Strained Labor Considerations

As an example of the critical infrastructure insider experience, the aviation worker experience, specifically, is increasingly challenging due to labor market instability and increasing automation. Help-wanted signs and intense hiring campaigns are increasingly common. This is a particularly concerning issue for business owners and the service and transportation industry, including aviation businesses. As the country continues to emerge from COVID-19, the labor pool remains restricted, and measures of unemployment remain historically low (Figure 2).[34]

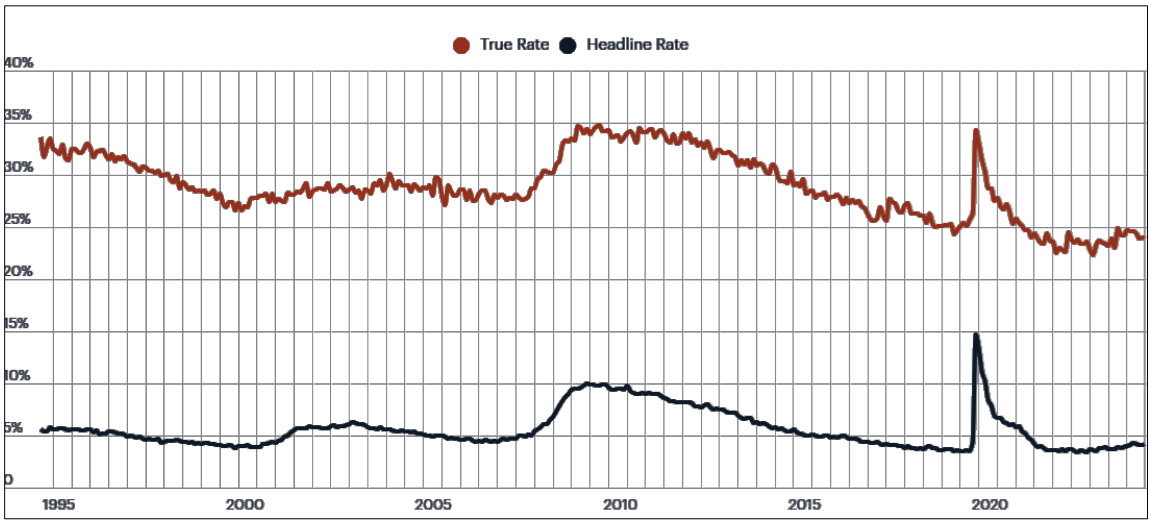

Figure 2. True vs. Reported Headline Rates of Unemployment.[35]

Paradoxically, this has occurred even though automation has been introduced into every possible process to increase resilience in the face of labor shortages and increasing labor costs. This confluence of factors has caused a perplexing situation in which businesses do not have enough people to perform some functions and need fewer people to perform others: the World Economic Forum states that 39 percent of workers' core skills

[34] Ludwig Institute for Shared Economic Prosperity, "True Rate of Unemployment," October 2024, https://www.lisep.org/tru.

[35] Source: Ludwig Institute for Shared Economic Prosperity.

are expected to change over the next five years.[36] Additionally, advances in automation, artificial intelligence, and robotics are straining employee relationships with their employers and altering the work being performed.[37] A clear indication of this conflict is the 2024 port strike affecting the East and Gulf Coasts spurned by the attempts of critical infrastructure operators to automate seemingly mundane activities.[38] At the macro level, this does not change the day-to-day reality that thousands of people are involved in the maritime transportation delivery pipeline, but it does portend significant changes to the economic systems of those insiders performing the labor. From the adversarial perspective, the day-to-day experience of aviation workers, and all employees, matters. Considering the act of self-policing, there are and may be fewer people to watch, certainly; however, the people who could otherwise watch also have more to do and are thus less capable of self-policing their ranks.

The issue of automation is more acute in the aviation industry. While substituting human beings for technology will, by definition, reduce the number of insiders, such efforts will likely inhibit social control and cause intra-group conflict in the short term by straining aspects of employee-employer relationships and reducing individual economic security and may increase the overall risk posed by AIP. Growing dissatisfaction and lower-than-average compensation drive aviation worker disengagement. U.S. aviation workers are doing more with less support and have less margin for error. This is a general theme affecting broader industries, however, workers in the aviation environment are being optimized, competing with machines and business automation, being forced to work with machines and automated processes, being measured strictly against performance outcomes, and are doing so at lower-than-average rates of pay and without common benefits such as paid time off.[39] Relative shortfalls in compensation and recognition must be highlighted

[36] Saadia Zahidi, *Future of Jobs Report 2025* (Geneva: World Economic Forum, 2025), 33, https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf.

[37] Zahidi, 6.

[38] Andrea Hsu, "Strike Ends for Dockworkers," NPR All Things Considered, October 4, 2024, https://www.npr.org/2024/10/03/nx-s1-5139450/dockworkers-port-strike-deal.

[39] Karla Walter and Aurelia Glass, "Airport Service Workers Deserve Good Jobs," Center for American Progress, March 7, 2023, https://www.americanprogress.org/article/airport-service-workers-deserve-good-jobs/.

in the context of the macro-economic situation in the U.S. wherein significant inflationary pressure has reduced the buying power of wages faster than wage pressure has been able to respond. These factors combine to form a petri dish prepared to grow worker dissatisfaction, discontent, and disengagement, all of which contribute to, agitate, and empower AIP.

4. Inhibited Law Enforcement

Police and intelligence resources have challenging jobs that are more demanding today than ever. The labor issues affecting all sectors are especially acute for law enforcement: news coverage related to police action, resulting protests, and declining trust between communities and police organizations has made work in security riskier and less attractive, despite excellent compensation packages.[40] Serrato recently completed a holistic analysis of efforts to defund or unbundle policing from social issues and notes the impractical reliance on police to tackle and resolve complex and challenging social issues such as drug abuse, homelessness, and petty crimes.[41] These issues spill into airports and distract law enforcement and intelligence resources from their mission. While much effort is being made to repair the relationships between law enforcement and served populations, and police organizations and politicians have identified the unsustainability of policing in this environment, there is no immediate solution to unbundle the security mission from the social mission. The increasing complexity of police work will continue to make their role in insider threat mitigation more difficult and inevitably less effective.

5. Modern Airports

The increasing interconnectedness and commercial diversity of the aviation environment will also further challenge insider threat mitigation. A modern commercial airport is a collection of spaces specialized for various functions and uses. The last two

[40] Tim Newburn, "The Inevitable Fallibility of Policing," *Policing and Society* 32, no. 3 (2022): 447, https://doi.org/10.1080/10439463.2022.2037557.

[41] Gerardo H Serrato, "Defund or Unbundle the Police? A Strategy to Enhance the Reputation and Morale of Law Enforcement Agencies in The United States." (master's thesis, Naval Postgraduate School, 2022), 31.

decades have seen increased investment and the diversification of that investment in airport spaces, particularly at larger airports.[42] Modern airports often feature extensive services, lounges, shopping, and entertainment offered in secured and public spaces. Airports are integrating more completely into commercial and transportation systems to increase profitability, acquire prestige, and compete effectively in national and international markets. Airports are also being connected to mass transit systems in many regions such as Washington, DC.[43] In addition to becoming more complex, airports are now becoming features of more complex and valuable systems and, therefore, may be more valuable and vulnerable targets to opportunistic AIP.

Despite labor shortages, new business opportunities and more diverse commercial offerings will attempt to attract additional employees, increasing the pool of individuals who may become adversarial, and provide adversaries additional opportunities to establish trust in the aviation environment. Perhaps no other U.S. airport is a demonstration of this march into modernity than the Los Angeles International Airport, which is investing $15 billion to complete many improvements to virtually all aspects of the airport: airfield, automated people movers, central rental car lots, connection to surface mass transit, vastly improved concessions, additional gates, and new terminals, illustrated in Figure 3.[44]

[42] Vik Krishnan et al., "Turning on the Revenue Tap: How U.S. Airports Could Make the Most of Additional Liquidity," Business and Lobby Group, Mckinsey, February 8, 2022, https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/turning-on-the-revenue-tap-how-us-airports-could-make-the-most-of-additional-liquidity.

[43] Jordan Pascale, "What You Need to Know About Taking the Silver Line to Dulles," DCist, accessed January 15, 2025, https://dcist.com/story/22/11/02/what-you-need-to-know-about-taking-the-silver-line-to-dulles/.

[44] Tyler Evains, "LAX Transformation More than Halfway Done, Last Phase Underway," *Daily Breeze*, January 28, 2023, Electronic edition, sec. News, https://www.dailybreeze.com/2023/01/28/lax-transformation-more-than-halfway-done-last-phase-underway/.

Figure 3. Construction of Mass-Transit Linkages at Los Angeles International Airport Demonstrating Increasing System Complexity.[45]

6. Increasing AIP Capability

The threat from AIP is increasing due to the convergence of technological advancements, workforce dynamics, and evolving socio-political factors. Technological advancements, such as expanded access to sensitive information through networked systems and access to terrorist tradecraft through the internet and particularly generative Artificial Intelligence (AI) have lowered the barriers for insiders to exfiltrate, sabotage, or misuse critical data. Moreover, the proliferation of AI and automation has amplified the potential impact of insider actions, as a single compromised system can now disrupt entire operations, or a simple query can easily obtain the foundational instructions for explosives or narcotic synthesis.[46] This risk is compounded by the growing adoption of remote and hybrid work models, which create challenges in maintaining consistent oversight and identifying behavioral anomalies that may signal insider threats. Organizations are

[45] Source: Engineering News-Record, "LAX People Mover Passes Construction Milestone," Transportation, May 11, 2022, https://www.enr.com/articles/54095-lax-people-mover-passes-construction-milestone.

[46] Clarisa Nelu, "Exploitation of Generative AI by Terrorist Groups," International Centre for Counter-Terrorism – ICCT, June 10, 2024, https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

challenged to recognize these trends and enhance their detection, deterrence, and response measures, and to adapt to this evolving threat landscape.

C. RESEARCH QUESTIONS

This thesis attempts to answer the following research questions:

1. Primarily, to what extent can the principles of behavioral economics, classical economics, and other prominent psychological theories be applied to insider threat models and countermeasures, and what novel decision-making (or resource allocation) insights might such application offer?

2. Secondarily, and in relation to behavioral economics, when considering the perspectives of agents within critical infrastructure systems, what barriers and factors contribute to investment decisions and as an extension, the formation of AIP mitigation strategies and the deployment of countermeasures at airports and other critical infrastructure?

3. Additionally, do common AIP countermeasures perform in a manner consistent with expectations derived from economic models and other significant psychological theory?

D. RESEARCH DESIGN

This thesis uses a blend of counterfactual analysis, thought experiments, and sequential games to explore the aviation industry's efforts to mitigate insider risk in the context of economics, particularly the themes described by Prospect Theory to answer the stated research questions. As Booth explains in his analysis of management decisions and strategy, counterfactuals provide an attractive opportunity to focus upon and perhaps uncover causality within events and games, notably in economics and historical study, despite their occasional lack of empirical rigor.[47] As noted historian Bulhof describes, counterfactual analysis is everywhere; it permits us to learn from past decisions and

[47] Charles Booth, "Does History Matter in Strategy? The Possibilities and Problems of Counterfactual Analysis," *Management Decision* 41, no. 1 (2003): 100, https://doi.org/10.1108/00251740310445545.

consists of a defined conditional statement: if p, then q.[48] This conditional statement permits the assessment of the necessary result of a defined path and its parameters. One of the world's foremost historians, Niall Ferguson, summarizes two methods for counterfactual analysis: the use of thought experiments and the imagination to consider alternative paths in specific scenarios and those used for economic analysis.[49] AIP are the subject of this thesis, and each adversary is set upon a decision path wherein causes and results may be considered virtually. Therefore, analysis of attack pathways given past and existing policies and the pressures new policies will exert is of obvious importance. This thesis will suppress wildly speculative, imaginary constructs that have detracted from some efforts using this method and will instead draw from actual events and cases composited through thought-experiment subsequently captured within games.

The case study will occur through a comprehensive understanding of three high-profile and publicly available incidents of insider criminal activity at commercial airports over the last 10 years. Prior research and public search engines will be used to survey recent history for compelling cases. These cases will be assessed to determine how the AIP tactics identified could be further weaponized by AIP. The cases will be composited and used to develop a thought experiment. The resulting simplified scenario will be primarily analyzed through sequential gaming and mechanism design lenses with strictly controlled parameters and inputs. Through this process, discussion of the tactics deployed in the composite scenario wherein an insider adversary with near-perfect knowledge will aspire to attack aviation assets. Finally, this thesis will develop and propose a means to quantify risk reduction for AIP countermeasures in the context of comprehensive insider threat mitigation strategies and socio-economic theories.

The Theory of Mechanism Design (MDT) is particularly applicable in reviewing insider risk management and decision-making in the context of deployed countermeasures. MDT recognizes and explores the relationship between individual decision-makers and

[48] Johannes Bulhof, "What If? Modality and History," *History and Theory* 38, no. 2 (1999): 145–48, https://www.jstor.org/stable/2505660.

[49] Naill Ferguson, *Virtual History: Alternatives and Counterfactuals* (London: Macmillan, 1997).

individuals with unique and varying information levels through game theoretical tools.[50] This theory permits the evaluation of agent decision-making within an institution's design: the evaluation of AIP decision-making in the context of critical infrastructure security systems. Though this general framework is often used to model complex interactions between decision-makers in economic environments, its use of network modeling and mathematical evaluation should be capable of producing precise and probabilistic assessments.

Prominent decision-making and psychological theory spanning the field of behavioral economics and decision-making will be applied to countermeasure selection to make sense of countermeasure effect on AIP and assess the sometimes counter-intuitive results of such enterprises. As informed by these theories, the counterfactual analysis featured in this thesis attempts to root the process of AIP countermeasure selection in empirical study. Through this multi-disciplinary approach, this thesis will step away from pure thought experiments and shield itself from accusations of parlor games. While attempting to answer the research questions, it will also:

- research and examine cases of AIP activity in the aviation environment to catalog and understand the real and counterfactual influence of mitigation measures on AIP;
- identify opportunities to improve the performance of existing and proposed mitigation measures, including the physical screening of aviation workers at commercial airports; and
- propose a novel framework with which security professionals can more adeptly understand the theoretical underpinnings of their adopted insider threat countermeasures and inform related strategic decision-making within the contexts of comprehensive insider threat mitigation endeavors.

[50] Matthew O. Jackson, "Mechanism Theory" (working paper, California Institute of Technology, 2003), 4, http://www.ssrn.com/abstract=2542983.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

Insider threats continue to pose a grave concern to critical infrastructure, particularly the nation's 434 commercial airports, despite the airports' wide array of mitigation tactics such as criminal history and terrorist contact vetting, screening of employees, and reporting of insider threats, all of which are primarily rooted in traditional utilitarian and crime control theories. This multidisciplinary literature review delves into contemporary academic discussions of and recommendations for insider risk mitigation terms, tactics, and strategies from published research concerning crime control, behavioral economics, and applications of theory in critical infrastructure protection (CIP) practices demonstrating general academic concurrence around crucial terms, insider threat mitigation strategies, available mitigation tactics, and specific areas of insider threat mitigation controversy. It explores available frameworks for determining application efficacy and universality. Finally, this review explores how academia has viewed adversarial insider personnel (AIP) decision-making, creativity, and response to countermeasures through the lenses of behavioral economics and traditional psychological concepts. As it endeavors to discover applicable knowledge and gaps in the academic body, the literature illustrates that there are many tools and frameworks for assessing insider threat mitigation tactics. Furthermore, despite a wealth of theoretical insight into adversarial development and decision-making and calls for comprehensive insider threat mitigation strategies, there is a conspicuous lack of research to develop a quantifiable framework to facilitate and inform insider threat mitigation strategies.

A. CONCURRENCE REGARDING INSIDER THREAT MITIGATION STRATEGY

A significant body of research focuses on the task of identifying insider threats. Contributing to the Insider Risk Group, LLC, psychologists Mark Lenzenweger and Eric Shaw applied research, training, and experience in the field of intelligence to develop a "Critical Pathway to Insider Risk" (CPIR), which they describe as a flexible and adaptive

framework to assess individuals using a "multifactorial model of accumulating risk."[51] The CPIR is a construct of observed traits and factors from previous insider incidents, organized notionally into a pathway. The primary conceptual vulnerability with CPIR and other similar frameworks, such as the Federal Bureau of Investigation's Pathway to Violence Model, is that such frameworks are intended to provide opportunities for intervention but must rely upon available information.[52] Information is typically widely available after AIP activity has been discovered; information sources multiply after a physical attack or arrest. However, before probable cause is established, many plots and threat scenarios do not provide immediate access to information.

This dearth of actionable threat indicators and information has hypothetically been solved by so-called ongoing evaluation, continuous vetting, or risk assessment. In these models, individuals work with trained investigators at regular intervals to assess psychometrics associated with insider risk, providing a baseline for individual attributes facilitating subsequent observation and analysis.[53] This approach raises immediate concerns, though none mark the concept as completely implausible. First, psychological evaluation of this quality and frequency is taxing and expensive for businesses engaged in infrastructure operations, relegating the method to only the highest-value targets. Second, organizations will likely find routine intrusive investigation distasteful at the least and socially toxic given norms related to privacy and persistent stigma associated with mental health care and illness. Therefore, while promising, CPIR and recurring psychological evaluation applications appear limited to education, post-incident investigation, extremely high-value insiders, and ongoing academic endeavors.

Likely due to the multi-faceted tasks related to detecting insider threat indicators and predicting AIP activity, the literature demonstrates that researchers have generally

[51] Mark F. Lenzenweger and Eric D. Shaw, "The Critical Pathway to Insider Risk Model: Brief Overview and Future Directions," *Counter-Insider Threat Research and Practice* 1, no. 1 (August 2, 2022): 2, https://citrap.scholasticahq.com/article/36186.

[52] Robert A. Fein, Bryan Vossekuil, and Gwen A. Holden, "Threat Assessment: An Approach to Prevent Targeted Violence," *Research in Action*, July 1995, 2–4, https://doi.org/10.1037/e517592006-001.

[53] Giliam De Valk, "On Screening and the Insider Threat – A Methodological Exploration," *National Security and the Future* 20, no. 1–2 (January 9, 2020): 47, https://doi.org/10.37458/nstf.20.1-2.5.

found comprehensive insider threat mitigation strategies, those which address different aspects of insider formation and activity, are critical and that no one-size-fits-all approach to selecting and applying insider risk mitigation tactics. Contemporary research, such as that developed by Black, has argued that additional initial vetting and background investigation are central to lowering insider infiltration.[54] Nick Catrantzos produced an influential vision of creating environments where insider threats, AIP in this thesis, cannot hide extending on Black. He argued that a "No Dark Corners" approach to insider threat mitigation and CIP, that the culture, practices, and design of workspaces should be modified to reduce the opportunities for insider ideation and operation of AIP in critical spaces.[55] Still others propose that critical infrastructure operators should pay more attention to insider threat mitigation tactics such as variations of physical screening, awareness training for insider threat detection and reporting, and continuous vetting of transportation workers.[56] Brian Bean reiterated that there is no standard approach to insider threat mitigation. Still, he argues that any successful program must take steps to prevent, deter, and detect insider threats in the aviation environment.[57] There are few criticisms of tactics in the research; many tactics have been explored, but no single tactic is a silver bullet. This thesis will explore the gaps and look beyond the questions of what- and how-programs should be built.

B. THE PROLIFERATION OF TACTICS

The proliferation and multiplication of options to counter insider threats, combined with absent or ineffective tools to evaluate risk mitigation, cost, and benefit, obscures a clear path to standards or collective agreement within the critical infrastructure community. The Safe Skies organization, a non-profit aviation and transportation research authority, has created a broad review of options and recommendations focused on the mitigation of insider risk, which provides full life cycle consideration of potential AIP to include

[54] Alan Black, "Managing the Aviation Insider Threat" (master's thesis, Naval Postgraduate School, 2010), 38, https://hdl.handle.net/10945/5039.

[55] Catrantzos, "Insider Threat," 66.

[56] Mathew, "Insider Threat," 70.

[57] Bean, "Mitigating Insider Threats in the Domestic Aviation System," 70–72.

background information vetting, suspicious activity reporting, physical screening, derogatory intelligence development, investigation, behavioral monitoring and screening technology, and employee engagement and development.[58] These recommendations defer tactical and strategic decisions regarding insider threat mitigation to local leadership and regulatory bodies without providing a useful frame with which to inform them.[59] Despite its success in summarizing and presenting many options, the reporting does not present precise tools to evaluate the combined effectiveness of selected tactics, nor are tactics yet proven feasible through cost-benefit analysis.[60] Further, government researchers have presented simplified and, at times, limited views on practical approaches to insider threat mitigation in the aviation sector while assessing a small collection of contemporaneous insider incidents, and policy specialists have been quick to group concerns and action areas such as vetting, mental health, awareness and reporting, access controls, and surveillance in an attempt to grasp and communicate threat indicators, but fall short of describing how mitigation efforts work together to detect and deter AIP.[61] It is clear that there are many security tactics and tools to organize them yet few tools to examine and understand their application strategically. Researchers in the financial and information risk management sectors have struggled with this reality as well. They have consistently identified the need to assess AIP mitigation benefits against various business costs using reliable modeling.[62] Current assessment options provide for a systematic approach to mitigation tactic implementation decisions; however, without frameworks for accurately gauging the cost-benefit for each option or education on which options should be paired with others and the peculiarities of the institution being protected, decisions are left to leadership intuition or,

58 Grizzle, *Insider Threat Mitigation at Airports*, 1–99.

59 This statement does not imply that the Safe Skies organization is at fault in any way. It would appear that they are playing a vital and intelligent role in communicating valuable information to stakeholders in the aviation community and beyond.

60 Grizzle, *Insider Threat Mitigation at Airports*, 18.

61 Bart Elias, *Strange Occurrences Highlight Insider Threat to Aviation Security*, CRS Report No. IN10954 (Washington, DC: Congressional Research Service, 2018), 1–2, https://crsreports.congress.gov/product/pdf/IN/IN10954/2.

62 Matt Bishop et al., "A Risk Management Approach to the 'Insider Threat,'" in *Insider Threats in Cyber Security*, ed. Christian W. Probst et al. (Boston, MA: Springer U.S., 2010), 125, https://doi.org/10.1007/978-1-4419-7133-3_6.

perhaps more troubling, based on raw cost alone. This landscape presents an opportunity for synthesis and to integrate comprehensive interdisciplinary strategies with aspects of existing risk-based and cost-benefit frameworks.

Though this thesis is focused on aviation CIP, insider threats are not exclusive to critical infrastructure. As such, several other sectors have worked to address insider threats in protected environments. Additionally, some tactics for insider threat mitigation are broadly applied to all potential threats. In the realm of counter-smuggling, U.S. Customs and Border Patrol (CBP) uses physical inspections to deter and detect adversarial operations. CBP focuses on ensuring that the goods and people entering the country are doing so according to law. For at least two decades, the CBP has worked to implement and adjust inspection programs through performance monitoring and adjustments to random inspection baselines to effectively perform their mission and assess the magnitude of the smuggling problem.[63] The use of physical inspection, particularly random physical inspections, in CIP environments, though not focusing on insider threats, provides insight into inspection effectiveness and support of its use.

Prisons and jails represent an informative analog for mitigating AIP risk in critical infrastructure environments. Both contexts provide assets that require protection, display perimeter security, and require a regulated membrane through which legitimate and illicit goods are transported. Prisons are also particularly representative analogs as they contain distinct populations of insiders, perhaps more distinct than in critical infrastructure environments, and a presumably adversarial-by-default insider constitution. Due to the issue presented by corrupt staff, the United Nations has published a template prison operations handbook focused on physical security, dynamic security, and intelligence with five standards pertaining to security officer integrity and random inspections of staff,

[63] Richard Stana, *Customs and INS: Random Inspection Programs Can Be Strengthened*, GAO-02-215R (Washington, DC: Government Accountability Office, 2001), 2, https://www.gao.gov/assets/gao-02-215r.pdf; Rebecca Gambler, *CBP Should Update Policies and Enhance Analysis of Inspections*, GAO-19-658 (Washington, DC: Government Accountability Office, 2019), 9–32, https://www.gao.gov/assets/710/700787.pdf.

physical spaces, and procedural audits.[64] Likewise, a publicly available, iterant, and perpetually draft assessment tool for understanding penal facility security produced by the Department of Justice illustrates the importance of insider threat awareness and detection through its assessment survey factors which include physical inspection baselines, higher-level random inspections, random physical space inspections, perimeter security, and other measures.[65] Recently, John Wooldredge reinforced the complexity but demonstrated the maturity of prison security in a comprehensive review of relevant literature indicating a very well-developed academic body considering crime control, cultural analysis, and social analysis of trends related to violence in prison environments, citing a perpetual need for more comprehensive frameworks to propel these issues toward modern solutions.[66]

C. UNDERSTANDING RISK AND POLICY IMPLICATIONS

Researchers have noted that opportunities exist to expand and enhance the authorities of some regulatory bodies to increase critical infrastructure operators' ability to detect and respond to insider threats, noting the human, sentient element of such adversaries and arguing for better human intelligence.[67] Bean observed that agencies and the government may lack the authority to engage in the most effective offensive measures relating to domestic intelligence collection, given current legal limitations.[68] Little controversy surrounds the idea that increased surveillance improves security, but

[64] United Nations Office on Drugs and Crime, *Handbook on Dynamic Security and Prison Intelligence* (Vienna: United Nations, 2015), 25,38,48,58, https://www.unodc.org/documents/justice-and-prison-reform/UNODC_Handbook_on_Dynamic_Security_and_Prison_Intelligence.pdf.

[65] This source discusses the search rates for employees, inmates, residential units, etc. Rod Miller and John E. Wetzel, "Jail Vulnerability Assessment: A Systems Approach to Improve Safety and Security" (working draft, Washington, DC, December 2008), 44, 52, 103, 155, 201, https://correction.org/wp-content/uploads/2014/10/Jail-Vulnerability-Assessment-JVA-Final-Draft.pdf.

[66] John Wooldredge, "Prison Culture, Management, and In-Prison Violence," *Annual Review of Criminology* 3 (2020): 182, https://doi.org/10.1146/annurev-criminol-011419-041359.

[67] Zachary D. Zeigler, "Leveraging DHS Assets: Potential for the Transportation Security Administration to Enhance U.S. Government Intelligence Capabilities" (master's thesis, Naval Postgraduate School, 2021), 10–11, https://hdl.handle.net/10945/68400.

[68] Bean, "Mitigating Insider Threats in the Domestic Aviation System," 12.

significant controversy surrounds the government's authority in this area.[69] Despite the potential complexity of implementing increased surveillance and the possible social cost associated with diluting privacy, the value that better intelligence provides to plot infiltration and insider threat mitigation, on the whole, cannot be overstated.

Available sources also indicate that regulatory intervention in the arena of CIP insider threat mitigation may not adequately articulate strategic guidance nor routinely communicate cost-benefit analyses, the absence of which has contributed to some resistance from critical infrastructure operators. For instance, in 2020 and 2021, the Government Accountability Office recommended that the Transportation Security Administration (TSA) improve its insider risk mitigation strategy and processes.[70] In response to this and other recommendations, the TSA required improved physical screening of aviation workers to reduce insider risk in 2023.[71] However, aviation operators and their representatives responded by objecting to the means and methods of these proposed mitigation efforts.[72] Security professionals agree that physical screening is effective for discovering and deterring illicit material, as it provides a means for detection and a link to punishment, yet disagree on the cost-benefit provided by specific procedures

---

[69] Jay Stanley, "How the TSA's Facial Recognition Plan Will Go Far Beyond the Airport," American Civil Liberties Union: News and Commentary, October 22, 2018, https://www.aclu.org/news/privacy-technology/how-tsas-facial-recognition-plan-will-go-far; Katherine LaGrave, "How TSA's 'Quiet Skies' Program Tracks U.S. Passengers," Condé Nast Traveler, July 2018, https://www.cntraveler.com/story/how-tsa-quiet-skies-program-tracks-us-passengers; Rebecca Beitsch, "House Approves Contentious FISA Bill in Bipartisan Vote," The Hill, April 12, 2024, https://www.aol.com/house-approves-contentious-fisa-bill-171241728.html.

[70] McNeil, *Aviation Security*, 37; Triana McNeil, *Airport Worker Screening: TSA Could Further Strengthen Its Approach to Estimating Costs and Feasibility of Security Measures*, GAO-21-273 (Washington, DC: United States Government Accountability Office, 2021), 15, https://www.gao.gov/assets/gao-21-273.pdf.

[71] David Pekoske, "2023 Year in Review: TSA Highlights a Year of Innovation and Improvements to Security Effectiveness, Efficiency and the Passenger Experience," Transportation Security Administration, January 12, 2024, https://www.tsa.gov/news/press/releases/2024/01/12/2023-year-review-tsa-highlights-year-innovation-and-improvements; David Pekoske, "2023 TSA Year in Review" (Transportation Security Administration, 2024), https://www.tsa.gov/sites/default/files/17228_info_tsa_2023_year_in_review.pdf; Homeland Security & Government Affairs, "Chairman Johnson Asks TSA for Solutions on Passenger Screening and Insider Threats," Majority News, June 7, 2016, https://www.hsgac.senate.gov/media/reps/icymi-chairman-johnson-asks-tsa-for-solutions-on-passenger-screening-and-insider-threats/.

[72] McNeil, *Aviation Security*; Daines, Steve and Zinke, Ryan, "Letter to TSA Regarding Aviation Worker-Screening Rule," August 23, 2023, 1–3, https://www.daines.senate.gov/wp-content/uploads/2023/08/2023.08.23_Letter-to-TSA-re-Aviation-Worker-Screening-Rule.pdf.

(electronic, pat-down, property searches, etc.). Such activity does result in the discovery of contraband, and screening is relatively easy to execute, manage, and track. In parallel, researchers such as Monica Whitty address the concept of physical pathway reduction as an attempt to provide a conceptual model for insider risk mitigation: fewer pathways should reduce risk.[73] This discourse and ongoing research reflects the collaborative friction experienced between academia, industry, regulatory, and legislative entities in identifying, communicating, and implementing initiatives focused on insider threat and AIP mitigation.

The broad literature indicates that regulatory and industry authorities in the aviation environment appear split over the technical aspects of insider threat mitigation measures and how they might be implemented. A specific area of controversy is the domestic application of aviation worker screening when compared to International Civil Aviation Organization (ICAO) Standards: TSA requires a minimum baseline of random physical aviation worker screening, while ICAO indicates all aviation workers are to be screened.[74] Qualitative research performed by Zeballos indicates that traditional security measures may result in the perception that a system is both more secure and more equitable; randomness may be an effective addition to or pivot from existing predictable security measures, particularly those focused on AIP; and that commercial airports are experimenting with random security measures.[75] Other applications have demonstrated that random inspections can improve safety performance without harming business interests.[76] The available literature does not provide a reliable means of quantifying the

[73] Monica T. Whitty, "Developing a Conceptual Model for Insider Threat," *Journal of Management and Organization* 27, no. 5 (2021): 927, https://doi.org/10.1017/jmo.2018.57.

[74] Aviation Security International Civil Aviation Organization, *Managing Insider Risks*, 01 ed. (Montréal: ICAO HQ, 2022), 1–3, https://www.icao.int/Security/Security-Culture/State%20and%20Industry%20Promotional%20Material/ICAO%20Pamphlet%20Managing%20Insider%20Risks.pdf; Airports Council International, "ACI-NA Position on TSA's Aviation Worker Screening National Amendment."

[75] Melina Zeballos et al., "Why and How Unpredictability Is Implemented in Aviation Security – A First Qualitative Study," *Heliyon* 9 (2023): 10, https://doi.org/10.1016/j.heliyon.2023.e13822.

[76] David I. Levine, Michael W. Toffel, and Matthew S. Johnson, "Randomized Government Safety Inspections Reduce Worker Injuries with No Detectable Job Loss," *Science* 336, no. 6083 (2012): 908,911, https://www.jstor.org/stable/41584864.

effect of deterrence, an essential aspect in this context, in security environments.[77] This perspective is critical when considering insider threat mitigation for CIP and provides insights into how insider threat countermeasures should be assessed and strategies constructed.

Evaluative frameworks for general risk management have driven much of the insider risk mitigation discussion despite significant disagreement between academics and practitioners regarding their application to specific risk problems. The Department of Homeland Security's (DHS) quasi-mathematical framework for risk calculation, *Risk = Threat x Vulnerability x Consequence,* is classically utilitarian.[78] The framework is reflected in TSA's layered security approach and the Safe Skies recommendations discussed earlier. Many agree that DHS' utilitarian approach permits policy-makers and practitioners to understand the inputs to risk more effectively and facilitate decision-making, though it may not be the ideal method for counter-terrorism and insider threat applications.[79] Hubbard, a risk management authority, expands on this criticism, concluding that the field has declared this approach to risk management harmful and that "these popular methods should not be used for decisions of any consequence."[80] Despite the ambiguity and argument between sources on risk valuation methodology, the formula illustrates complexities associated with defender decision-making. Given its inability to precisely quantify risk and the risk-reduction provided by a given tactic, this method of managing insider risk does not promote the adoption of specific tactics or comprehensive strategy. Furthermore, this methodology could be used to improperly justify mitigation efforts from the basis of risk control and intervention through reverse induction. Therefore, this risk valuation method does not support decision-making as a strategic cornerstone; in the absence of effective frames, no definitive strategy prevails.

---

[77] Zeballos et al., "Why and How Unpredictability Is Implemented in Aviation Security – A First Qualitative Study," 10.

[78] Rand Beers, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (Washington, DC: Department of Homeland Security, 2011), 20.

[79] National Research Council, *Review of the Department of Homeland Security's Approach to Risk Analysis* (Washington, DC: National Academies Press, 2010), 17, https://doi.org/10.17226/12972.

[80] Douglas W. Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It*, 2nd ed. (Hoboken, NJ: Wiley, 2020), 164.

D. DECISION-MAKING: PSYCHOLOGY AND BEHAVIORAL ECONOMICS

The literature strongly indicates that social psychology and behavioral economics offer insight into human behavior and decisions under risk. Self-Control and Social Control Theories offer psychological insights into the behavior of individuals who may act against their organizations. Beyond psychological frameworks, economic frameworks offer more precise insights into decision-making. Game theory provides methods to precisely evaluate complex problems while Rational Choice Theory and Prospect Theory offer two effective frames for understanding how individuals make decisions based on their perception of gains and losses. These theories offer value to understanding AIP and considering AIP countermeasures.

1. Decision Control: Self and Social Control

Self-control and *Social Control Theory* assesses the extent to which human bonding, development, and socialization affect the capacity of insiders to make decisions consistent with organizational and other social norms. Social Control Theory emphasizes that strong social bonds between individuals and family, work, and community serve as deterrents against deviant actions.[81] *General Crime Theory, Expanding on Self and Social Control Theory*, proposed by Gottfredson and Hirschi, posits that individuals with low self-control, described across "six essential dimensions: impulsivity, preference for simple tasks, risk-seeking potential, preference for physical (as opposed to mental) activities, self-centeredness, and finally, the possession of a volatile temper," are more prone to engage in impulsive or deviant behaviors, including actions harmful to organizations.[82] People with low self-control might disregard long-term consequences for immediate gratification, making them more susceptible to risky or unauthorized behavior within workplace environments. Both theories emphasize the role of external factors and social structures in influencing individual behavior, particularly in deterring criminality.

---

[81] Travis Hirschi, *Causes of Delinquency* (New Brunswick, NJ: Transaction Publishers, 2002), 4–12.

[82] Bruce J Arneklev, Lori Elis, and Sandra Medlicott, "Testing the General Theory of Crime: Comparing the Effects of 'Imprudent Behavior' and an Attitudinal Indicator of 'Low Self-Control,'" *Western Criminology Review* 7, no. 3 (2006): 42.

Recent work has endeavored to integrate principles from each into hybridized approaches, noting that self-control is not insular and may be affected by structural and social components. According to one of the conjectures regarding the connectedness of self-control to other aspects of control and identity, "self-control influences the quality of social ties over the life course."[83] This synthesis between Self and Social Control Theories considers adversarial behavior—to the extent that adversaries are not necessarily abnormal, even if delinquent from a criminalistic perspective, and are instead behaving in ways that are more indicative of normal decision-making given unique, lived circumstances. Applying these theories to adversarial insider threat mitigation involves leveraging the principles of deterrence, socialization, and enforcing norms to reduce the likelihood of malicious insider activities. However, it also demands the consideration of adversaries as individuals responding to stimuli from their organization's environment.

Social Control Theory seeks to understand and describe the role of social bonds and societal norms in regulating individual behavior. According to this theory, individuals who are committed to conventional societal goals, are involved in legitimate activities, and believe in the moral validity of socially or legally enforced rules may be inhibited from participating in anti-social or criminal behavior with strong attachments to others.[84] Therefore, delinquent behavior will result from weak bonds with family, friends, and other social membership groups including the organization. Applied to insider threat mitigation, Self and Social Control Theories suggest that strengthening employees' ties to the organization, strengthening the organization's culture to reflect more communal goals, and promoting a robust ethical culture would reduce the likelihood of AIP formation and action. When employees feel a sense of belonging and responsibility towards their organization, they are more likely to conform to its norms and less likely to engage in illicit or harmful behavior.

---

[83] Travis C. Pratt, "A Self-Control/Life-Course Theory of Criminal Behavior," *European Journal of Criminology* 13, no. 1 (2016): 139, https://doi.org/10.1177/1477370815587771.

[84] Barbara J. Costello and John H. Laub, "Social Control Theory: The Legacy of Travis Hirschi's *Causes of Delinquency*," *Annual Review of Criminology* 3, no. 1 (2020): 24–25, https://doi.org/10.1146/annurev-criminol-011419-041527.

Applied to insider threat mitigation, these theories suggest that fostering high self-control through training and reinforcing positive social ties within the workplace can reduce the likelihood of insider threats by first considering AIP mitigation at a personal and social level.[85] While self-control and social control theories offer a foundational understanding of deviant behavior, their application to insider threat mitigation may oversimplify the complexities of insider motivations in professional settings. Self-control Theory assumes that impulsive behavior primarily drives threats, potentially overlooking that many insider threats are premeditated and strategic rather than impulsive. For instance, research suggests that insiders often plan breaches over extended periods, sometimes out of calculated grievances or perceived injustices.[86] This premeditated nature may not align well with the impulsive, low self-control profile described by Gottfredson and Hirschi. Similarly, while useful in highlighting the deterrent power of social bonds, social control theory assumes that maintaining such bonds is a priority for potential insider threats. Some insiders may rationalize betrayal to achieve greater individual goals or satisfy personal grievances that overshadow any existing social bonds to the organization. Therefore, while these theories provide a basis, they may fall short in predicting the behavior of those driven by rational, calculated motives rather than low self-control or weak social attachments. These theories offer compelling means to understand human behavior and lay a psychological foundation that facilitates a transition into economic models by framing insider threats as "rational" decision-makers influenced by social incentives and personal self-regulation.

The literature also suggests that the interactions of groups and the influence that groups have on individual behavior is another important psychological consideration when seeking to understand AIP. Social Identity Theory, developed by Tajfel and Turner, explains how individuals derive part of their self-concept from group memberships, leading

[85] Robert Willison and Merrill Warkentin, "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* 37, no. 1 (March 2013): 14, https://doi.org/10.25300/MISQ/2013/37.1.01.

[86] Eric Shaw, Keven Ruby, and Jerrold Post, *The Insider Threat to Information Systems*, vol. 2–98 (Washington, DC: Department of Defense Security Institute, 1998), 1, https://homes.cerias.purdue.edu/~mkr/sab.pdf.

them to act in ways that favor their in-group over out-groups.[87] In the context of insider threats, fostering a strong, positive organizational identity can reduce the appeal of actions that would harm the organization, as employees are less likely to act against a group they identify with and support.[88] Although Social Identity Theory offers valuable insights into understanding and building organizational loyalty, its application to insider threat mitigation may be overly optimistic. Social Identity Theory posits that a strong group identity reduces negative behavior toward the in-group, assuming employees uniformly identify with the organization. However, organizational identity is often complex and multifaceted, particularly in large, diverse workplaces. Employees may identify more strongly with their specific team or profession than with the organization as a whole, potentially fostering sub-groups that prioritize their own self and group interests over their host organizations.[89] Additionally, Social Identity Theory may not adequately address insiders who engage in malicious activity due to strong, competing identities outside the workplace, such as ideological or financial affiliations that could drive them to act against the organization's interests. Despite these counterarguments, it is generally believed that building stronger organizational identity through recognition programs and corporate identity-development programs may mitigate insider risks by better aligning employee loyalties with organizational goals.

2. Economic Decision-Making: Games, Rational Choice, and Prospects

A review of economics literature more granularly informs an understanding of how decisions are made to optimize gains. Economics as a field of study has considered risk and threats for hundreds of years. Modern Game Theory was set forth by von Neumann and Morgentsen's *The Theory of Games* in 1944; its roots can be traced back to at least the 18th-century minimax problem assessed by Waldegrave and Montmort, providing the basis

[87] Henri Tajfel and John Turner, "An Integrative Theory of Intergroup Conflict," in *Organizational Identity*, ed. Mary Jo Hatch and Majken Schultz (Oxford, UK: Oxford University Press, 2000), 33–40, https://doi.org/10.1093/oso/9780199269464.003.0005.

[88] Tajfel and Turner, 36.

[89] Blake Ashforth and Fred Mael, "Social Identity Theory and Organization," *The Academy of Management Review* 14, no. 1 (1989): 30–34, https://doi.org/10.5465/AMR.1989.4278999.

for expected utility as a means of minimizing losses and maximizing gains.[90] In 1950, Nash developed proofs that in finite games rational players will find and adopt either pure strategies, or one dominant course of action as defined by the game, or mixed strategies, distributions of defined options to provide the highest likelihood of optimal gain in order to optimize outcomes.[91] Subsequent researchers have introduced greater capability and specificity to the mathematical modeling of decision-making, applying these methods to epistemic modeling, evolutionary biology, and other challenging problems to provide frameworks in which entities can inform sequential decisions under varying information availability to compete and collaborate towards relative gains.[92] The analysis of games continues to offer new tools and lenses to assess individuals' actions and the effectiveness of tools and system designs in various applications, including political science and homeland security studies.

Games have been used broadly and pervasively to simplify and understand many types of problems, though not every issue can be suitably reduced to games. Researchers routinely note that game theory can be applied to a variety of situations wherein scenarios can be reduced to models that feature strategic interactions, conflicting interests, rational behavior, and well-defined payoffs. Many of these problems are quite practical, such as using models to understand energy markets and work toward more efficient and fair energy trading and distribution systems by informing incentive-controlled markets.[93] Further demonstrating games' adaptability to diverse research areas, even practical areas such as project management have been effectively explored as a rich environment for game theoretical exploration. To this end, specialized theories have emerged, including the

[90] W. A. V. Souza and M. C. Malavazi, "Game Theory: An approach through history and its applications," *Scientific Electronic Archives* 12, no. 1 (February 4, 2019): 3–4, https://doi.org/10.36560/1212019642.

[91] John F. Nash, "Equilibrium Points in N-Person Games," *Proceedings of the National Academy of Sciences of the United States of America* 36, no. 1 (1950): 2, http://www.jstor.org/stable/88031.

[92] Manfred J Holler, "Classical, Modern and New Game Theory" (working paper, Yale Law School, August 2001), 20–28, https://law.yale.edu/sites/default/files/documents/pdf/holler.pdf.

[93] Aviad Navon et al., "Applications of Game Theory to Design and Operation of Modern Power Systems: A Comprehensive Review," *Energies* 13, no. 15 (January 2020): 17–20, https://doi.org/10.3390/en13153982.

Bilton and Cummings Hypothesis, demonstrating that game theory improves academic analysis of agents involved in project management.[94] Finally, to demonstrate its broad application, game theory was even used as an exploratory tool in moral philosophy as early as 2004.[95] While the broad application of game theory to philosophical areas of study requires extreme care to ensure that the conditions are well-defined, the application of game theory to security games of all kinds is thoroughly demonstrated.

Mechanism Design Theory (MDT) is a subset of games intended to more narrowly facilitate the creation of optimized systems by focusing on institutional modification, resulting in optimized payoffs (rewards or changes to net valuation – decision utility) to individual agents. This optimization is quantified in a Social Choice Function. Economists Bergemann and Välimäki apply the concepts from MDT alongside behavioral economics and classic game theory, such as forward-looking agent models with dynamic private costs and known quasi-linear payoffs to evaluate markets.[96] Forward-looking agent models with dynamic private costs and quasi-linear payoffs enable a nuanced evaluation of markets by capturing agents' evolving individual costs, future-oriented decision-making, and balanced preferences between financial gains and personal or social risks. As seen in many MDT models, perfect collaboration seems impossible between presumably selfish security and AIP agents in a security game. However, MDT features offer tremendous value to adversarial-defender models wherein AIP and security agents are forward-looking and experience dynamic costs. Auction and market games featuring incomplete information and dynamic systems seem adaptable for use in understanding insider risk as a market. Security games produced within MDT, wherein incentives and penalties are the tool of the security decision-maker and are selectively applied, may enrich understanding of current

[94] Mahendra Piraveenan, "Applications of Game Theory in Project Management: A Structured Review and Analysis," *Mathematics* 7, no. 9 (2019): 2,31, https://doi.org/10.3390/math7090858.

[95] Steven T. Kuhn, "Reflections on Ethics and Game Theory," *Synthese* 141, no. 1 (July 2004): 2, https://doi.org/10.1023/B:SYNT.0000035846.91195.cb.

[96] Dirk Bergemann and Juuso Välimäki, "Dynamic Mechanism Design: An Introduction," *Journal of Economic Literature* 57, no. 2 (June 2019): 235–36, 263, https://doi.org/10.1257/jel.20180892 A Social Choice Function is an equation that describes the activity of a system in a manner that optimizes payouts for all agents, thus the equation describes an optimized scenario based on individual choices made en masse by each agent. .

systems and compel inductive analysis of security systems intended to mitigate and shift risk away from essential assets.

MDT has been applied as a means to understand various market systems and is adaptable to security games. MDT has been applied to a variety of systems' engineering problems. Without explicitly naming MDT, Huang discusses the application of incentives fundamental to MDT as a moderator of insider threat detection and deterrence in network environments; specifically, the research claims to better align the objectives of insiders and defenders through the implementation of incentives based on network design.[97] Process and system engineers leverage mechanism design, claiming that MDT provides a valid tool to optimize many systems, including security systems, ensuring the fewest resources are used to accomplish common goals wherein independent system participants each have varying degrees of information with which to inform their actions in the model. An example would be in the design of systems that incentivize investment in baggage screening equipment across airports.[98] In such research and applications, regulatory pressure or tax incentives might be used as an externality intended to modify agent behavior in games and optimize security performance across a transportation system.

MDT has not been applied to attacker-defender games in any notable way and are not perfect for every application, though its previous applications demonstrate potential value in security games. Mookherjee and Tsumagari note that institutions featuring decentralized and incomplete communication require increased assumption and heavier communication costs (loss of efficiency) when agents choose a mechanism or choose to participate in the system.[99] This example demonstrates systems that feature fewer

[97] Linan Huang and Quanyan Zhu, "Duplicity Games for Deception Design with an Application to Insider Threat Mitigation," *IEEE Transactions on Information Forensics and Security* 16 (2021): 3–7, https://doi.org/10.1109/TIFS.2021.3118886 A duplicity game is a strategic scenario where players use deception—such as feigned cooperation, misinformation, or hidden intentions—to gain an advantage, creating a setting of compromised trust where participants navigate layers of truth and lies.

[98] Ioannis Vasileios Chremos and Andreas A. Malikopoulos, "Mechanism Design Theory in Control Engineering: A Tutorial and Overview of Applications in Communication, Power Grid, Transportation, and Security Systems," *IEEE Control Systems* 44, no. 1 (February 2024): 30–34, https://doi.org/10.1109/MCS.2023.3329919.

[99] Dilip Mookherjee and Masatoshi Tsumagari, "Mechanism Design with Communication Constraints," *Journal of Political Economy* 122, no. 5 (October 2014): 25, https://doi.org/10.1086/676931.

structures, and MDT is less influential. Given that MDT requires stable structures within which to introduce influence, this observation is logical. This theory is potentially important to the discourse surrounding insider threat mitigation, as systems and agents are burdened by deciding when and how to invest resources to protect agents, and larger authorities are responsible for setting institutional requirements, presumably with frugality in mind. Though not ideal for every application, MDT is a promising theoretical foundation for the development of security games involving insider threat mitigation in critical infrastructure where stable policy environments exist to propagate MDT parameters.

Fundamental to all games is the expectation that agents will act in their best interest and seek strategies to optimize their gains and minimize their losses. Rational Choice Theory is a dominant extension of economics that intends to describe how agents work to determine their best strategies (choices) to maximize returns, extending Subjective Expected Utility Theory. Bounded rationality further extends this framework to explain the growing discrepancy between how Rational Choice Theory predicts strategic selection and decades of empirical evidence; as such, Rational Choice Theory was developed further to incorporate limited information and human capacity to integrate information, thus bounding rational choice.[100] Noted social scientist Herbert Simon describes bounded rationality as a "choice that takes into account the cognitive limitations of the decision-maker."[101] Key challenges persist in this field of study, including the issue of generating alternative choices, uncertain reactions to alternative choices and new choice parameters, and testing this theory in a variety of applications in the real world.[102]

Rational Choice Theory is a well-established economic position often applied to practical concerns that explore human limitations while illustrating perfect calculation. This theoretical approach regarding decision-making influences the most traditional

[100] Riccardo Viale, Shaun Gallagher, and Vittorio Gallese, "Bounded Rationality, Enactive Problem Solving, and the Neuroscience of Social Interaction," *Frontiers in Psychology* 14 (2023): 2, 7, https://doi.org/10.3389/fpsyg.2023.1152866.

[101] Herbert A. Simon, "Bounded Rationality," in *Utility and Probability*, ed. John Eatwell, Murray Milgate, and Peter Newman (London: Palgrave Macmillan UK, 1990), 15, https://doi.org/10.1007/978-1-349-20568-4_5.

[102] Viale, Gallagher, and Gallese, "Bounded Rationality, Enactive Problem Solving, and the Neuroscience of Social Interaction," 7.

options for threat mitigation. According to Rational Choice Theory, the traditional premise is that individuals will opt for the course of action that they believe will provide the most significant benefit at the lowest cost. Individuals will assess their options and make selections based on value given sufficient time and available information. Under this premise, insiders will proceed with malicious activities if they *perceive* the rewards—such as financial gain or personal-social satisfaction—to be greater than the risks of being punished. This decision-making process can be influenced by introducing incentives to interfere with or even shape it.

In the context of AIP and other threat mitigation, Rational Choice Theory has generally been applied and tested within the fields of criminology in decision-making. A strong argument can be made that criminology is not decision-making and that criminals are not insiders, and as such, this theory should not be represented in this research. This argument is strong in that there are nuances between insider threats in a corporate or government environment and criminals walking the streets. However, this theory is important. It is a dominant theory alongside crime control and has worked its way into all manner of corporate policy; think about auditing and red teaming practices in any law or tax firm. This theory has been well-studied in applications of white-collar crime. Such applications are very similar to insider threats and AIP. Though not *necessarily* criminal, AIP often engage in criminal activity, providing a sufficient overlap to consider AIP as a subset of criminals. Suppose one was to view criminality as the oldest insider threat to civilization. In that case, Rational Choice Theory provides insight into even the most ancient regulations such as the Code of Hammurabi and its many derivations, wherein criminal activity presumably resulted in a clear deterrent response.[103] Rational Choice Theory provides a significant window into decisions involving risk from a human and behavioral economics perspective.

Whereas Rational Choice Theory attempts to describe differences between ideal outcomes and empirical observations of human choice thorough bounding, Prospect

[103] Michael S. Proctor, "The Deterrent Effect of the Death Penalty: A Rational Choice Case Study" (PhD diss., University of Arizona Global Campus, 2021), 35–40, https://www.proquest.com/docview/2566283818.

Theory more elaborately, and perhaps accurately, explains how individuals make decisions in risky scenarios. Prospect Theory elicits themes that may dramatically enrich models depicting individual and group decision-making in game-based valuations of security tactics, among many other areas, deployed to aggravate AIP. In addition to bringing economic, physiological, and psychological elements to bear, Prospect Theory describes two main components of interest: a two-stage decision process and the use of biases and frames influencing perceptions of gains and losses. Prospect Theory has been extensively challenged, and it has been demonstrated to be an effective, though imperfect, model for understanding and, at times, predicting human decisions in economic and other environments. As Tversky and Kahneman note in their original presentation of Prospect Theory, the relevant concepts of human decision-making likely have consequences in other areas.[104] The application of Prospect Theory has been demonstrated in the context of homeland security by research assessing terrorists' choice of attack method, concluding that analysis of terrorist behavior is more effective from behavioral economics frameworks than methods focused purely on classical utility theory.[105] These areas may be of value in security modeling and the conceptual understanding of insider threats for security professionals and researchers, as Prospect Theory models may illustrate the complexity of adversarial decision-making in a more nuanced fashion.

Research regarding the mechanistic and physiological functions of the brain supports the central tenets of Prospect Theory, bounded rationality, and behavioral economics. The continually developing physiological understanding of how the brain works, specifically the probabilistic understanding of choice and thinking systems common to humans, supports the two-step process described by Tversky in Kahneman in the 1970s and the 1990s.[106] Glimcher and Fehr conducted novel research using Magnetic Resonance Imaging under controlled experimentation which reinforces the observations of decisions

[104] Kahneman and Tversky, "Prospect Theory," 26.

[105] Peter J. Phillips and Gabriela Pohl, "Prospect Theory and Terrorist Choice," *Journal of Applied Economics* 17, no. 1 (May 2014): 156, https://doi.org/10.1016/S1514-0326(14)60006-4.

[106] Kahneman and Tversky, "Prospect Theory," 12; Amos Tversky and Daniel Kahneman, "Advances in Prospect Theory: Cumulative Representation of Uncertainty," *Journal of Risk & Uncertainty* 5, no. 4 (October 1992): 299, https://doi.org/10.1007/BF00122574.

under risk, noting that neural complexes work in tandem to support efficient decision-making processing, such as using heuristics, biases, and frames to reduce cognitive load during risky decision-making into manageable chunks of information.[107] Various psychologists, economists, neurologists, and other researchers have criticized attempts to apply this research, in its current state, to normative modeling, noting that individual variations, unique physiology, and emotional context play a significant role in decision-making processes.[108] The capacity for models and frameworks to simplify human decision-making and behavioral observations should not be ignored nor overly emphasized. Models are useful in understanding complex problems, but they remove nuance from the analysis by their nature. The subject of this thesis at its most basic level is decision-making. The synthesis of this emerging understanding and research still lends credibility to the fundamentals of behavioral economics and, more importantly, provides additional insight into how human beings choose between hazardous and valuable prospects.

Concepts founded in Rational Choice, Self, and Social Control Theories, are driving most AIP mitigation efforts. Control theories dominate the security landscape with argumentation explaining why individuals may engage in criminal activity through the analysis of factors such as social attachment, commitment, bonding, and belief.[109] Researchers have indirectly observed the neo-classical economic influence of Hirschi's analysis of social costs and rewards: actors will make decisions and establish patterns of decisions predicated on their understanding of how the decision will add or diminish value relative to their attachment, commitment, bonding, and beliefs.[110] Given the historical interspersal of economic and sociological concepts, it is unsurprising that social control and crime control theories are evident in security tactics, particularly those intended to

[107] Paul W. Glimcher and Ernst Fehr, *Neuroeconomics: Decision Making and the Brain*, 2nd ed. (Boston, MA: Academic Press, 2014), 976.

[108] Gui Xue et al., "Brain Imaging Techniques and Their Applications in Decision-Making Research," *Acta Psychologica Sinica* 42, no. 1 (2010): 16, https://doi.org/10.3724/SP.J.1041.2010.00120.

[109] Roy F. Baumeister and Kathleen D. Vohs, eds., *Handbook of Self-Regulation: Research, Theory, and Applications* (New York: Guilford Press, 2004), 539–41.

[110] Costello and Laub, "Social Control Theory," 25.

detect. Recent calls to increase detection are a call to increase the likelihood of punishment (loss) and affirm deterrence. Similarly, many tactics in the literature, such as team-building and employee development, extend from social control theory. By increasing the value of social bonds within the organization, individuals are presumably less likely to act in their self-interest and more likely to conserve value in their interpersonal relationships. The interplay between theories and their related tactics compels the consideration of evaluative frameworks that also consider a broader array of theoretical factors as the foundations for each theory may affect contextual support for other countermeasures and the adopted security strategy as a whole.

Research directly relating behavior economics to security policies is sparse and needed. The National Academies of Science, Engineering, and Medicine published an in-depth review of behavior economics and its policy implications in 2023. The research discussed many actual and potential touchpoints for criminal justice despite finding very little research directly linking behavior economics to more effective criminology.[111] The researchers responsible for this report noted that several observed phenomena within the realm of attacker-defender security may be explained by behavioral economics more effectively than the traditional economics theory. Examples of such phenomena include varied effectiveness for increased punishment, crime prevention due to selective risk aversion, and security procedure ambiguity as an explanation for criminal ideation due to individuals' general bias to familiar choices.[112] For instance, some security policies at airports require employees to participate in insider threat awareness and reporting activity, which communicates presumably unknown risks of detection and punishment to AIP. This is intended to detect insider threats but also to adjust the AIP calculus and prevent AIP activity. Given the lukewarm position toward behavioral economics provided by such an esteemed group, it is surprising that research related to the use of unpredictable security

[111] Alison Buttenheim, Robert Moffitt, and Alexandra Beatty, eds., *Behavioral Economics: Policy Impact and Future Directions* (Washington, DC: National Academies Press, 2023), 169, https://doi.org/10.17226/26874.

[112] Buttenheim, Moffitt, and Beatty, 169–72.

policies in airports continues to find that increasing uncertainty by decreasing information availability to potential adversaries is a promising strategy for insider threat mitigation.[113]

Taquechel and Lewis attempt to quantify the results of deterrent actions in part using an approach founded in both Prospect Theory and economic games. They found that obfuscating activities aiming to improve deterrence did not affect the adversary; specifically, adversarial target selection was not changed.[114] If increasing uncertainty provides no security value and no effect on the adversary, how has it become such an attractive option? Alternatively, are efforts to quantify the impact of deterrence according to Prospect Theory models simply too incomplete and imperfect? This research has demonstrated a broad and diverse set of Prospect Theory-based countermeasures, and most, if not all, overlap in some way with deterrent intent. Therefore, it is possible that some are more effective than others. Work is ongoing, and the efforts to quantify deterrence based on Prospect Theory remain compelling.[115] This research strongly suggests the value of manipulating the availability and framing of information regarding magnitude and probabilities of loss before adversarial decision-making in ways that both make use of bias and result in AIP's inaccurate and predictable misestimation of risks.

Leveraging Prospect Theory for insider threat mitigation in any way involves recognizing that not all insiders will respond to uncertainty similarly. Individuals will present with varying risk tolerances and may interpret uncertainty differently based on their unique psychological, social, and situational profiles. In conclusion, Prospect Theory provides another valuable lens through which to view AIP decision-making and threat mitigation, particularly by focusing on the roles of decision bias, framing, the decision process, and uncertainty. Significant evidence confirms that organizations can influence the decision-making processes of AIP by manipulating uncertainty and strategically

---

[113] Zeballos et al., "Why and How Unpredictability Is Implemented in Aviation Security – A First Qualitative Study," 10.

[114] Eric F. Taquechel and Ted G. Lewis, "More Options for Quantifying Deterrence and Reducing Critical Infrastructure Risk: Cognitive Biases," *Homeland Security Affairs* XII (September 2016): Article 3, https://www.hsaj.org/articles/12007.

[115] Eric Taquechel and Ted G. Lewis, "Risk, Deterrence, and Prospect Theory: Decision Bias Influence on Quantifiable Deterrence Efficacy in Reducing Risk," *Homeland Security Affairs* XVIII (November 2022), https://www.hsaj.org/articles/21639.

framing potential outcomes. A specific opportunity exists for security policies: in the context of Prospect Theory, policies may be tuned to provide less information regarding detection methods, capabilities, and schedules apart from confirmation that they exist and should simultaneously provide frequent high-quality information on loss, the consequences of adversarial activity. Despite a lack of literature that precisely documents how and to what extent these powerful ideas predictably relate behavioral economics to security and insider threat mitigation, critical infrastructure operators are implementing security policies that rely upon Rational Choice Theory and Prospect Theory concepts to demonstrate effectiveness through deterrence and risk shifting.

E. CONCLUSION

This chapter has reviewed various literature covering insider threats, specifically in airport environments, and topics related to the research question: psychology, behavioral economics, and game theory. The review has illustrated that certain terms of art are diffused between disciplines. Through the analysis of this literature, this research will focus on *threats* and *risk*, described respectively as an intelligent adversary with intent and capability to cause harm and the likelihood that such a threat will succeed. This literature review has further yielded that insider risk mitigation decisions have become more complicated as tactics have proliferated. While options are available to those responsible for CIP, there is no dominant strategy or planning rubric. Further, while evaluative frameworks exist for considering the problem and solutions, using such tools and proposed solutions carries active controversy and opportunities for further research and collective education. Finally, one area of expanding and evolving academic success is using games and behavioral economics to add value and make sense of strategic decision-making by critical infrastructure institutions.

THIS PAGE INTENTIONALLY LEFT BLANK

III. INSIDER THREAT CASE STUDIES: THE PATHS ARE LEGION BEFORE THE INSIDER

Despite the increasing problems posed by AIP as previously described, insiders have long posed a security problem for critical infrastructures, especially airports. Past AIP activity is a rich source of information to assess real-world cases of insiders using their position of trust within secure aviation environments to perpetrate crime and violence. Three such well-documented cases are reviewed in this chapter to analyze the methods used by AIP to avoid security and the security features that may have affected their decision-making. These cases will be subjected to counterfactual analysis to determine hypothetical adversarial responses to plausible but absent security measures, such as those proposed and implemented after such incidents gained special attention from authorities.

A. WHEN TRUST IS THE PROBLEM

In many critical infrastructure environments, a level of trust is bestowed upon personnel with a need to access security-restricted areas once initial training and vetting processes have been completed. In the aviation sector, this level of trust is enshrined in the Code of Federal Regulations and used as a label – unescorted access authority to the secured area.[116] This begs the questions – what measures are in place to validate the appropriate use of such trust and are these procedures effective?

1. Case 1: Even Smuggling Is Bigger in Texas

In 2015, a conspiracy of employees with access to the secured area of their airport and intimate involvement with baggage handling operations conducted illicit smuggling of drugs to at least three other states using unsuspecting airlines as the means of transport. The significant smuggling operation was halted by law enforcement and intelligence officers at Dallas/Fort Worth International Airport (DFW), involving vetted AIP who used

116 Office of the Inspector General, *Audit of Access to Airport Secured Areas (Unclassified Summary)*, OIG-07-35 (Washington, DC: Department of Homeland Security, 2007), 1, https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/OIG_07-35_Mar07.pdf; Michael D. Rennhack, "Unescorted Access vs. Security Clearance," NukeWorker Forum, October 2013, https://www.nukeworker.com/forum/index.php?topic=37139.0.

their positions to bypass security measures and transport drugs illegally for money. This case highlights airport security vulnerabilities related to random inspection, trust verification, and the exploitation of insider access by AIP and involved several airport employees who exploited their insider access to bypass security checks. The conspiracy was formed by AIP with knowledge of the airport's security system and airline operational procedures related to baggage operations and security screening, including a supervisory crew chief for Envoy Airlines and several baggage handlers employed by Envoy and Spirit Airlines.[117] To avoid detection and ensure success, the AIP worked with each other to smuggle narcotics onto commercial flights, bypassing security protocols through creative problem-solving:[118]

- AIP used their security badges to access restricted areas of the airport, avoiding the usual passenger screening processes and providing a convenient method of introducing illicit substances into the security-restricted area.
- A member of the conspiracy was able to access information related to random narcotics detection canine sweeps.
- The AIP conducted counter-surveillance and acted as lookouts to avoid law enforcement detection.
- The AIP also took special care to avoid detection. For instance, simulated drugs were handed off to each other, demonstrating specialized roles, in secure areas of the airport, such as restrooms or food court areas, beyond any airport or TSA checkpoints.

According to press sources, the FBI, with assistance from the Dallas Police Department, IRS Criminal Investigation, and the DFW Airport Police Department, began

[117] Kevin Krauss, "DFW Airport Drug-Smuggling Crew That Offered to Fly Explosives Admits Guilt," *Dallas News*, May 10, 2019, sec. Crime, https://www.dallasnews.com/news/crime/2019/05/10/dfw-airport-drug-smuggling-crew-that-offered-to-fly-explosives-admits-guilt/.

[118] U.S. Attorney's Office, Northern District of Texas, "Lead Defendant in DFW Airport Drug-Smuggling Ring Sentenced to 16+ Years," United States Department of Justice Northern District of Texas, December 6, 2019, https://www.justice.gov/usao-ndtx/pr/lead-defendant-dfw-airport-drug-smuggling-ring-sentenced-16-years.

the investigation in August 2016.[119] Reporting also documents undercover agents providing the conspirators with dummy substances, which the AIP believed to be methamphetamine, and monitored their activities. The investigation revealed that the conspirators smuggled purported crystal methamphetamine onto flights destined for Newark, New Jersey; Charlotte, North Carolina; and Phoenix, Arizona in exchange for financial compensation. According to ongoing reporting and updates, 12 individuals were indicted and subsequently received substantial prison sentences. Finally, in response to the incident, the airport reduced the number of access points to security-restricted areas and implemented some level of employee screening at these access points to the secured area.[120]

This conspiracy effectively documents why and how a collection of like-minded AIP might choose to abuse trust, and it further demonstrates several qualities regarding the threat AIP pose to critical infrastructure. In this case, AIP used several privileges inherent to their trusted status to engage in illicit activity: airport-issued ID media, knowledge of planned screening activities, avoidance of law enforcement, and avoidance of physical security measures. The conspirators all possessed airport-issued IDs and performed work in security-restricted areas. This fact indicates access to the aircraft up to departures and aligns with baggage handling duties. Each of the conspirators developed a detailed knowledge of security countermeasures to increase the likelihood of their success. They then applied this knowledge creatively to plan and avoid detection. The conspirators seemed to enjoy the belief that they operated with less attention and suspicion, given their efforts to avoid law enforcement searches and patrols while demonstrating a keen awareness of their risks.

There are at least three notable observations from this case relating to the group's consideration of passenger safety and access to the aircraft. Firstly, while the conspirators appeared to have been motivated by money and notoriously stated their willingness to transport explosives aboard passenger aircraft, the group seems to consider the impact on

[119] Krauss, "DFW Airport Drug-Smuggling Crew That Offered to Fly Explosives Admits Guilt."

[120] Due to the sensitivity of the airport response to this conspiracy, the precise rate of screening and composition of its procedures are unknown to this research.

passenger safety.[121] This evidence indicates that there was dissension in the group and also indicates some conflict and dissension on this issue: flying explosives on passenger aircraft. This thesis can only speculate on the group's broad motivations and dissent: the conflict was likely rooted in ethical concerns, business risk mitigation, or some combination of these and other factors. The important aspect of this observation is that the group was not a monolith, it seems to have experienced its own growth and conflict and constantly adapted to its external and internal environment. Secondly, AIP used the opportunities and skills they had and those they could develop. In this case, AIP also specialized to contribute value to the group's objectives in presumably efficient ways. Finally, the creativity and opportunism displayed by this group were highly effective. The use of spotters in this case demonstrates how adaptable AIP can be in the face of threat mitigation tactics reflecting an important willingness to seek out and accept certain risks in order to reduce others. One would presume that in conspiracies of this type, the fewest number of people needed to execute operations would be ideal, as the group thereby limits its exposure to potential leaks and discovery. However, in this case, the group determined that additional individuals, and the associated risks a more elaborate conspiracy would generate, were more acceptable than the baseline risk of detection presented by their planned, illicit activities in relation to known security measures. Admittedly, the decision to include any specific number of individuals was not necessarily planned or even deliberate. The inclusion of some individuals may have been coincidental. However, given the group's other indications of careful planning, it is more likely that the decision to include additional individuals was deliberate. Therefore, it is notable that a small group of individuals determined that there was enough value in working together, working through intra-group conflict, to accomplish their illicit goals using their provided access and roles.

2. Case 2: Just One Bag—Daallo Flight 159

On February 2, 2016, Daallo Airlines Flight 159, an Airbus A321-111, experienced an in-flight explosion shortly after departing from Aden Adde International Airport

[121] Roberts, "Airline Employee, Heading DFW Airport Drug-Smuggling Ring, Sentenced to 16 Years in Prison."

(Mogadishu), Somalia.[122] The aircraft, enroute to Djibouti, was carrying 74 passengers and 7 crew members. Twenty minutes into the flight, an explosive device concealed in a laptop detonated, creating a hole in the fuselage remarkably close to the wing and fuel storage area. Almost miraculously, the aircraft returned safely to Mogadishu, with the only fatality being the suspected bomber. This event resulted from a conspiracy by the Islamist military organization Al-Shabaab to smuggle an improvised explosive device (IED) onboard a passenger aircraft.[123] The IED was smuggled aboard the aircraft in a laptop, bypassing security checks due to inside assistance at Mogadishu Airport from AIP. In this case, AIP was used by the terrorist organization to bypass security measures and move the IED in security-restricted areas and eventually onto the aircraft. Sources indicate AIP bypassed several security measures including the following:

- passenger screening: the on-aircraft courier was able to avoid required passenger screening with AIP assistance; the device was passed around screening procedures.
- luggage and device checks: standard protocols for checking electronic devices and luggage for explosives were also bypassed with the assistance of AIP. The laptop, which contained the explosive device, was not subjected to a thorough inspection.
- access control measures: access control measures to security-restricted areas were compromised, allowing unauthorized access and manipulation of security checks.
- monitoring and surveillance: there were lapses in monitoring and surveillance that failed to detect the unusual activity of AIP and the courier.

Case 2 may seem impractical to use in case studies due to its occurrence in Somalia; however, despite the criticism of lax security levied by Daallo and the media against Mogadishu Airport, the case demonstrates significant vulnerabilities that seem relevant domestically at airports and across critical infrastructure. The criticism that a similar

[122] Paul Cruickshank and Robyn Kriel, "Source: 'Sophisticated' Laptop Bomb on Somali Plane Got through X-Ray Machine," CNN, February 11, 2016, https://www.cnn.com/2016/02/11/africa/somalia-plane-bomb/index.html.

[123] Feisal Omar and Abdi Sheikh, "Somalia Sentences Two to Life in Prison for February Airline Blast," Reuters, May 30, 2016, https://www.reuters.com/article/idUSKCN0YL1DJ/.

incident could not occur domestically is weak. Mogadishu Airport is not the same as any airport in Los Angeles, New York, or any other city in the U.S. This is true. However, violence is an attractive option in any political environment wherein there are fundamental disagreements, minority groups seeking power, and the degradation of quality public discourse.[124] Further, commercial airports across the world are remarkably similar despite their differences. They are structurally similar, given their shared functions. Furthermore, influence from large aircraft operators and international regulatory bodies such as ICAO ensure other symmetries and at a minimum, efforts to implement security standards.[125] Despite the marked differences between airports and countries, there are still valid lessons to glean from past AIP activities worldwide.

The plot was not penetrated by intelligence services prior to the event, so all investigations occurred after the incident. Investigation revealed that the courier was likely intended for a Turkish Airlines flight but was transferred to Daallo Airlines when Turkish Airlines canceled its flight for the day. At least two airport employees were found to have facilitated the bomber's bypass of security checks.[126] Ten individuals related to the conspiracy were convicted in connection with the plot, emphasizing the involvement of an organized group capable of circumventing airport security protocols.

In the wake of the event, the airport implemented enhanced security measures, including stricter checks on electronic devices, and may have improved monitoring of airport personnel.[127] Before the incident, aviation security standards at the airport required technology-based property screening such as physical inspection and X-ray. In this case, the modified laptop was passed through screening measures, but the measures had been nullified by AIP. Considering the prosecutions and convictions, the conspirators had penetrated several security processes and levels of leadership at the airport, ensuring that

[124] McMasters, "Societal Polarization: An Evolving Threat to U.S. Homeland Security," 13–15.

[125] "Department of Civil Aviation and Regulation," Republic of Somaliland, accessed November 7, 2024, https://caaa.govsomaliland.org/article/department-civil-aviation-and-regulation.

[126] Robyn Kriel and Faith Karimi, "Airport Workers Seen with Laptop in Somalia Jet Blast," CNN, February 8, 2016, https://www.cnn.com/2016/02/07/africa/somalia-airplane-explosion-video/index.html.

[127] Cruickshank and Kriel, "Source."

security procedures were defeated. Daallo Airlines CEO Mohammed Yassin also emphasized the need for continuous improvement in security practices, including stricter checks on electronic devices and other potential threats.[128] However, this call for action misses the point: the proper application of pre-existing security procedures would likely have caught the device at the security checkpoint – the issue was not physical screening procedures but rather a dynamic response to security measures, the human element. Sources indicate that this incident illustrated serious vulnerabilities in domestic aviation security, particularly the vulnerability created by leveraging insiders at airports.[129] The security measures at play were intended to deter an external threat, and AIP were used to defeat these measures, indicating that the AIP were not deterred from violating access control measures, and were not deterred by the threat of surveillance, monitoring, or physical screening at access points or within security restricted areas. If predictably applied, such measures would have been avoided, given the extent and sophistication of the conspiracy. Unpredictable security measures and invisible security measures would have served as a deterrent in this case as they would have been more difficult to know and avoid.[130] This illustrates the adaptability of AIP and provides compelling evidence that insider threat mitigations should feature unpredictability to some significant extent.

3. Case 3: It's People—The Crew Are People

In December of 2018, law enforcement discovered a significant smuggling operation involving flight attendants traveling through John F. Kennedy International Airport (JFK) in New York. The scheme exploited the Known Crewmember (KCM) program, which is designed to allow airline personnel to pass through a special security

[128] Martin Rivers, "Learning the Lessons of a Lucky Escape," Air Transport, September 15, 2016, https://www.timesaerospace.aero/features/air-transport/learning-the-lessons-of-a-lucky-escape.

[129] Transportation Security Administration, "TSA Insider Threat Awareness," Symposium Briefing (Montreal, Canada: International Civil Aviation Organization, November 2018), 7, https://www.icao.int/Meetings/AVSEC2018/Documents/TSA%20Insider%20Threat.pdf#search=employee%20screening.

[130] Zeballos et al., "Why and How Unpredictability Is Implemented in Aviation Security – A First Qualitative Study," 9.

lane with less scrutiny than regular passengers.[131] At least four flight attendants were connected directly with cash smuggling operations in support of illicit drug trafficking. News reports further indicate that the flight attendants used their KCM status to transport approximately $8 million in bulk cash, which was linked to narcotics sales, including fentanyl, from the U.S. to the Dominican Republic.[132] Sources continue to elaborate that the smuggling operation spanned several years, during which the attendants passed through airport security with large sums of cash and delivered it to contacts in the Dominican Republic in exchange for a commission ranging from $1,000 to $2,000 per successful transfer.

The investigation was led by Homeland Security Investigations (HSI) in collaboration with the U.S. Attorney's Office for the Southern District of New York and the New York Police Department. In October 2021, investigators identified a significant money laundering organization in New York City, which specialized in moving cash proceeds from narcotics sales.[133] A cooperating witness within this organization provided crucial information that helped law enforcement set up sting operations, wherein the flight attendants were caught smuggling law enforcement funds that they believed to be sourced from illicit drug sales.[134] The flight attendants were arrested on May 7, 2024, and have since pled guilty to operating an unlicensed money transmission business.[135]

---

[131] Christopher Fant, "United States v. Hernandez, 24 Cr. 447 (RA) (S.D.N.Y. Jul. 26, 2024); Sealed Complaint" (Department of Justice, April 30, 2024), 1–5, https://www.justice.gov/usao-sdny/media/1351111/dl. KCM is a registered trademark of Air Transport Association of America, Inc. and the Air Line Pilots Association, Int'l.

[132] Rob Quinn, "Feds: Flight Attendants Smuggled $8M in Drug Money," Newser, May 9, 2024, https://www.newser.com/story/350095/4-flight-attendants-accused-of-smuggling-drug-money.html.

[133] U.S. Attorney's Office, Southern District of New York, "Flight Attendants Charged in Connection with Smuggling Drug Money to the Dominican Republic," United States Department of Justice Southern District of New York, May 8, 2024, https://www.justice.gov/usao-sdny/pr/flight-attendants-charged-connection-smuggling-drug-money-dominican-republic.

[134] Department of Homeland Security, Homeland Security Investigations, "Flight Attendants Charged with Smuggling Drug Money into Dominican Republic," Homeland Security Investigations, May 2024, https://www.dhs.gov/hsi/news/2024/05/08/flight-attendants-charged-smuggling-drug-money-dominican-republic.

[135] Nicholas Biase and Shelby Wratchford, "Four Flight Attendants Plead Guilty to Smuggling Drug Money to the Dominican Republic," United States Department of Justice Southern District of New York, August 14, 2024, https://www.justice.gov/usao-sdny/pr/four-flight-attendants-plead-guilty-smuggling-drug-money-dominican-republic.

This case suggests that security measures related to trusted population programs like KCM are insufficient and facilitate AIP commission of illicit activity. It has revealed critical vulnerabilities within the airline security system, specifically the potential for abuse of the KCM program by a population with extraordinary trust.[136] More generally, it suggests that the creation of a more trusted population is a bane to a secure environment. A population of individuals with a means to bypass security measures is made more attractive to criminals and terrorist organizations; this population is ripe for adversarial leverage, as seen in the previous case. The demonstrated lack of deterrence does not seem related to a lack of awareness, as smuggling and insider betrayal are popular topics in fiction and art. For instance, CBP's counter-smuggling and AIP mitigation work were showcased in a popular television show in 2012.[137] A simple internet search demonstrates various popular media plots related to flight attendant smuggling: Jackie Brown, Crew, and The Flight Attendant.[138] More importantly, at least 5 high-profile smuggling operations have been featured by news outlets since 2017, and many have already been prosecuted.[139]

---

136 The Known Crewmember® (KCM) program is a joint initiative between Airlines for America (A4A) and the Air Line Pilots Association, Int'l (ALPA). KCM ties airline employee databases together in a seamless way and enables Transportation Security Administration (TSA) security officers to positively verify the identity and employment status of crewmembers. – https://www.tsa.gov/for-industry/known_crewmember.

137 U.S. Immigration and Customs Enforcement, "HSI Special Agents at JFK International Airport Work 'To Catch a Smuggler,'" February 10, 2023, https://www.ice.gov/news/releases/hsi-special-agents-jfk-international-airport-work-catch-smuggler.

138 *Tarantino, Quentin, director. Jackie Brown*, Crime, Drama, Thriller (Miramax, A Band Apart, Lawrence Bender Productions, 1997); Yockey, Steve, creator. *The Flight Attendant*, Comedy, Drama, Mystery (Warner Bros. Television, Berlanti Productions, Yes, Norman Productions, 2020).

139 David Propper, "American Airlines Mechanic Convicted of Stashing $320K of Cocaine under Cockpit of Plane," *New York Post*, May 3, 2023, Electronic edition, https://nypost.com/2023/05/03/american-airlines-mechanic-convicted-of-stashing-320k-of-cocaine-under-cockpit-of-plane/; Jennifer Peltz, "'Finch-Smuggling Kingpin' Gets Prison Time for Sneaking Birds Into NY for Competitions," NBC New York, February 10, 2023, https://www.nbcnewyork.com/news/local/crime-and-courts/finch-smuggling-kingpin-gets-prison-time-for-sneaking-birds-into-ny-for-competitions/4096768/; Andrew McMunn, "Man Arrested at JFK Airport after 40 Lbs. of Cocaine Found in Bags of Jumbo Shrimp, Federal Officials Say," WLBT3, January 21, 2024, https://www.wlbt.com/2024/01/21/man-arrested-jfk-airport-after-40-lbs-cocaine-found-bags-jumbo-shrimp-federal-officials-say/; Tom Shea, "Man Caught at JFK Airport Trying to Smuggle Fentanyl Inside Candles from Mexico," News Source, 4NBC New York, April 12, 2023, https://www.nbcnewyork.com/news/local/crime-and-courts/man-caught-at-jfk-airport-trying-to-smuggle-fentanyl-inside-candles-from-mexico/4235727/; Andrew Keshner and Thomas Tracy, "Woman Busted at JFK Airport Smuggling Cocaine in Motorized Wheelchair's Cushion," *Daily News*, June 13, 2017, Online edition, sec. New York News, https://www.cclec.org/enforcement/woman-busted-at-jfk-airport-smuggling-cocaine-in-motorized-wheelchairs-cushion/.

Surely, the AIP in this case were aware of the potential consequences of their decisions; these AIP knew the risks and made the decision to participate in the game. While successful investigation and subsequent arrests are significant steps in addressing the exploitation of airport security systems by narcotics traffickers, this case and the prosecution of other frequent cases do not appear to deter smuggling operations effectively. People have diverse motivations to bypass security procedures and AIP observe, learn, and find or create weak points in a security system.

B. CASE STUDY SYNTHESIS

These three cases share central themes related to the planning, execution, and sustainment of AIP operations. Table 1 provides a summary of the analysis from each of the cases. Despite the difference between these cases, security procedures were different in each case, the roles of various AIP were diverse, and each case was observed at quite different locations; all cases illustrate the capacity for attacker adaptation and evolution specifically related to predictable security measures. Given the opportunity to understand a predictable security system, a motivated insider will plan measures to defeat security countermeasures. There is strong evidence that various avoidance strategies were applied in each of these cases. In case 1, a variety of passive and active security avoidance techniques were applied by AIP to reduce or manage the chance of detection and loss: AIP exhibited great effort to choose the best times and places, avoiding scheduled screening and employing spotters to reduce the likelihood of coming into contact with security personnel and other employees.

Table 1. Summary of Case Study Attributes

Factor	Case 1	Case 2	Case 3
Misuse of Trust	X	X	X
Active Avoidance/Countersurveillance	X		
Passive Avoidance – use of concealment techniques, timing to avoid security	X	X	X
Use of Inside Information	X		X
Operation in a Secured Area	X		X
Penetration and Recruitment		X	X
Conspiracy	X	X	X
Dynamic Adversarial Tactics	X	X	X

The captain of Daallo flight 159, responsible for safely landing the aircraft after the bombing, publicly criticized the security posture of the airport because he had not observed identity badges displayed during his experience at the airport, noting that anyone could have had access to the aircraft and access control seemed ineffective.[140] While the captain questions this issue and baggage checks, in this case, access to the aircraft seemed at least somewhat controlled, considering that the conspirators chose to introduce the explosives device directly through the checkpoint instead of through the restricted areas surrounding the aircraft. Further, the conspiracy was developed to involve multiple security layers and officials. While this element of the plot may have been an opportunistic development, i.e., sympathetic security officials may have proposed the attack pathway and already been in useful positions, it is also logical that such individuals would have possessed an expert understanding of the most vulnerable attack pathway to the aircraft. Had a different

140 Phillip Baum, "Daallo Airlines Bombing: Interview with Captain Vladimir Vodopivec," *Aviation Security International*, February 2017, 29, https://www.avsec.com/media/files/int01.pdf.

pathway, with less risk to the conspirators, been present, it is reasonable to presume it would have been selected.

Each of these cases is complex and a trend toward complexity is a surprising attribute to associate with criminal insider activity as fewer mouths to feed also suggests fewer loose lips and generally means higher personal gains and less risk. Having fewer people involved in each plot decreases the activity's intelligence detection surface areas. However, in each of these cases, more than 5 people were involved in various phases of the conspiracy. For cases 1 and 3, evidence indicates that the deliberation, planning, and decision-making included more individuals than were necessary to execute successful operations. In each of these cases, the plotters could have decided to operate alone and instead accept the risk associated with encountering random screening or being challenged in the secured area, accepting the risk of potential discovery. They chose against this. In these cases, leaders and planners involved additional individuals in security or counter-security positions to offset their risk of detection (loss). This tendency toward risk management is also demonstrated by the cash amounts used in case 2, wherein each AIP was provided a $60,000 package for transportation. This amount exceeds that which would be required by financial reporting regulations yet is well under the total money moved during the operation in any flight or time period. The decision to transfer money using multiple individuals in the trusted class indicates some deliberation and preference for risk diversification: the planners seem to have balanced the potential for loss among the risk of discovery, monetary loss, and opportunity loss. AIP are employing some semblance of an economic frame in each of these cases.

C. COUNTERFACTUAL ANALYSIS

The observations from the case studies raise two significant questions: how can security be made more dynamic to inhibit attacker planning, and is there a threshold beyond which uncertainty surrounding countermeasures better mitigates risk? As with any public incident, there are actual responses from regulatory authorities in each case. In response to case 1, the DFW Smuggling case, DFW implemented immediate employee screening and decreased its number of employee access points to security-restricted areas. In response to

case 2, the bombing of Daallo Flight 159, Daallo and Mogadishu Airport worked to improve physical screening and oversight of security operations. In response to case 3, JFK smuggling, the TSA worked to strengthen initial and recurrent vetting related to the KCM program. Would these efforts have been effective at preventing each of these cases? This thesis will now apply a counterfactual framework to explore the effects of increasing physical screening at access points to aviation-secured areas, improving vetting and behavioral monitoring, and increasing intelligence.

1. Aviation Worker Screening at Access Points to Secured Areas

Despite significant support, screening AIP at fixed access points would not likely prevent, or even deter, AIP from using their unique privileges and access to introduce illicit material into security-restricted areas. At airports, screening all aviation workers is a plausible scenario through which to assess each of these cases, as the requirement exists in many countries. Notably, non-passenger security screening requirements were not effectively applied to the departure airports for any of the three cases. Representative controls reflecting full non-passenger screening do exist: fully compliant members of ICAO have implemented aviation worker screening at perimeter access points.[141] The rationale behind this standard is that full aviation worker screening, particularly when mixed with random access point screening, deters AIP from introducing prohibited items into security-restricted areas, where there is an expectation that dangerous and illicit material should not be present.[142]

ICAO and the National Safe Skies Alliance both recommend that aviation worker screening be equivalent to passenger screening. However, this requirement frames passenger and insider screening as the same problem-solution set. Additionally, Safe Skies recommends random, limited inspections of AIP for unauthorized items at access points to

[141] International Civil Aviation Organization, *ICAO Pamphlet: Managing Insider Risks*, 1st ed. (Montreal, Canada: ICAO Aviation Security, 2022), 1,4, https://www.icao.int/Security/Security-Culture/State%20and%20Industry%20Promotional%20Material/ICAO%20Pamphlet%20Managing%20Insider%20Risks.pdf.

[142] Grizzle, *Insider Threat Mitigation at Airports*, 18.

the security-restricted area.[143] These recommendations encourage the security community to disregard the unique aspects of the insider population, such as knowledge of security systems, and fail to address the adaptability demonstrated by AIP: they have access to real-time security information within dynamic environments, are often entitled to security information, have access to (nearly) all areas of the airport, and possess the initiative to act in response to security decisions. Passengers do not naturally have access to security information without insider assistance, do not typically have access to multiple pathways to assets, and cannot conveniently modify attack plans once initiated.[144] The common discourse for this type of screening is that it works: 6,737 firearms were discovered at airport security checkpoints in 2023.[145]

Despite claims that screening at access points is effective at deterring AIP, this premise is concerning because external threats are not the same as those posed by AIP. A screening checkpoint is not the only place where illicit material can be introduced. Further, screening that only occurs at one location, or class of locations, is not unpredictable. Therefore, while screening at access points is likely better than nothing, as unauthorized items are often discovered, it does not solve the introduction of contraband around perimeter fencing, via exempted individuals and vehicles, or the construction/production of contraband in the secured area. The counterfactual response of the conspirators in case 1 to the premise of full and/or random inspection at access points would be to use safe areas of the perimeter to pass material into the secured area, while making use of lookouts and insider information to plan the safest times and places and avoid detection. Should such opportunities not exist, the next likely option would be to infiltrate the screening process to pass contraband through the screening checkpoint, the option demonstrated in case 2. By contrast, the flight crew in case 3 would be daunted by the introduction of any

[143] Grizzle, 18.

[144] These aspects of insider populations seem prescient to Safe Skies research – each is referenced in various documents. However, the documents cited are written in a manner that aligns and connects with various existing recommendations, requirements, and industry practices.

[145] Transportation Security Administration, "TSA Detects 6,737 Firearms at Airport Security Checkpoints in 2023," Transportation Security Administration, accessed January 12, 2025, https://www.tsa.gov/news/press/releases/2024/01/10/tsa-detects-6737-firearms-airport-security-checkpoints-2023.

(additional) screening into the KCM process. To continue smuggling operations, the crew members would expand their conspiracy and leverage other, more trusted, AIP or TSA security personnel referencing case 2, to move the money into the sterile areas of the airport for eventual transport. Therefore, the introduction of screening for employees and KCM would significantly change the AIP *business* models employed in the cases but would not likely prevent such plots from succeeding.

Despite forcing a change to tactics, random aviation worker screening checkpoints fixed to access points and processes would not likely prevent, or even deter, AIP from using their unique privileges and access to introduce illicit material into security-restricted areas. This analysis is supported by recent incidents. Despite increased non-passenger security screening of potential AIP in international locations, incidents of smuggling and insider operations continue to demonstrate the adaptability of AIP to static security measures such as predictable physical screening. For instance, in May of 2024, six individuals with trusted access to Schiphol Airport, a location where AIP are screened, were arrested for conspiring to bypass aviation security processes and facilitating a drug smuggling operation. They were only discovered due to an anonymous tip logged from another country.[146] Where there is a will and an opportunity to evolve, there is a way to modify an attack to fit the defensive landscape. Physical screening predictably deployed to access points has not and will not affect the ultimate capability of AIP.

2. Increased Recurrent Vetting

Initial and recurrent vetting are valuable tools to mitigate AIP activity and would have inhibited AIP in some cases. Vetting has been an important component of insider threat mitigation for decades. In the energy sector, certain secret information has been designated important to national security and defense and is protected under the U.S. Code of Federal Regulations since the Manhattan Project.[147] Individuals continue to be vetted before permitting access to information related to certain critical infrastructure using

[146] Hanneke Sanou, "Police Arrest Six Airport Workers for Drug Smuggling," *Dutch News*, May 31, 2024, https://www.dutchnews.nl/2024/05/police-arrest-six-airport-workers-for-drug-smuggling/.

[147] 10 CFR Part 95 § 95.25 (2023) Protection of National Security Information and Restricted Data in storage.

generally the same processes.[148] Protecting this information from adversarial insiders or individuals seeking such positions is a twofold process: identifying the sensitivity of access and vetting individuals to determine the appropriateness of the access. In 2010, researcher Alan Black called for more effective vetting measures for mitigating AIP and proposed potential improvements to vetting and profiling potential AIP recommending recurrent vetting, *rechecking*, and a full 10-year vetting with access to juvenile records.[149] In 2017, Brian Bean reviewed vetting requirements for aviation workers, noting that a culture of awareness, a strong counterintelligence program and behavioral monitoring using employees as sensors are crucial to insider threat mitigation strategies.[150] In 2018, TSA issued proposed rulemaking with the intent of expanding the list of criminal records and offenses vetted and extending the lookback period.[151] The U.S. recently introduced more frequent vetting of individuals with access to the secured areas of airports. Individuals working at airports are now subject to FBI assessment of background offenses and connection to known terrorists through the Record of Arrest and Prosecution (RAP) Back Program.[152] This move reflects the evolving vetting posture of the TSA for aviation installations, making the process more similar to that of other critical infrastructure systems in the U.S. already subject to Transportation Worker Identification Card (TWIC) requirements. It also reflects actions underway in the Department of Defense, which

[148] 49 CFR Part 1520 (2023); Transportation Security Administration, *SSI Best Practices Guide* (Washington, DC: Transportation Security Administration, 2023), https://www.tsa.gov/sites/default/files/ssi_best_practices_guide_for_non-dhs_employees.pdf; Transportation Security Administration, "Sensitive Security Information," Transportation Security Administration, June 2023, https://www.tsa.gov/for-industry/sensitive-security-information.

[149] Black, "Managing the Aviation Insider Threat," 31–40.

[150] Bean, "Mitigating Insider Threats in the Domestic Aviation System," 21–25.

[151] Department of Homeland Security, "View Rule: 1652-AA70," Office of Information and Regulatory Affairs, November 2018, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201810&RIN=1652-AA70.

[152] Transportation Security Administration, "The TSA Workforce Has Adapted to the Changing Threat Environment, Remains Steadfast and Committed to Securing the Nation's Transportation Systems," Statements, October 27, 2022, https://www.tsa.gov/news/press/statements/2022/10/27/tsa-workforce-has-adapted-changing-threat-environment-remains; Tuyet-Quan Thai, "TSA Can Improve Aviation Worker Vetting," GAO Report (Washington, DC: Department of Homeland Security Office of the Inspector General, June 2014), 16, https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/2015/OIG_15-98_Jun15.pdf; McNeil, *Aviation Security*, 17.

already required strict recurrent vetting of clearance holders.[153] Vetting is a powerful tool to ensure that trust is being provided to the correct people and being withheld from the people who are most likely to abuse such trust.

In the cases, initial vetting was not effective at mitigating AIP in two of the three cases assessed. In case 1, all involved AIP had been vetted and would not have been identified as potential threats due to their clean backgrounds and lack of contact with known terrorists. However, had their business expanded to include terrorists known to intelligence services, there is a chance that the interaction may have led to recognition of the participants as AIP. The degree to which such recurrent vetting has been publicized leads to further conclusion that capable organizations with connections to terrorist organizations will likely be compelled to use clean-skin individuals as agents to penetrate security systems in critical infrastructure and be further compelled to use clean-skin agents to interact with potential smugglers in transportation environments. As illustrated in case 3, the trusted population is a desirable pool from which to recruit. Thus, individuals with access to the KCM program are a highly desired partner for illicit operations. In case 2, the available literature does not permit a conclusive analysis of the effect that recurrent vetting may have had on the scenario. Hypothetically, if a connection to terrorist organizations in Somalia had been a parameter that people could have reliably vetted against, then the plot may have been both interrupted and penetrated, illustrating the value of this countermeasure. Applying this observation to homeland security, the context offered by case 2 may forecast a complex and multi-polar environment to which the U.S. is transitioning – an environment with fewer arrests, prosecutions, and intelligence resources to support vetting actions.[154] Fewer official contacts with police and a higher bar for prosecution may well result in a less effective vetting system.

---

[153] Transportation Security Administration, "TWIC," Transportation Security Administration, 2024, https://www.tsa.gov/twic; David Vergun, "All DoD Personnel Now Receive Continuous Security Vetting," DoD News, October 5, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2800381/all-dod-personnel-now-receive-continuous-security-vetting/.

[154] John Gramlich, "Federal Criminal Prosecutions Fall to Lowest Level in Nearly Two Decades," Pew Research Center, March 28, 2017, https://www.pewresearch.org/short-reads/2017/03/28/federal-criminal-prosecutions-fall-to-lowest-level-in-nearly-two-decades/.

3. Increased Intelligence Gathering and Investigation and Employee Monitoring

The inherent challenges of relying on employee awareness programs, despite their well-documented success in cultivating safety-oriented environments, become apparent when considering Social Identity Theory and elements of Social Control Theory, which point to deeper psychological and sociological motivations that enable insiders to bypass self-policing mechanisms. Two of the three cases present conspiracies which were infiltrated via solid investigatory work. In case 1, smuggling services were offered by AIP to undercover agents, resulting in a grand and lengthy investigation to document the conspirators' business model over time. In case 3, testimony provided after an arrest from connected individuals led to the identification of the smuggling operation, and the investigation revealed an intricate and well-developed money-moving operation. However, case 2 bucks this trend, as the plot was not penetrated, and an act of violence was not prevented.

Active intelligence and surveillance may be more effective at discovering and infiltrating AIP conspiracies than a reliance on employee reporting of suspicious behaviors. It is often joked that the same stinger missile has been sold to 150 would-be terrorists; smugglers are forced to navigate a world of potential clients that include honeytraps. The investigation of identified criminal activity then yields new investigatory opportunities. This is not to say that improved employee awareness and cultural qualities supporting safety and security are not valuable; they certainly are to more than just security.[155] However, all the Cases indicate that complex conspiracies can flourish within environments even where safety and security have been baked into the culture for some time.

Given the academic recommendations of the early 2000s related to comprehensive insider threat mitigation to include employee support and mental health awareness themes and the integration of organizational psychology in insider threat mitigation over the last

[155] Kim Maley et al., "Effective Workplace Culture: The Attributes, Enabling Factors and Consequences of a New Concept," *International Practice Development Journal* 1, no. 2 (October 2011): 15, https://www.fons.org/wp-content/uploads/2024/03/IPDJ_0102_01.pdf.

decade, it is unlikely that idealized employee awareness programs were absent from the domestic case studies. In fact, a review of public information campaigns illustrates that such employee awareness programs have been advertised features of the security programs at airports, other critical infrastructure, and even Las Vegas Casinos since the early 2000s.[156] Therefore, in practical application, the perceived capability of such programs toward deterring AIP in each of these cases should remain guarded. These programs are not new and should not be viewed as a way to fill an existing gap; that said, if such programs can be improved, gaps could be closed. In 2018, the TSA implemented an improved Insider Threat Program through its Federal Air Marshal services that uses self-reporting. Employee and airport reporting are intended to facilitate national mitigation efforts.[157] The results of this program are somewhat shrouded, though the Government Accountability Office provides some evidence of success for this program and the broad class of awareness, reporting, and intelligence programs in its reporting on TSA's insider threat mitigation efforts.[158] In each of the Cases, employees may have been observed acting out of the norm either at or away from work. For instance, other flight crew members traveling with the AIP in case 2 may have noticed suspicious activity in the Dominican Republic. Improved observation and reporting of such observation could have led to faster and more effective investigation and plot infiltration.

More advanced behavioral monitoring may be a new layer with which to multiply the effectiveness of existing security procedures and institutional momentum with regard to physical screening. Technology now exists to monitor employee location via access card. Equally importantly, technology is now capable of real-time analysis of movement patterns and financial records to identify suspicious behavior. Amazon Inc. notoriously implemented artificial intelligence-enabled employee-tracking systems to improve

156 Diane Ritchey, "See It, Say It, Spread the Message in Las Vegas," *Security Magazine: Security and Business Resilience*, June 6, 2011, https://www.securitymagazine.com/articles/82102-see-it-say-it-spread-the-message-in-las-vegas.

157 Zeigler, "Leveraging DHS Assets," 61–64; Serge Potapov and Philip Kaplan, *Privacy Impact Assessment for the Insider Threat Unit Database* (Washington, DC: Department of Homeland Security, 2018), 1–5, https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa048-april2018.pdf.

158 McNeil, *Aviation Security*, 33–35.

efficiency and COVID-19 prevention.[159] Requirements to implement such technologies into access control, challenge procedures, and vetting processes may redefine physical screening at access points as valuable and further mitigate AIP measures at acceptable costs. Though such a solution conjures an Orwellian vision of critical infrastructure workspaces—these measures are intrusive, run afoul of privacy regulations, and may be used in ways that reduce employee well-being with some form of *Big Brother* always watching—this research has not identified legal obstacles to hypothetical policy requirements ensuring all critical infrastructure-issued access media be capable of contributing to employee location.[160] Coupled with existing practices of challenging individuals in secured areas for access to media, such a tool would provide insight into employee behavior and perhaps faster intervention targeting. In all three cases, the use of real-time analysis of employee movement would flag AIP as they deviated from their routine assigned activities, significantly increasing the effort required to complete activities observed in each case. Security agents could then use such flags to effectively direct surveillance, screening, and investigative resources.

D. CONCLUSION

These cases illustrate AIP's impressive capability to defeat existing and counterfactually applied security tactics. The Cases and the counterfactual analyses further highlight the disparate drives that may propel AIP along their paths toward action. In two of the cases, the crew members and the ground crews, teams of individuals, worked to make money. The conspiracy discussed in the analysis of case 2 demonstrates the willingness of followers to kill and maim to advance their own ideological agenda. While this thesis does not focus on terrorism, it demonstrates that terrorist tactics, including the use of mass violence to influence politics, is a persistent aspect of the insider threat posed by AIP. People are masters of using what they have, can see, and can do to change the

[159] Sissi Cao, "Amazon Unveils AI Worker Monitoring for Social Distancing, Worrying Privacy Advocates," *Observer*, June 16, 2020, sec. Technology, https://observer.com/2020/06/amazon-artificial-intelligence-monitor-warehouse-worker-social-distancing-coronavirus/.

[160] Dexter Tilo, "Amazon Fined for 'excessive' Employee Monitoring," Human Resources Director, January 24, 2024, https://www.hcamag.com/us/specialization/employment-law/amazon-fined-for-excessive-employee-monitoring/474239.

world – it is the human element. Most importantly, the cases and counterfactual analysis demonstrate the capacity of AIP to form complex teams with specialized roles and adapt to security measures. Therefore, while security measures may be considered on their own, in direct opposition to adversarial action, given the propensity of teams to act as adversarial units, security measures are more effectively assessed in a system's context, not on their own. This was illustrated by the counterfactual addition of technology to monitor employee behavior in the aviation sector and its potent relationship to existing challenge programs and access control systems.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. WINNING THE BATTLE, LOSING THE EDGE—INSIDER THREAT MITIGATION IN AIRPORTS

While the case studies presented in the previous chapter provide insight into the relationship between security systems used to protect critical infrastructure and adversarial tactics to defeat such systems, this chapter seeks to apply game theory and counterfactual analysis to evaluate the theoretical effectiveness of certain tactics used to secure airports from insider threat activity and the potential for adversarial decision-making to circumvent airport agent actions at various levels of critical infrastructure: system, airport, and adversarial-agent level. The primary intent of this analysis is to provide a rigorous assessment of airport security mechanisms designed to mitigate insider threats. At least two levels of analysis are helpful for this objective: the study of airport participation in security systems and the analysis of AIP strategies toward defeating security tactics.

Critical infrastructure is a complex environment and the challenges posed by insider threats are wicked and nuanced as demonstrated in the previous chapter. Simplifying environments in the real-world, such as an airport or airport systems, and simplifying complicated challenges, such as those posed by AIP, permits focused analysis on aspects of the insider threat problem faced by critical infrastructure. Modeling realistic scenarios by applying market-based games and sequential attacker-defender games may identify security system weaknesses and assess from where they arise, tracing modeled system weakness to tactic selection. Mechanism Design Theory (MDT) is a valuable tool capable of modeling airports as agents in regulated markets and permitting the hypothetical application and reimagination of airport security protocols based on real-world case studies. In this analysis, these mechanisms are tested using evolved sequential games to simulate various scenarios and assess institutional performance. This approach permits a simplified examination of how different security measures shape adversarial decision-making via payoff manipulation within simple models of an otherwise complex airport environment. This method offers practical insights into the effectiveness of proposed mechanisms in real-world settings and a theoretical perspective on case studies from the

last chapter further demonstrating that adversarial agents benefit from possessing the initiative and are deterred by truly unpredictable and unknowable security measures.

A. MECHANISM DESIGN THEORY (MDT): SECURITY GAMES

Game Theory permits complex systems, or aspects of such systems, to be studied and better understood in simplified and controlled scenarios where players (Agents), their actions (strategies), and outcomes (utility payoffs) are strictly defined and limited. MDT is an applied economics tool in the general field of game theory which focuses on creating systems or protocols to achieve optimized payoffs in which all agents maximize their utility; the theory challenges system designers to ensure that agents contribute to and participate in the institutional system in an efficient manner. Optimization occurs when particular tactics dominate others based on their perceived outcomes in the form of payoffs for each agent, sometimes referred to as strategic dominance, even when participants have private information and may act in their interest. Famously, these theories are often used to describe and design strategy-proof market and auction scenarios.[161] In the context of airport security, mechanism design might assist in constructing protocols that ensure safety and efficiency while focusing on potential insider threats while also extending the general understanding of how airports systems are incentivized to invest in security.

Security games, a specialized kind of economic game, may benefit from the integration of MDT concepts. Security games generally seek to model the economic relationship between individual agents, such as airports and/or adversaries, and their willingness to invest in additional security resources, to preserve the public good, collaborate to defeat system controls, or stabilize market conditions.[162] Questions of investment in socially responsible security technology have been examined through this lens. One such example is modeling airlines' willingness to invest in new security technologies, specifically baggage screening equipment, as such agents must balance the

[161] Michael Kearns et al., "Mechanism Design in Large Games: Incentives and Privacy," *American Economic Review* 104, no. 5 (May 2014): 405, https://doi.org/10.1257/aer.104.5.431.

[162] Chremos and Malikopoulos, "Mechanism Design Theory in Control Engineering," 30.

investment cost against the shared cost of catastrophe.[163] Though baggage security can be different from threats posed by AIP as a baggage system can be accessed more readily by internal threats, this research is an excellent proxy for insider threat mitigation which this analysis can assess and extend. Kunreuther and Heal, in their 2003 analysis, noted several gains and losses stemming from the investment decision point with two- and three-agent games, even though each agent was provided with perfect information in the model. Notably, Kunreuther and Heal's analysis of baggage screening investments discusses a strong connection between airport agents and the natural inclination of airlines to avoid voluntary investment in additional security features. While they illustrated that airports are connected and exist as part of a more extensive critical system and noted that attacks of baggage systems would exhibit a significant contagion effect, because baggage may be processed from airport to airport and airline to airline, their research highlighted the necessity of government intervention in certain security game scenarios due to inherent market pressure causing agents to act selfishly and withhold individual investment.[164]

B. AIRPORT SYSTEMS—THE GAME

Kunreuther and Heal's analysis is ripe for adaptation to airport security investment decisions thus extending their analysis. The first step is the construction of a model with multiple airports. The careful construction of this model is essential. First, the parameters of the game are defined. The institution, the airport system, is defined as a collection of airports participating in business and competing for profit while also working to preserve the common good, a secure aviation environment.[165] This model further assumes that each airport is the same and has perfect or near-perfect information regarding potential risks and any potential costs. This assumption is practical given the degree to which airports participate in cooperative associations but also necessary to simplify and construct the

[163] Howard Kunreuther and Geoffrey Heal, "Interdependent Security," *Journal of Risk and Uncertainty* 26, no. 2 (May 2003): 233–45, https://www.jstor.org/stable/41755017.

[164] Kunreuther and Heal, 234–35.

[165] While most airports are not for profit institutions, they are considered self-sustaining. Therefore, the profitability, net revenue generation, of an airport drives typical business competition between airports as there is a limited demand for the services and spaces that an airport makes available for sale – commercial, airspace, gate space, and various facilities.

game.[166] It is also assumed that each airport must decide to invest (I) or not invest (A) in further security measures to mitigate insider threats. Further, given agent competition, it is also presumed that any agent's actual decision to invest in additional security is not perfectly coordinated and that airports could withhold information regarding this decision from each other and independently make this determination.

Airports' choices are as follows:

- Airport 1 invests in enhanced security measures.
- Airport 1 does not invest in enhanced security measures.
- Airport 2 invests in enhanced security measures.
- Airport 2 does not invest in enhanced security measures.

Should Airport 1 invest a portion of profit (M) for security enhancements, represented as cost of investment (C_I), they are presumed to have reduced the likelihood and impact of AIP activity, producing a net utility of $M - C_I$. It should also be presumed that a ripple effect of loss is often observed in the event of significant incidents. Sometimes, this effect reduces the overall income of the system, resulting in a weaker loss suffered by other agents. Therefore, in games where only one airport invests, both airports are exposed to some risk of contagion loss, expressed as a remaining risk. Further, in any event where only one airport has invested in mitigating AIP activity, the cumulative probability of attack, a portion of risk calculation, has shifted, conserving some portion of the total risk, and increasing the risk presented by AIP for the agent choosing not to invest. Should both airports invest within a closed two-airport model, it would be presumed that contagion loss has no influence and that the system has mitigated the threat.

A Nash equilibrium occurs when no player can unilaterally change their strategy to achieve a better payoff, assuming the other players' strategies remain unchanged implying

[166] Colleen Chamberlain and Brian Kalish, "AAAE Aviation Security Summit," American Association of Airport Executives, accessed January 14, 2025, https://aaae.org/securitysummit; Kevin Burke, "Airports Council Releases Statement on Rodney Scott Nomination to Serve as Customs and Border Protection Commissioner," Airports Council International – North America, December 9, 2024, https://airportscouncil.org/press_release/airports-council-releases-statement-on-rodney-scott-nomination-to-serve-as-customs-and-border-protection-commissioner/.

a rational state where no agent would alter their strategy. Presuming the following constraints and inputs:

- M = $1,000,000 for each airport
- Cost to Invest (C_I) = 2% of M when agent invests and 0% of M when agent abstains.
- Cost of Liability (C_L) arising from an attack = 30% of M, or $300,000 and is modified by the agent's decision to invest – when an airport invests, the cost is reduced by 98%.
- System Risk (R) =0.0025 estimating on the following national forecasting method: one top twenty airport will be attacked every 20 years.
- Payoff Function = M – Modified C_I – (Modified C_L*R)[167]

This model indicates an equilibrium at I:I, wherein both airports invest. Given the equilibria observed in this model, illustrated in Table 2, it might be presumed that airports will naturally invest in additional security measures to produce a socially responsible and secure system as each agent is compelled to invest and produce better outcomes for themselves and the system. Consumers, constituents, and spectators should only wait as agent investment will occur with haste – problem solved. However, this model has revealed two equilibria, implying that there is an independent incentive for airports to cooperate and choose not to invest as a block. Given this model and its results, airports would naturally be inclined to cooperate, though the decision to invest or abstain from investment is equally compelling in a competitive environment.

[167] As this model is linear, M could be considered as a true variably wherein the payoff function could be imagined for every M, payoff = M – Modified C_I – (Modified C_L*R), permitting rapid scaling. $1,000,0000 is a simple placeholder. Further, this note applies to subsequent airport-level models.

Table 2. Airport MDT Game 1

		Airport 2 (A2)	
		Invest (I)	Abstain (A)
Airport 1 (A1)	I	$999,983, $999,983	$999,983, $999,625
	A	$999,625, $999,983	$999,625, $999,625

1. Model Elaboration

However, actual observations conflict with this first model iteration: recent and ongoing airport security decisions do not regularly reflect these results. As discussed in Chapter I, with respect to aviation worker screening as an investment option, only a few airports have chosen to invest heavily, while most have not. The evidence supporting this discussion, particularly regarding infrastructure operator reticence to invest at levels exceeding regulatory requirements, does not align with model outcomes. Further, individual airports and associations have publicly positioned themselves to resist such investments and regulations requiring such investments.[168] There must, therefore, be other complicated factors at play that must be considered to extend the model and understand these market and agent decisions more accurately.

One explanation for this misalignment may be that a significant incident is unlikely to affect any agent and would be limited in its immediate consequence to each agent. A rudimentary analysis quickly demonstrates that a multi-million-dollar investment to mitigate a substantial, but low probability, incident does not make rational business sense for an individual agent. Recent analysis of such incidents suggests that while the overall impact of an AIP activity varies by intention and tactic, a targeted attack intending to maximize system damage will cause a system loss valued at $17.3 billion; at the same time,

[168] Airports Council International, "ACI-NA Position on TSA's Aviation Worker Screening National Amendment," 3. There are many examples of airports investing in security to protect itself from theft, liability, and regulatory expansion – where investment does not present local ROI. This point is directed at local investment to reduce regional, system, and national risk. .

each agent only absorbs a small fraction of this loss, which is unlikely to exceed $3 million.[169] Thus, when local losses are manageable, more expensive investments are more difficult for airport business managers to justify and purchase.

Additionally, the cost for threat mitigation can exceed the simple cost of its purchase. A 2014 review of insider threat mitigation at airports relying on an in-depth survey of subject-matter experts revealed a fascinating anecdote: Denver International Airport employed 100% employee screening before the 9/11 attacks but "had to stop" because the airport frequently discovered too many drugs.[170] Conducting screening is an intuitive response to insider threat smuggling operations. However, once the operator detects elicit activity (an alarm), regardless of the employee's motivation, alarms must be resolved via secondary inspection, investigation, and at times prosecution and extensive employee relations. Simply stated, airports have found the costs associated with responding to and resolving alarms more burdensome than anticipated, which extends the basic cost for security systems. Alarm resolution plays a role in their decision-making. Airports are not naturally incentivized by the common good or their place in the system to invest in security, especially when the detection of contraband and illicit activity causes extraneous costs to the business model from the agent's perspective.

Secondarily, this absence of natural incentives to invest in such security is amplified by insurance markets that cover acts of terrorism and other AIP activity, such as theft. Third-party and public liability insurance is a growing market, particularly in North America, and it provides airports broad support and shields them from economic damages in the wake of various catastrophes, including those caused by AIP.[171] Multiple analyses of the public liability market in the aviation sector pegs its valuation at over $2 billion

169 Adam Rose et al., "The Role of Behavioral Responses in the Total Economic Consequences of Terrorist Attacks on U.S. Air Travel Targets," *Risk Analysis* 37, no. 7 (2017): 1415, https://doi.org/10.1111/risa.12727.

170 Jon M. Loffi and Ryan J. Wallace, "The Unmitigated Insider Threat to Aviation (Part 1): A Qualitative Analysis of Risks," *Journal of Transportation Security* 7 (2014): 321, https://doi.org/10.1007/s12198-014-0144-4.

171 Ionut Valentin Lom, "Current Global Trends of Aviation Insurance," *INCAS BULLETIN* 14, no. 4 (December 2, 2022): 197, https://doi.org/10.13111/2066-8201.2022.14.4.16.

through 2028, demonstrating broad participation by airports in the insurance market.[172] This participation effectively eliminates the incident costs for each agent.

2. Extending and Revising the Model

Integrating the observations from the previous model is straightforward, presuming insurance market participation by the agent airports:

- the agent-level consequence of the incident (C_L) is replaced by the Cost for Liability Insurance (C_{LI}), which is then fixed at 1% of M, a value intended to account for typical insurance premiums;[173]
- costs associated with any deductible will be included in C_{LI}; and
- a new variable for operating cost delta is further added to demonstrate the additional costs associated with each airport's choice to invest in illicit activity detection (C_O), valued at 0.2% of M when investment is chosen.

In this scenario, to capture these adjustments, the payoff function = M-C_I-C_O-C_{LI}. This game, illustrated in Table 3, better represents the observed dynamics, providing a more complete, though complex and accurate, perspective on the real impasse at which many airports find themselves. There is little real incentive for airports to invest in security measures which seem essential to the common good. This observation is compounded when insurance becomes an option to mitigate capital loss. This game may further explain much of the resistance by airport associations to TSA's expanding requirements for aviation worker screening observed during 2023.[174] Profit and loss are primary motivators for system operators, including self-sustaining enterprises such as airports.[175] National

[172] Lom, 198–99.

[173] Risk Management Group, "General Liability Insurance for Airport Service Providers," Risk Management Group, accessed December 8, 2024, https://trmg.net/policies/airport-service-liability/; Sunset Aviation Insurance, "Airport Liability Insurance," Sunset Aviation Insurance, Persistent and Undated, https://sunsetais.com/airport-liability-insurance/.

[174] Airports Council International, "ACI-NA Position on TSA's Aviation Worker Screening National Amendment."

[175] Krishnan et al., "How U.S. Airports Could Make the Most of Additional Liquidity."

security may benefit from acknowledging and working with these drivers, not disregarding them.

Table 3. Airport MDT Game 2

		Airport 2 (A2)	
		I	P
Airport 1 (A1)	I	$920,000, $920,000	$920,000, $990,000
	P	$990,000, $920,000	$990,000, $990,000

3. Incentivized Security

Given this scenario and its problem set, there are at least two potential alternative mechanisms to incentivize agent participation:

- Subsidization: Subsidies through grants or tax credits may be provided for activities that generate positive externalities. For example, governments sometime apply subsidization programs to education, childbirth, homeownership, or renewable energy projects to encourage more investment in these socially beneficial activities.[176]
- Pigouvian Taxation: These taxes are imposed on activities that generate negative externalities. For instance, a carbon tax on emissions incentivizes firms to reduce

[176] Mark P. Keightley, *Why Subsidize Homeownership? A Review of the Rationales*, CRS Report No. IF11305 (Washington, DC: Congressional Research Service, 2019), 1–3; Oiwan Lam, "Can Childbirth Subsidies Solve South Korea's Low Birth Rate?," Global Voices Online, May 20, 2024, https://globalvoices.org/2024/05/20/can-childbirth-subsidies-solve-south-koreas-low-birth-rate; *Why Should Taxpayers Subsidize Poverty Wages at Large Profitable Corporations?; Hearing Before the Committee on the Budget, United States Senate*, 117th Cong. 1 (2021).

pollution, as they now bear the cost of the environmental damage they cause.[177] In this case, though not the cause of insider threats, an externality, airports are the target.

Neither option nor a combination of these options would require airports or their tenants to pay directly or completely for security improvements. While competition may prevent airports from raising fees to recoup investment, well-constructed government intervention compels investment in security while also distributing the cost to secure the system across the transportation sector or beyond, securing the common good with common resources.

For this incentivized game, presume that Congress has identified insider threat mitigation as a priority and has determined to impose a fee or tax equal to $50 per privileged employee per year.[178] This is a significant amount of money that will affect the business model of each airport subject to the tax scheme. Economic studies focused on the impact of incentivizing tax structures has repeatedly found that they are capable of changing business behavior.[179] For an airport like Los Angeles International Airport (LAX), operated by Los Angeles World Airports (LAWA), with an estimated 30,000 employees, this results in a taxed revenue of $1.5 million per year (Employees X Fee = taxed amount). These fees are significant but not daunting considering LAX's published net income during 2023 and forecasted net revenue for 2024, $1.7 billion and $2.0 billion, respectively.[180] However, this new fee might also be understood by comparing it against

[177] Jon Strand, *Importer and Producer Petroleum Taxation: A Geo-Political Model*, vol. 2008 (Washington, DC: International Monetary Fund, 2008), https://www.elibrary.imf.org/view/journals/001/2008/035/article-A001-en.xml; Koskela Erkki and Ollikainen Markku, "Optimal Design of Forest Taxation with Multiple-Use Characteristics of Forest Stands," *Environmental and Resource Economics* 10, no. 1 (July 1997): 41–62, https://doi.org/10.1023/A:1026472622826; Sarr Hamet, Mohamed Ali Bchir, and François CoChard, "Is the 'Average Pigouvian Tax' Robust to the Size of the Group of Polluters?," *Review of Agricultural, Food and Environmental Studies* 102, no. 3 (September 2021): 285–95, https://doi.org/10.1007/s41130-021-00145-z.

[178] In general, airport operators pay little to no federal taxes at present, through there are fees imposed on airport activities for various purposes. If the reader wishes, consider these taxes instead as fees per employee. The term tax was chosen to align with historical use of the term Pigouvian.

[179] Ajay Agrawal, Carlos Rosell, and Timothy S Simcoe, "Tax Credits and Small Firm R&D Spending" (Working Paper, Cambridge, MA, National Bureau of Economic Research, 2019), 28.

[180] Los Angeles World Airports, *Fiscal Year 2023–2024 Proposed Budget* (Los Angeles: Los Angeles World Airports Board of Airport Commissioners, 2023), 4, https://www.lawa.org/-/media/lawa-web/lawa-investor-relations/files/lawa-annual-budget/2023/lawa-annual-budget-fy-2024.ashx.

other available budget lines: for instance, a $1.5 million tax liability is 3% of the funds requested by the airport operator for planning capital improvements and 2% for vehicle and equipment purchases. While the budget, fees, and outlays are significant, the LAWA budget indicates budget flexibility in response to incentives.[181] Finally, while LAX is not every airport (once you have seen an airport, you have seen one airport), these fees do not implement a market of unfair competition. All commercial airports would be required to participate in the same market with the same new rules, and the number of employees (a value controlled to an extent by the operator) serves as a proxy for proportion tax burden; all airports are affected equivalently and fairly. This rational is supported by multiple analyses including that of Airports Council International (ACI) and International Civil Aviation Organization (ICAO), which both have indicated that commercial airports can operate profit margins above 15% and tend to achieve such margins above one million passengers per year, Figure 4.[182]

[181] Los Angeles World Airports, 7.

[182] Infrastructure Management Programme and Airports Council International, *State of Airport Economics* (Montreal, Canada: International Civil Aviation Organization, 2015), 5, https://www.icao.int/sustainability/airport_economics/state%20of%20airport%20economics.pdf.

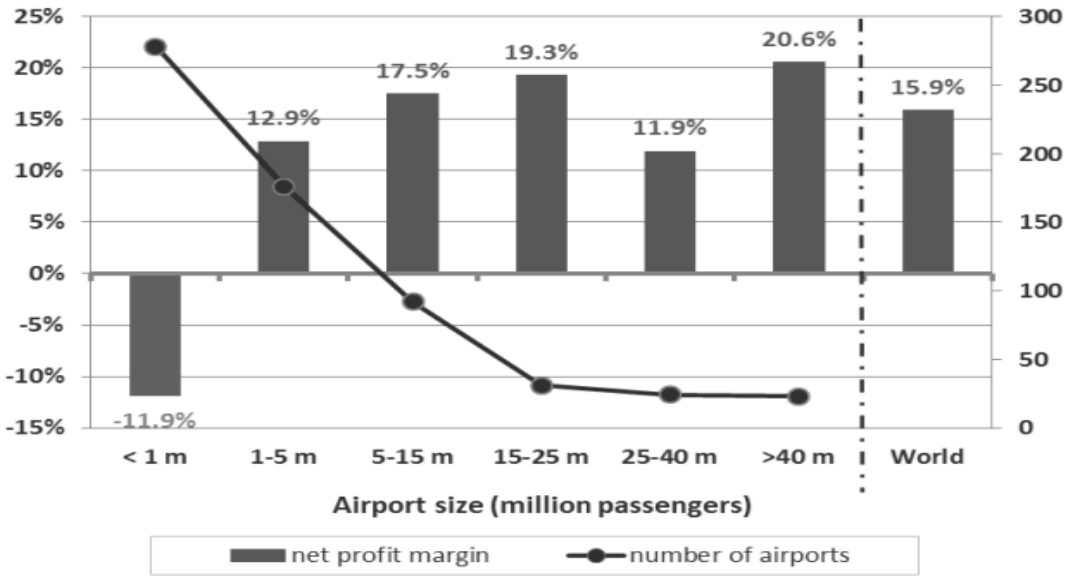

Figure 4. Airport Net Profit by Passengers Per Annum[183]

To apply this tax structure to counter AIP action, these funds could be itemized for deduction if reinvested for insider threat security enhancements or granted back to airports through federal oversight. To reduce administrative costs and decrease market friction, itemization and deduction may be preferred by some government organizations even though this may increase the potential for fraudulent airport activity investment and tax activity. Therefore, in this incentivization model, airports are encouraged to spend money on AIP mitigation activity consistent with federal guidelines to reduce tax liabilities otherwise imposed by legislation.

While airports have many options to invest their income this game will specifically consider the procurement of security teams that would be directed to conduct screening, surveillance, and other interventions to counter AIP. Considering the average salary for security services in the Los Angeles market of $55,000 per year, plus a percentage of 15% for benefits and capital investment associated with each security worker, each would cost

[183] Source: Infrastructure Management Programme and Airports Council International, 5.

$63,250 annually.[184] Adding management overhead ($75,000) to these employees at a rate of 1:6, a conservative span of control for management, provides a security staffing function of ($63,250 *6) + $75,000 = $454,500. An annual $1.5 million expenditure against the privileged employee tax might be used to implement as many as 3.3 screening units of 6 screeners, capable of cumulatively producing as many as 32,950 hours of security activity per year or 2,745 hours per month. This calculation includes an adjustment for 20% of the hours paid as time not worked, such as training and leave, consistent with general human resources practices. While some resources may be used for physical screening and security, other teams could focus on preliminary intervention and investigation to resolve and mitigate at-risk or suspected individuals, augmenting existing law enforcement and intelligence efforts.[185] Despite significant existing airport investments in law enforcement and security, the increased targeted spending may yield considerable investment in AIP mitigation activity given evidence of ongoing smuggling activity.

Using the previous model but adding tax liability (T_L*Number of Employees), the payoffs may be calculated as illustrated in Table 4, Airport MDT Game 3, with an adjusted payoff function of $M-(T_L-C_I-C_O)-C_I-C_O-C_{LI,}$ where M is Profit, T_L is Tax Liability, C_I is cost to invest or investment, C_O is cost to operate, and C_{LI} is the cost of loss per incident, including insurance modifications, presuming that a tax credit is provided for airport agent investment in security to a maximum amount of the tax rate paid by the airport—in this model, set at 25% of M—which is far more than the investment.

[184] Citiguard, "How Much Does It Cost to Hire a Security Guard?," Citiguard, February 15, 2024, https://www.mysecurityguards.com/blog/how-much-does-it-cost-to-hire-a-security-guard/; ZipRecruiter, "$16-$37/Hr Airport Security Screener Jobs in Los Angeles," ZipRecruiter, accessed December 8, 2024, https://www.ziprecruiter.com/Jobs/Airport-Security-Screener/-in-Los-Angeles,CA.

[185] Scott Zamost and Morgan Brennan, "Take a First-Ever Look at How LAX Airport Targets Threats from Airport Workers," Airlines, September 7, 2017, https://www.cnbc.com/2017/09/07/inside-lax-airport-security-as-it-targets-insider-threats.html.

Table 4. Airport MDT Game 3

		Airport 2 (A2)	
		I	P
Airport 1 (A1)	I	$740,000, $740,000	$740,000, $740,000
	P	$740,000, $740,000	$740,000, $740,000

This game demonstrates how a subsidy and tax incentive system can be applied by regulators and lawmakers to incentivize airport operator decision-making on economic terms. Applying tax and credit mechanisms in this simple model has removed economic pressure to abstain from investment. The model becomes perfectly symmetrical and unnaturally smooth. There are admittedly unidentified effects associated with such a proposal: while the consequences of such actions are not fully explored, one positive tangential effect is additional pressure on airports to minimize the number of individuals with privileged access as the cost of investing in additional security is tied directly to the proportionality to the number of insiders. Further, such an approach, for better or worse, scales the needed investment roughly to airport size, this model demonstrates that under certain conditions, particularly when facing threats that will cause more harm to the system than to any individual and insured agent in the system, shared security systems could benefit from an economically minded regulatory hand.

MDT thus provides a helpful framework for observing and assessing agents in such well-regulated institutions. Using this frame to determine airport participation in security markets, even in simple modeling, has illustrated many obstacles preventing significant voluntary investment in security measures above-and-beyond regulatory requirements. Most, not all, commercial airports are business ventures. This frame has reinforced the importance of economic implications and influences inherent to security investment decisions. Further, MDT has demonstrated that economic incentive schemes exist and that

they may be used to drive significant investments in improved security features specifically intended to mitigate threats posed by AIP.

C. ADAPTED MDT—A SEQUENTIAL ADVERSARY-DEFENDER GAME

This section will shift the focus of analysis from the airport agents to the AIP, placing them at the center of the problem at hand, and will permit a comprehensive inventory of economic perspectives while considering the extensive case analysis. AIP are likely less concerned about the macroeconomic implications of security features and more interested in avoiding the more immediate consequences of their adversarial goals. Dynamic games are more applicable modeling tools to better understand strategic situations where players (in this case, airport personnel and potential insiders) make decisions over time, with each decision potentially affecting future actions and outcomes. These games are suitable for simulating complex, evolving security scenarios and capturing strategic interactions between insiders and security personnel. The method can accommodate changes in tactics and strategies over time, reflecting the adaptive nature of threats and responses. For this research, the underlying concepts of MDT are also being combined with counterfactual analysis and thought experiments, all of which are being adapted to the construction of hypothetical attacker-defender games in the hopes of providing insights into multi-agent environments which are closer virtualizations of real-world critical infrastructure, while providing a structured environment to evaluate the effectiveness of various security strategies. The fundamental premise is to design the game's rules so that the best strategy for the participants leads to the optimal outcome for the security system as described by the social choice, payoff functions.

1. MDT Applied to Adversarial Gaming

MDT can be applied to adversarial games, even though the theory is not made specifically for this purpose. MDT concepts permit game developers to enforce incentives/ disincentives in simulation. Such capability is useful in crafting systems where the objectives of self-interested agents align with simulation or institutional objectives, even under conditions of incomplete information, as the variables are systematic and not

necessarily agent dependent.[186] Traditionally, the application of this theory drives micro-economic market games. As this research focuses on assessing AIP activity as an economic enterprise, this theory becomes a very useful tool, especially considering the relationship between AIP resource utilization and their perceived attack value. The application of MDT to adversarial games requires a deeper understanding of several essential concepts:

- Social Choice Function/Payoff Function—A social choice function represents the optimized outcome for all self-interested parties in the context of the institutional design. In such an outcome, all agents achieve maximum utility value.
- Individual Rationality—All agents participating in the system and its mechanisms have full knowledge of their role as either adversarial agent (AA) or security agent (SA). However, while the AA has nearly perfect information, the SA can only possess limited or revealed information about other agents. Furthermore, the agents may have incomplete information regarding the mechanism itself.

MDT describes several concepts and practices that lend themselves to simulating hypothetical institutions outside of purely economic games. As previously discussed, MDT has not been directly applied to adversary-defender game modeling. The purpose of mechanism design is to understand systems of economic actors and apply incentives to ensure optimized action by rational actors. Even though MDT was not created to analyze security games, it has been used in security settings and serves in this thesis as the kernel of analysis: how can a system be modified to incentivize polite behavior and inhibit AIP? Applying MDT concepts to this simulation provides necessary support and stimulates the creation of protocols that can reflect real-world security scenarios and, at a minimum, informs an approximate social choice function.

2. Combining MDT and Attacker-Defender Games

Integrating mechanism design into attacker-defender simulations offers several benefits, including enhanced predictive power, the ability to model complex interactions,

[186] Andreu Mas-Colell, Michael Dennis Whinston, and Jerry R. Green, *Microeconomic Theory* (New York: Oxford University Press, 1995), 29.

and the provision of a systematic framework for evaluating security measures. In the context of MDT, a single airport security system can be considered an institution and further simplified in an illustrative model to facilitate further design and testing. An airport is a complex set of interconnected systems through which security measures are applied. In attacker-defender games, mechanism design thus simulates the strategic interactions between attackers, who seek to breach security, and defenders who aim to thwart these efforts. The individuals activated in such a system are AIP, referred to as adversarial agents (Aas), and airport security agents (SAs). With these agents in mind, the design might include randomized security checks, multi-layered defenses, and adaptive response strategies, all tailored to the insights gained from previous analysis real-world data via the case studies. Researchers can identify optimal strategies and vulnerabilities by iteratively testing these models and refining security measures to enhance resilience against evolving threats. These simulations help stakeholders visualize the potential outcomes of different security strategies, fostering a deeper understanding of the tradeoffs involved in security decision-making.

While MDT-driven games are an effective tool for assessing systems, challenges such as the need for accurate modeling of attacker behaviors, the complexity of delimiting real-world scenarios, and the computational demands of running large-scale simulations remain. For instance, uncertainty is a crucial real-world component of modelling AIP and defender decisions. While AIP have the opportunities, training, and connections to develop a detailed operating picture of security activities, security systems are challenged to identify an adversary in an environment filled with look-alike targets as demonstrated in the cases analysis where compromised security agents, flight crew, and ground crew were all capable of illicit activity for significant periods of time without detection. Sequential games help model strategies under these asymmetrical uncertainties, providing a more realistic assessment of specific security measures and mixtures of these tactics.

The sequence of these games consists of the SAs deploying tactics throughout the simulated space consisting of the perimeter to the secured area, the secured area of an airport, and assets within the secured area, and the AA selecting responses to these deployments. The desire for the AA is different than that of the SA, and each is represented

by a distinct payoff function. The social choice function for the game, describing the overall goodness of the system is represented by dominant strategies and equilibria, commonly referred to as Nash equilibria, at which points the choice to alternate a strategic selection would not result in a better payoff for either agent. By considering AA's potential for strategic behavior, these sequential games offer insights into how security protocols can be designed to preempt and counteract adversarial behavior using sets of probable security tactics.

D. A GAME OF WATER AND DANGEROUS DRUGS

To assess the most critical components related to adversarial attack a model must reduce the complicated nature of an airport, which may be distilled to interconnected systems consisting of ground transportation, aircraft services, cargo, baggage, concessions, passenger screening, and many other elements intended to facilitate commercial air traffic. These systems must then be delimited and aggregated to capture the relevant systems and aspects of a commercial airport as they are applicable to AIP and defense against insider threats:

- This model provides strategic choices for the security agents, AIP, and the basic layout of an airport: a secured area with assets, perimeter access points from unsecured areas to secured areas, and screening efforts to mitigate threats. Consider an AIP with a consistent intent to harm the system within which the AIP has consistent interaction and broad access.
- This model considers an institution that deploys physical screening randomly to all employee access points within an airport, such that every third employee receives some level of physical screening. Presuming that the deployment is incomplete and randomly initiated at access points, there is some probability that the AA will encounter physical screening at an access point. This probability of encounter is defined as the likelihood that an aviation worker will be confronted by screening upon selection, transiting an access point, given the 1:3 ratio of aviation workers selected for screening at any given access point. This probability

would be affected by the number of access points available to the AA in relation to the number of access points supporting random screening at any given time.

- Further, the model acknowledges that AA possesses perfect or near-perfect information regarding the deployment schedules of the screening teams given the lessons learned from the case studies: lookouts, inside information, and opportunity to send contraband around screening procedures, such as by throwing it over a fence for retrieval. Finally, the probability that screening would result in detection would further affect the payoff function for an adversarial actor.
- The model also considers alternative options for physical screening. Screening activity is not anchored to access points. Instead, the practical decision to base screening operations at access points appears rooted in the perception that more screening equates to better screening or more effective deterrence. Alternative options are instead available to SA to compare static screening randomly deployed to access points alongside random screening performed dynamically within the secured area. This suggestion fits analysis from the beginning of the century related to profiling effects on crime rates in airport security – targeting high-risk populations does not necessarily decrease the overall crime rate due to the potential to adapt or disguise as a trusted individual.[187] Random inspections can be effective at improving security system performance.[188] This alternative option is significant due to the prevalence of AAs to adapt their behaviors as acutely observed in cases 1 and 3.

The following games have two objectives: assess the economic value of AIP activity under limited assumptions and understand the relationship between AIP and the airport operator. To meet these objectives, the games are designed, assessed, modified, and repeated while applying the concepts of MDT to evaluate economic impact based on

[187] Nicola Persico and Petra E. Todd, "Passenger Profiling, Imperfect Screening, and Airport Security," *The American Economic Review* 95, no. 2 (2005): 131, https://www.jstor.org/stable/4132803.

[188] Levine, Toffel, and Johnson, "Randomized Government Safety Inspections Reduce Worker Injuries with No Detectable Job Loss," 910; Ryan J. Wallace and Jon M. Loffi, "The Unmitigated Insider Threat to Aviation (Part 2): An Analysis of Countermeasures," *Journal of Transportation Security* 7 (2014): 325, https://doi.org/10.1007/s12198-014-0150-6.

adversarial and security agent decisions and system incentivization. The design of the games considers the following elements: players and strategies, a thought exercise-driven scenario, estimations, payoff functions, and analysis.

1. Game 1

Consistent with the discussion above, the game is defined:

a. Roles and Strategies

The AA seeks to attack a critical component within the security area for which SA is responsible. The game's scope and analysis will be a single attack path. In scoping this way, the costs associated with each agent's actions are normalized. Any game modeling an AA and SA should consist of limited sequential action in which the SA acts first and the AA responds. This is partially caused by the fact that the SA is unaware of the AA's impetus and can only seek to predict the AA's strategy and prevent illicit activity. In this way, the AIP is the focal point of the game, reacting to the mechanism that the security agent has implemented.

The AA's objective in this game is to gain access to assets in the secured area with an illicit payload. The strategies available to an actual insider are manyfold; however, the model is a simple representation of these options. Where there is known screening activity, the AA can choose to defeat security and enter with the illicit material, thus challenging the probability that they will be selected for screening by the SA or challenging the likelihood that screening would successfully detect the illicit material (Strategy 1). Alternatively, the AA may pass the material through the perimeter and retrieve it once in the secured area, challenging the likelihood that the activity would be detected or prevented at the perimeter or the secured area (Strategy 2). Or the AA may pass, taking no action, and choose to wait until the next turn (Strategy 3). Condensing available actions into these three strategies permits the model to constrain the real slate of potential adversarial strategies while retaining the qualitative aspects of adversarial decision: flexibility and initiative. Finally, the access point, perimeter fence, and secured area are presumed to be simple checkpoints through which the AA may transit, during this transit the AA may

encounter screening. The AA may only be detected if carrying illicit material during the screening.

Conversely, the SA seeks to detect or delay the AA, presuming that such a strategy reduces losses. The SA may choose to conduct security screening at the access point (Strategy 1). The SA may perform security operations in the secured area containing the critical component (Strategy 2). Alternatively, the SA may patrol the perimeter (Strategy 3). Finally, the SA may choose to mix strategies in some proportion between the access point, the perimeter, and the secured area (Strategy 4—Balanced).[189] A balanced strategy is available to the SA and not the AA. At the same time, the AA has the initiative to act. While the AA may choose to pass, the SA must always act: the airport operator has purchased security resources, and it would be economically irrational to spend the money and achieve no benefit.

b. A Scary Scenario

For a more tangible scenario, the model for this game reflects an AA plan to smuggle a significant amount of nearly pure fentanyl into the secured area of an airport for delivery to three aircrafts' potable water tanks to maximize death and disruption. While unproven for this specific application, the use of opioids as a chemical weapon has been historically demonstrated.[190] Given its availability and ease of production, fentanyl is a

[189] This mixed strategy does not mean to state that a probabilistic and technical mixed strategy as often described in game theory; rather, this mixed strategy provides a randomized mix of investments for the SA that the AA may not be able to adequately predict nor perfectly plan around.

[190] John P Caves Jr., "Fentanyl as a Chemical Weapon," in *Proceedings* (Center for the Study of Weapons of Mass Destruction Symposium, National Defense University: CSWMD, 2019), 2–4, https://wmdcenter.ndu.edu/Portals/97/CSWMD%20Proceedings%20Dec%202019.pdf.

compelling attack vector.[191] Fentanyl is water-soluble, tasteless, and odorless.[192] While the water systems for aircraft are primarily used for lavatory functions, they also typically supply the water for coffee, tea, and, for some aircraft operators, all drinking water.[193]

The tanks on an average aircraft hold about 1,000 liters.[194] While most aircraft employ some level of water treatment, such as filtration and/or ozonation, given the tiny size of fentanyl particles (0.2–2 microns) and its relative molecular stability, filtering and treatment processes are generally ineffective against fentanyl contamination, with a significant percentage of the molecules escaping and surviving such processes.[195] A lethal dose of fentanyl is reported to be as little as 2 mg. However, some literature indicates that through oral absorption, a more effective lethal dose is closer to 20 mg.[196]

---

[191] Maurice Tamman, Laura Gottesdiener, and Stephen Eisenhammer, "We Bought What's Needed to Make Millions of Fentanyl Pills–for $3,600," Reuters, July 25, 2024, https://www.reuters.com/investigates/special-report/drugs-fentanyl-supplychain/; Susan M. Cibulsky et al., "Public Health and Medical Preparedness for Mass Casualties from the Deliberate Release of Synthetic Opioids," *Frontiers in Public Health* 11 (May 12, 2023): 5, https://doi.org/10.3389/fpubh.2023.1158479; Caves Jr., "Fentanyl as a Chemical Weapon," 4; Megan Craig, "Fentanyl Could Be Weaponized and Used for Terroristic Mass Poisoning," News Medical, June 1, 2023, https://www.news-medical.net/news/20230601/Fentanyl-could-be-weaponized-and-used-for-terroristic-mass-poisoning.aspx.

[192] Department of Homeland Security, Office of Science and Technology, "Master Question List (MQL) for Synthetic Opioids" (Washington, DC: Department of Homeland Security, Office of Science and Technology, September 2021), 2, https://www.dhs.gov/sites/default/files/publications/21_1110_st_csac_mql_synthetic_opioids_30sep2021_pr_508.pdf; Wisconsin Department of Health Services, "Dose of Reality: Get the Facts on Opioids," Wisconsin Department of Health Services, January 30, 2022, https://www.dhs.wisconsin.gov/opioids/facts.htm.

[193] Johnny Jet, "You Probably Won't Be Drinking the Water, Coffee or Tea on Airplanes After Reading This," Johnny Jet, May 7, 2024, https://johnnyjet.com/you-probably-wont-be-drinking-the-water-coffee-or-tea-on-airplanes-after-reading-this/; Zach Wichter, "Is Airplane Coffee and Tea Safe to Drink?," *USA Today*, August 2023, Online edition, sec. Cruising Altitude, https://www.usatoday.com/story/travel/columnist/2023/08/23/airplane-coffee-tea-safe-drink/70653256007/.

[194] Timothy Estrella, "Airplane Water and Wastewater Systems," Aerospace and Defense, May 2021, https://insights.globalspec.com/article/16509/airplane-water-and-wastewater-systems.

[195] Drug Enforcement Agency, "Facts about Fentanyl," United States Drug Enforcement Agency, 2023, https://www.dea.gov/resources/facts-about-fentanyl; Garyfalia A. Zoumpouli et al., "Simultaneous Ozonation of 90 Organic Micropollutants Including Illicit Drugs and Their Metabolites in Different Water Matrices," *Environmental Science: Water Research & Technology* 6, no. 9 (2020): 2473–74, https://doi.org/10.1039/D0EW00260G; Raven Reitstetter and Travis Losser, "The Synthetic Opioid Fentanyl Is Degraded by Temperature and Ultraviolet Irradiation in the Environment," Environmental Protection Agency, January 2017, https://www.epa.gov/sites/default/files/2018-11/documents/decon_poster_099.pdf.

[196] Karina Sommerfeld-Klatta et al., "Severe and Fatal Fentanyl Poisonings from Transdermal Systems after On-Skin and Ingestion Application," *Toxics* 11, no. 10 (2023): 4–5, https://doi.org/10.3390/toxics11100872.

To ensure a higher mortality rate upon exposure and higher valuation, the AA might choose a dose of 20 mg per 180 ml consumed liquid, equal to about a 6 oz cup of coffee or tea.[197] This plan would require about 111 grams of fentanyl per aircraft given the equation of 20 mg * (1000L/.18L) where the average clean water tank for an aircraft is about 1000L, or about 5,500 lethal doses for each aircraft. This amount, ten ~30-gram packages, each about the size of a deck of cards, fits into typical uniform pockets or could be disguised as lunch items as shown by Figure 5. Of course, if the fentanyl were pure, with a density between 1.064 and 1.142 g/cm^3 varying by analog, 300 grams would fit neatly inside one 12 oz thermos. This payload could presumably be supplied to the aircraft holding via the supply hose connection.

[197] Megan Becker, "Four Charged in Chillicothe after Drug Search," *Chillicothe Gazette*, June 23, 2022, https://www.chillicothegazette.com/story/news/2022/06/23/four-charged-chillicothe-after-drug-search/7710872001/; WSYX Staff, "Chillicothe SWAT Team Seizes 38 Grams of Fentanyl in Drug Bust," WSYX, June 23, 2022, https://cwcolumbus.com/news/local/chillicothe-swat-team-seizes-28-grams-of-fentanyl-in-drug-bust-detective-division-search-warrant-crack-cocaine-paraphernalia-charges-jefferson-avenue.

Figure 5. ~38 Grams of Seized Fentanyl Prepared for Distribution Demonstrating Compact Size[198]

c. Estimating Loss

The consequence of a successful attack of this type can be estimated in two ways. The local loss to the airport authority and its tenants is as described, sans rebuilding:

- The cost to shut down air operations at a single port is unlikely to exceed one-half of the previously identified $3 million, or $500,000 per day, including the trailing investigation and security costs.[199]
- In an attack perpetrated on three aircraft, the damage caused to the system is estimated by cost in lives: conservatively, 10% of 320 passengers on each of two aircraft, and all lives and a total loss of the third aircraft.[200] A recent value of a statistical life (VSL) analysis within the transportation environment provides an

198 Source: WSYX Staff, "Chillicothe SWAT Team Seizes 38 Grams of Fentanyl in Drug Bust."

199 Rose et al., "Consequences of Terrorist Attacks on U.S. Air Travel Targets," 1415.

200 Airways Staff, "Airways Top 10 Largest Passenger Aircraft in Service," *Airways Magazine – Airlines*, May 18, 2024, https://airwaysmag.com/new-post/top-10-largest-passenger-aircraft – These figures would apply to the smallest of the big commercial aircraft and align to prior terrorist selections of aircraft.

average valuation of approximately $7.1 million per life lost within developed countries.[201] The highest valuations in the reviewed study approached $2 billion, indicating some disagreement. This model will convert each human life to a monetary value of $7.1 million, adopting the most conservative estimation to ultimately restrain adversarial payoffs. At $7.1 million per statistical life, this portion of a successful AA attack cost is $2.726 billion.

- The cost of aircraft replacement, $25 million depreciated cost for the average commercial airliner, is added to this value for a total cost of at least $2.78 billion.[202]
- The system cost is beyond the validation of this research. Still, given the analysis of previously discussed incidents, it would likely exceed $3 billion, including stoppages, inspections, subsequent security measures, and practical changes to service and equipment.

d. Estimating Probabilistic Security Values

The security value of strategies employed by the SA informs the payoff function of the AA. The model's detection algorithms must be estimated to ensure that the payoff calculations in the model approximate reality in reflecting agent rationality. The security value of the system depends on the strategic choices of SA and AA. The probability of an encounter is reduced by the expected security value of SA choice. This factor is a fractional number, less than one and greater than zero (*Security Value = Probability of Encounter X Probability of Detection*). Many factors affect the actual probability of encounter and actual effectiveness of any security measures. Therefore, less-than-perfect procedures and less-than-complete encounter rates will consistently demonstrate a security value of less than 1 for any random encounter, as illustrated by Table 5.

[201] Elena Keller et al., "How Much Is a Human Life Worth? A Systematic Review," *Value in Health* 24, no. 10 (October 2021): 1536, https://doi.org/10.1016/j.jval.2021.04.003.

[202] "Airbus A320 Charter – Rental Cost and Hourly Rate," Paramount Business Jets, accessed July 12, 2024, https://www.paramountbusinessjets.com/private-jet-charter/aircraft/airbus-a320.

Table 5. Security Value Table

Security Value Table		Liklihood									
		0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
Effectiveness	0.1	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09	0.1
	0.2	0.02	0.04	0.06	0.08	0.1	0.12	0.14	0.16	0.18	0.2
	0.3	0.03	0.06	0.09	0.12	0.15	0.18	0.21	0.24	0.27	0.3
	0.4	0.04	0.08	0.12	0.16	0.2	0.24	0.28	0.32	0.36	0.4
	0.5	0.05	0.1	0.15	0.2	0.25	0.3	0.35	0.4	0.45	0.5
	0.6	0.06	0.12	0.18	0.24	0.3	0.36	0.42	0.48	0.54	0.6
	0.7	0.07	0.14	0.21	0.28	0.35	0.42	0.49	0.56	0.63	0.7
	0.8	0.08	0.16	0.24	0.32	0.4	0.48	0.56	0.64	0.72	0.8
	0.9	0.09	0.18	0.27	0.36	0.45	0.54	0.63	0.72	0.81	0.9
	1	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1

Given these considerations, the security values for each strategy are set as follows:

- SA Strategy 1: For an access point deployment in this scenario, the expected security activities at an access point will occur at regular intervals; for every three employees using the access point, only one will be exposed to security activity (.33) given the one to three screening ratio previously discussed. For this model, the effectiveness score will be set at 0.5, meaning that the security procedures are expected to discover half of the threats present, resulting in a security value of 0.15.
- SA Strategy 2: In any system with more than one access point to a secure area, there are more aviation workers present in the secured area than would be encountered at any single access point. However, the number of aviation workers screened may be reduced by movement time and space between employees available for screening within the secured space. Conversely, employees may avoid locations where screening is occurring at access points, a more difficult proposition in their area of work. Therefore, the likelihood of an encounter is similar, at 0.3, effectiveness is similar at 0.5, thus providing a security value of 0.15.
- SA Strategy 3: The strategy of focusing security activity along the perimeter of the secured area is intended to address the AA's capacity to move freely within the secured area and bypass screening activity elsewhere. Though imperfect, patrols are highly effective at detecting past and present physical security breaches, set at 0.9. However, despite this effectiveness, it is assumed that all perimeter areas are not continuously monitored. LAX's perimeter fence is about 9 miles long and complicated by various terrain, a difficult space for four security teams to maintain observation.[206] Assuming that a security team can effectively monitor 0.11 miles of fence at any given time, this model will fix the probability

[206] Stronghold Engineering, "Air Operations Area Perimeter Fence Project," Stronghold Engineering, September 21, 2012, https://www.strongholdengineering.com/projects/air-operations-area-perimeter-fence-project/.

of encounter at 0.05. The security value of SA (S3) is therefore calculated at 0.045.

- SA Strategy 4: Strategy 4 is an equally, not optimally, mixed application of the previous three strategies, resulting in the sum of 1/3 of each of the above security values distributed against various AA strategies. SA Strategy 4 results in a variable security value, depending on the AA's chosen plan.

e. Payoff Functions

Probabilities of attack success further modify the potential outcomes of agent strategies. Different AA strategies probabilistically result in successful adversarial activity depending on the security value of the SA strategy. The value for the AA in this model is calculated as the attack value previously estimated at $2.78 billion multiplied and reduced by some expected probability of success independent of SA strategy – a success or failure rate depending on the agents' perspective. A conservative adversary may consider this likelihood of success meager as she imagines the ways in which she may fail. A confident actor who has planned well might eliminate some of this probability of failure. For this model, we will modify the attack value by 0.03, presuming that the AA believes that they will only be successful 3% of the time, regardless of SA's efforts to detect and disrupt the AA's strategy.

Payoff for the SA is calculated on two fronts: for the airport, the loss is estimated as a sum of the valuation of the expected deaths, cost incurred due to local damage and investigation, insurance costs, and cost of ongoing and increased security operations (loss on AA success). The loss to the SA is moderated, as the single SA (airport) will only absorb a fraction of the damage, as the greater remainder is absorbed by the extra-model system. The cost of operations was previously explored and set at a $1.5 million yearly investment to provide several security teams. This realistic annual investment would provide for four security teams and their leadership in the Los Angeles investment market. Given this example, the cost of operation can also be estimated at 0.007% of an airport's revenue. Still, given the variances in airport size and performance across the U.S., it is unlikely that this ratio would provide applicable insights into economic performance across all airports.

Despite this limitation, any realistic valuation is helpful toward constructing an accounting of airport operating costs, and anything learned from such valuation is still relevant even if airport size requires future modification to this model's considerations. Given this value, the cost of strategic security operations is set at 0.007% of airport revenue. The fixed estimate of $2 billion annual income for an airport such as LAX provides $1.5 million for a yearly security investment.

The payoffs for each outcome are moderated by the security value (a probabilistic factor) fixed on each strategy deployed by SA. For any strategy combination for AA and SA, whereas the security value is a probability derived from estimated effectiveness and exposure probabilities unique to the SA's strategy, the utility payoff functions for AA and SA may be described by payoff function, Equations 1 and 2, respectively:

AA Utility (SA Strategy)=((1-Security Value of SA Strategy)*(AA Valuation of (1) Activity))-(Security Value of SA strategy*$7.1 Million)

SA Utility (AA Strategy)=Security Value (Local Value of Attack (2) Prevented/Loss Absorbed)-Operating Cost

f. Analysis

Applying the scope, parameters, payoff functions, and strategies, the best strategy combinations for the AA are as follows: as discussed above, the attacker may choose either the simple action (S1—defeat known security measures at access points), the complex action (S2—circumvent access point security), or the option to Pass (S3—not attack, defer based on defender selection).

- If the defender chooses S1: the best AA response is S2 (Complex), with a payoff of $83,292,000.
- If the defender chooses S2: the best AA response is S1 or S2 (Simple or Complex), with a payoff of $69,733,200.
- If the defender chooses S3: the best response is S1 (Simple), with a payoff of $80,097,000.

- If the defender chooses S4: the best response is S1 (Simple), with a payoff of $74,252,800.

The game illustrated by Table 6 simplifies security systems and demonstrates adversarial flexibility and initiative to act. AA Complex (S2) is a lucrative response to security agent deployments to access points and dynamic deployments, maximizing payoffs at SA1:AA2. SA3:AA1 strictly dominates the board. The system is naturally inclined to restrain the payoff for AA and concedes the ability to prevent an attack at the set exposure rates and system effectiveness. The AA Pass (S3) is strictly dominated by either AA's simple or complex strategies. An attacker could choose to pass but should not pass indefinitely. While repeated iterations will cause the SA to lose its operating cost continually, the AA should eventually choose an active strategy while seeking to produce the most beneficial outcome.

Table 6. Game 1—Attacker Defender

		Security Agent			
		S1 Access Point	S2 Dynamic	S3 Perimeter	S4 Balanced
Adversarial Agent	S1 Simple	AA: $69,733,200, SA: $10,993,800	69,733,200, $10,993,800	$80,097,000, $35,981,400	$74,252,800, $2,664,600
	S2 Complex	$83,292,000, ($1,500,000)	$69,733,200, $10,993,800	$42,615,600, $35,981,400	$65,213,600, $2,664,600
	S3 Pass	$7,100,000, ($1,500,000)	$7,100,000, ($1,500,000)	$7,100,000, ($1,500,000)	$7,100,000, ($1,500,000)

2. Game 2

Game 1 illustrates a simplified security system that fails to incentivize the AA to pass and either shift risk elsewhere or refrain from attack. The system is changed in game 2 to incentivize the pass strategy. Specifically, Game 2 will assess an increase in security resources and determine if such a design modification results in greater balance to the game and the creation of equilibria at AA3.

a. Design Modification of SA Strategies (Incentive Control)

Increasing the airport's investment in security by a factor of 10, presuming linear expansion of the security value, would result in outcomes that rationally force the adversary to pass.[207] A linear effect on the security value of the tactics may be inappropriate. Some have argued from a vulnerability perspective that an exponential relationship exists between vulnerability and investment; however, as Taquechel and Lewis acknowledge, there are varied relationships between investments and vulnerability reductions.[208] Given the low frequency application of security being discussed in this model, linear expansion is an acceptable parameter. The SA strategies available in Game 2 are adjusted as follows:

- Strategy 1 – Value: for an access point deployment in this scenario, the expected security activities at an access point occur for each employee accessing the security-restricted area. The effectiveness score is set at 0.7 and the exposure rate set to 1.0, resulting in a security value of 0.7 (Effectiveness x Encounter) against AA strategies employing illicit activity at the access portal.
- Strategy 2 – Value: the encounter probability is like the previous scenario for a dynamic deployment in the secured area (Game 1). Therefore, the exposure rate is lower than improved access point screening (S1), at 0.7, while the effectiveness is held at 1.0, providing a security value of 0.7 (Effectiveness x Encounter) against all active AA strategies.

[207] This also increases the expenditure from $1.5 million to some amount less than $15 million. $14 million was chosen for modelling presuming that the scaling of activity resulting in a ~10% efficiency gain.

[208] Taquechel and Ted G. Lewis, "More Options for Quantifying Deterrence and Reducing Critical Infrastructure Risk," 8.

- Strategy 3 – Value: patrols are linearly increased by a factor of 10. The security value of SA (S3) is calculated at 0.45 against SA strategies requiring illicit activity at the perimeter.
- Strategy 4 – Value: strategy 4 is an equally, not optimally, mixed application of the previous three strategies, resulting in the sum of 1/3 of each of the above security values distributed against, but dependent upon, a variety of AA strategies.

b. Analysis

As illustrated by Table 7, applying the scope, parameters, payoff functions, and modified SA strategies, the best strategy combinations for the AA are:

- If the defender chooses S1: the best response is S2 (Complex) with a payoff of $83,292,000.
- If the defender chooses S2: the best AA response is S1 or S2 (Simple or Complex) with a payoff of $56,798,200.
- If the defender chooses S3: the best response is S1 (Simple) with a payoff of $80,097,000.
- If the defender chooses S4: the best response is S2 (Complex) with a payoff of $44,122,133.
- Nash Equilibria are observed at Attacker S3, Defender S2: payoff = ($7,100,000, -$5,670,000)

Table 7. Game 2—Increased Resources

		Security Agent			
		S1 Access Point	S2 Dynamic	S3 Perimeter	S4 Balanced
Adversarial Agent	S1 Simple	$6,458,800, $56,798,200	$6,458,800, $56,798,200	$80,097,000, $23,481,400	$32,069,867, $9,599,400
	S2 Complex	$83,292,000, ($14,000,000)	$6,458,800, $56,798,200	$42,615,600, $23,481,400	$44,122,133, $9,599,400
	S3 Pass	$7,100,000, ($5,670,800)	$7,100,000, ($5,670,800)	$7,100,000, ($5,670,800)	$7,100,000, ($5,670,800)

Modifying the design by increasing investment, and therefore security value and resources attributed to SA strategies, results in a more balanced game. The payoffs differ considerably between Game 1 and Game 2, indicating that the investment and, this analysis suggests, exposure rate and screening effectiveness do have a significant impact on adversary valuation and modelled decision-making. Though some themes have carried through to the new scenario, in either game, the parameters do not incentivize a rational security agent to deploy to an access point with the anticipation that static screening permits illicit material to pass around the screening location(s). Notably, AA3 (Pass) is no longer strictly dominated. Most importantly, SA2 compels AA to adopt AA3 (Pass). The tactical selections and level of investment are directly tied to adversarial response and in these games result in the dominance of AA strategy pass, fundamentally supporting the use of dynamic screening tactics, the application of security resources, and the concept of risk-shifting.

E. CONCLUSION

This chapter has focused on using games' analysis using MDT, counterfactual analysis, and thought exercises to model airport, adversarial agents', and security agents' decision-making in airport systems.

- Through the review of agent competition, basic market models affirmed and extended early research demonstrating that agent investment in security improvements is not naturally incentivized. This observation is likely the result of distributed loss: an agent is unlikely to invest in preventing security incidents, including those caused by AIP, because most of the damage in average incidents will impact the system and will likely not be localized and concentrated with the agent making the decision.
- Because the cost to airport agents is not localized and is distributed, it is no surprise that insurance is a significant player in insider risk-mitigation and further influences agent decisions to invest in security improvements independently. Insurance provides a market means of distributing risk and devaluing investment activity.
- Conversely, tax and fee mechanisms and regulatory action incentivize airport investment activity, mitigating system-level risk and preserving the common good at the macroeconomic scale.
- Finally, both adversarial-defender Games 1 and 2 demonstrated that dynamic (unpredictable) SA strategies provide valuable payoffs to the SA. This result is driven by the adversary's place in the decision process. The adversary responds to the security environment as defined by SA.

Despite the limitations associated with the methods applied in this chapter, the insights illustrate a greater understanding of insider threats and their mitigation. The nature of modeling is incapable of capturing the detail and specificity to completely recreate the world: agents are far more complex, and their options are far more varied. While this model presumes a conservative but creative attack vector, the use of illicit narcotics as a chemical weapon, many other less innovative and passive options remain available to adversaries

for disrupting business. Despite the research indicating a compelling argument, the use of fentanyl in the scenario-building phase of this chapter is virtually untested. Though the simulation of decision-making offered by these models is informative, it is noted that further work and alternative methods could better estimate information related to VSL, operating costs, attack frequency, and return on investment for specific AIP mitigation technologies and processes. Finally, while using loss as a proxy for attack and attacker valuation of strategies in the sequential games is logical, it is open to compelling counterarguments regarding the subjective valuation of outcomes, especially when such activity is attached to intangible concepts such as honor or ideology. Additionally, human wetware is not a precise calculating machine like the simple software models used to calculate the payoffs in this model. Despite these limitations, these games reduced the complexity of the problems, silenced a noisy environment, and offered real insight into the challenges of insider threat mitigation.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONSIDERATION OF BEHAVIORAL ECONOMICS AND PSYCHOLOGICAL THEORY

The previous chapter assessed organizational and adversarial decision-making through economic lenses—these lenses were used to understand complex decision-making processes and interactions between threats and their targets by simplifying and constraining reality. However, researchers have repeatedly observed that individuals and organizations do not always make mathematically optimum decisions. While models illustrate and help facets of complex issues, frameworks are often more useful sensemaking tools to understand intricate relationships and systems such as the psychological and behavioral mechanisms that drive individuals to act counter to organizational interests. Prominent psychological theories seek to explain the gap between the precise and rational outcomes often seen in games and the messier business of decision-making in the real world. Social and behavioral economics theories such as Self-Control Theory and Social Control Theory, Social Identity Theory, Rational Choice Theory, and Prospect Theory, offer important insights into these decision-making, behavioral mechanisms, and key traits which influence insider decision-making. By developing frames which organize and evaluate countermeasure selection decisions through the lens of broad socio-economic theories, the effect of these selections on AIP is better informed and the challenging evaluation of AIP mitigation strategies may be tackled with more structure.

This analysis seeks to anchor the characteristics of AIP countermeasures being explored or already in use by academics and practitioners in the field of critical infrastructure security in psychological theory. Security professionals can more effectively assess and implement appropriate countermeasures by understanding the context of their probable effect on AIP, their theoretical underpinnings, and their nuanced relationship with each other. Each countermeasure will be assessed against the following psychological and behavioral economic theories:

- Social Identity Theory indicates that critical infrastructure organizations should be aware of the social drivers to insider threats, consistent with comprehensive

mitigation strategies, and that security countermeasures which are visible and social will have a social effect on the groups exposed to them.

- Self and Social Control Theories assess the extent to which human bonding, development, and socialization affect the capacity of insiders to make decisions consistent with organizational and other social norms.[209]
- Rational Choice Theory holds that individuals engage in a calculated process when deciding to engage in insider threats (decision-making), weighing the perceived benefits against potential repercussions.
- Prospect Theory describes how cognitive biases, risk perception, and a two-step decision process can lead to otherwise unexpected decisions for AIP. The theory holds the potential to more completely articulate why individuals may become adversarial and engage in risk-seeking activity.

These theoretical positions will be used to understand and assess various aspects of comprehensive insider life cycle mitigation, and decision processes in relation to AIP countermeasures to synthesize a novel evaluative Decision Control Framework (DCF). Comprehensive insider threat mitigation programming is developed on the foundations of complex theories. Unintentionally, perhaps, comprehensive insider threat mitigation draws from a diverse background of psychological theories that are not contradictory but also not wholly compatible. The theories applied thus far for analysis are produced from different disciplines and focus on various aspects and observations of human behavior and risky decision-making. Nevertheless, despite their different origins, their overlapping themes provide an encompassing perspective to better understand adversarial behavior and the insider threat life cycle. Considering these aspects of each countermeasure while planning and implementing new initiatives is a complication for an already daunting task. The tactics used to mitigate AIP should be informed by each other and the unique aspects of the critical infrastructure environment.

209 Carter Hay and Walter Forrest, "The Development of Self-Control: Examining Self-Control Theory's Stability Thesis," *Criminology* 44, no. 4 (November 2006): 740, https://doi.org/10.1111/j.1745-9125.2006.00062.x; Pratt, "A Self-Control/Life-Course Theory of Criminal Behavior," 130–35.

All AIP countermeasures are first designed to affect an AIP and then understood to affect the employees. Informed by the adversarial perspective, regardless of a psychological or economic approach, the first question at hand for evaluating a countermeasure is how well a particular countermeasure can be observed and subsequently learned by an adversary. This question lies at the root of its effect: how will employees in general or AIP respond to the system and what countermeasures are used to protect the system? A visible countermeasure will influence behavior and decision-making, while an invisible measure is less likely to be considered by the adversary. Additionally, visible countermeasures might also be learned, and AIP may adapt. Visible countermeasures known to the extent that they are or become predictable are an objective to defeat but not necessarily an obstacle to adversarial success. Further, countermeasures may affect each other. For instance, rational or prospective security, such as increased punishment or physical screening tactics, may adversely affect countermeasures rooted in individual control or social action. The DCF is proposed to organize such assessments in practical and research contexts. Considering countermeasures as part of a system through this lens is an untested method to plan, implement, and research insider threat programs and their constituent parts.

A. SELF AND SOCIAL CONTROL THEORIES—CRIMINOLOGY AND THE CRIMINAL

Self and Social Control Theories offer theoretical support to AIP mitigation strategies. Both offer perspectives on mitigating and preventing insider threats within organizations via the management of mental-health and social health bonds. Organizations can build and reinforce these social bonds to operationalize Social Control Theory in the context of mitigating insider threats. For instance, institutions might foster a more positive organizational culture where employees feel valued and connected to their peers and their legitimate mission: meaningful work assignments (shift bids, project bids), team-building activities (trust falls), clear communication of organizational values (weekly newsletters), and opportunities for professional development (a professionally-oriented Master's Program for instance) could theoretically enhance employees' attachment to the organization and their commitment to its success, thereby decreasing the likelihood of

adversarial activity.[210] Additionally, promoting ethical behavior through training programs, leadership, and consequence awareness programs can reinforce employees' beliefs in organizational rules and morality. Institutions engaged in these types of programs for the purpose of mitigating AIP behavior do so with support from Self and Social Control Theories.

Some organizations already apply self-control concepts to mitigate AIP's development by fostering a culture emphasizing long-term consequences of AIP activity over its immediate rewards. Training programs that highlight the severe repercussions of adversarial activity, both for the individual and the organization, and the implementation of stringent oversight mechanisms that make impulsive actions less appealing to execute draw principally from Self Control Theory. Additionally, promoting a supportive work environment that addresses employee grievances before they escalate can reduce the likelihood of insiders acting out in ways that threaten security.[211] Finally, some institutions have implemented mental health awareness and support programs directly linked to improving employee well-being and group identity/belonging, citing the need to reduce employee stress and estrangement.[212] It is thought that by reducing psychological strain and increasing the value of group identity, insiders will avoid adversarial behavior in favor of conserving social value.[213] By aligning organizational policies with the principles of self-control theory, companies may theoretically decrease the likelihood of insider threats by encouraging more thoughtful, deliberate behavior among employees.

Self and Social Control Theories thus offer a lens through which adversarial insiders and mitigation efforts might be better understood and assessed, even if they offer limited value at the individual employee level. Specifically, working to understand the relationship between the individual adversary and internal and external factors that

---

210 Whitty, "Developing a Conceptual Model for Insider Threat," 925–27.

211 Bean, "Mitigating Insider Threats in the Domestic Aviation System," 50–60.

212 Megan Gates, "Insider Threat: The Shift from Report to Support," *Security Management*, September 1, 2021, http://www.asisonline.org/security-management-magazine/articles/2021/09/insider-threat-the-shift-from-report-to-support/.

213 Black, "Managing the Aviation Insider Threat," 50–54.

influence individual behavior is critical to addressing the insider threat problem. By combining personal impulse control from Self Control Theory with the focus on social bonds and normative influences from Social Control Theory, organizations might seek to create comprehensive strategies, when combined with other countermeasures and supporting theory, to deter adversarial actions. This hybrid approach recognizes that social structures can shape self-control, and that strengthening social ties within the workplace can enhance self-control over time. However, these theories also exhibit complex challenges when applied to individuals, as observed in applying market models to evolutionary agent models.[214] Therefore, a tailored approach that considers these individual differences would be essential. To implement such a program, ongoing psychological assessment to understand individual baselines and subsequent deviation, consistent with AIP formation and action, would better inform risk-management. This thesis does not need to illustrate in detail the dystopian picture that such a program would paint (daily psychological assessments conducted by AI efficiency coaches) nor does it need to point out how expensive, invasive, and susceptible to error such a program would likely be, at least currently.[215] However, this thesis counters such initial thoughts with the importance of averages and effort. It is accepted that individuals are different and that everyone will respond to stimuli uniquely. However, overall, there is value in understanding how ongoing investments and mitigations are likely to affect groups and the average population. While organizations are not currently capable of fine-tuning such assessment programs and responses for each individual, they may be able to sufficiently tune efforts to the problem for each unique infrastructure system or for high-risk individuals.[216] Unique and tailored psychological evaluation and intervention remains a promising area of research but falls short of technological readiness in most critical infrastructure use cases. Strong academic support exists for these theories as a basis for

[214] Mohammed Abdellaoui, "Rational Choice under Uncertainty," in *Cognitive Economics: An Interdisciplinary Approach*, ed. Paul Bourgine and Jean-Pierre Nadal (Berlin, Heidelberg: Springer, 2004), https://doi.org/10.1007/978-3-540-24708-1_2.

[215] Black, "Managing the Aviation Insider Threat," 54.

[216] Grizzle, *Insider Threat Mitigation at Airports*, 27.

ongoing attempts to foster positive organizational cultures prioritizing long-term goals, ethical behavior, and strong social bonds.

B. SOCIAL IDENTITY THEORY—THE RELATIONSHIP OF THE PERSON TO MANY WHOLES

What happens when the adversarial perspective shifts to the point where the needs, desires, and norms of the individual cannot be aligned with the norms of the organization? Social Identity Theory, developed by Henri Tajfel and John Turner in the late 1970s, and the research emanating from it, posits that people derive and reinforce a significant part of their identity and actions from the social groups to which they belong and, by extension, their relationships to other groups.[217] These groups can include professional affiliations, teams within an organization, or important, broader categories like nationality, ethnicity, and ideological community. Social Identity Theory suggests that individuals strive to maintain a positive self-concept by aligning their behavior with the norms and values of these groups, often leading to in-group favoritism and out-group discrimination.[218] Social Identity Theory supports critical infrastructure operator's tactics which leverage organizational culture initiatives to inhibit negative group selection and conflict between employees and the organization. This section explores how Social Identity Theory can be applied to deter and prevent insider threat activity. It briefly examines the mechanisms through which social identity influences behavior, discusses the implications for insider threat prevention, and proposes practical strategies for organizations to enhance their security posture using Social Identity Theory principles.

Social Identity Theory is grounded in the conceptual understanding that individuals categorize themselves and others into various social groups, ranging from small teams to entire organizations.[219] In the Social Identity Theory framework, these group memberships

---

[217] J. C. Turner, R. J. Brown, and H. Tajfel, "Social Comparison and Group Interest in Ingroup Favouritism," *European Journal of Social Psychology* 9, no. 2 (1979): 189,202, https://doi.org/10.1002/ejsp.2420090207.

[218] Ashforth and Mael, "Social Identity Theory and Organization," 35.

[219] Turner, Brown, and Tajfel, "Social Comparison and Group Interest in Ingroup Favouritism," 189–202.

are not merely superficial labels; they form a crucial part of an individual's self-concept and influence their thoughts, feelings, and behaviors.[220] There are several key concepts to Social Identity Theory:

- Social Categorization is an individual process by which individuals identify groups and mentally place themselves and others into groups based on shared characteristics or attributes.[221]
- Social Identification describes how individuals adopt the group's identity after categorizing themselves into a group.[222]
- Social Comparison and Competition: once individuals identify with a group, they compare their group (in-group) with other groups (out-groups).[223]
- In-group favoritism and out-group discrimination can lead to employee biases.[224]

Social identity influences behavior by aligning individual actions with group norms. When individuals strongly identify with a group, they are more likely to conform to their understanding of the group's norms and values, as their self-esteem is tied to the success and positive image of the group as seen by its members.[225] This conformity can lead to pro-social behaviors that benefit the group but can also contribute to inter-group conflict when the interests of different groups clash, particularly during competition. In the context of an organization, if employees strongly identify within the organization and perceive it as representative group, they may be more likely to engage in behaviors that support the organization's goals and to avoid actions that could harm it.[226] Conversely, if

220 Anders Strindberg, "Social Identity Theory and the Study of Terrorism and Violent Extremism," Research (Totalförsvarets forskningsinstitut (Total Defense Research Institute), December 2020), 14, https://www.foi.se/rest-api/report/FOI-R--5062--SE.

221 Tajfel and Turner, "An Integrative Theory of Intergroup Conflict," 38–42.

222 "Social Identity Theory," 38–42, accessed September 12, 2023, https://www.age-of-the-sage.org/psychology/social/social_identity_theory.htm.

223 "Social Identity Theory," 38–42.

224 Tajfel and Turner, "An Integrative Theory of Intergroup Conflict," 38–42.

225 Ashforth and Mael, "Social Identity Theory and Organization," 35; Tajfel and Turner, "An Integrative Theory of Intergroup Conflict," 40.

226 Tajfel and Turner, "An Integrative Theory of Intergroup Conflict," 42.

individuals are made to feel alienated or marginalized by the organization or some larger group to which the organization is connected, they may seek to realign their social identities, with some small percentage potentially leading to insider threat ideation. Finally, if individuals are already firmly and deeply aligned with an outside and competitive group (*contra* the security organization), Social Identity Theory implies that superficial efforts will not effectively realign deep loyalties and would thus not mitigate such inclinations.

Given the potentially powerful influence of social identity on individual behavior, Social Identity Theory provides an expanded lens through which AIP relationships with their host organization may be understood and through which efforts to mitigate insider threats may be more fully assessed. This theory lends academic support to several counter-AIP strategies:

- Corporate Identity: A strong organizational identity can serve as a protective factor against insider threats. In fact, an employee's withdrawal from social interaction and elevated interpersonal conflict are often cited as indicators of a potential insider threat: personnel are less likely to engage in behaviors that could harm an organization when they feel a deep sense of belonging and pride.[227] Clearly communicating the organization's mission, values, and goals can help employees understand their role within the broader organizational context and identify with the organization. When employees see their work as contributing to a meaningful mission, they may be more likely to identify with the organization and align their behavior with its values via in-group favoritism and categorization.
- Vetting: The practice of vetting and selecting employees is a primary approach to constructing a strong organizational identity. Effective selection programs are sometimes designed to foster a common background within the collective and this is supported by social categorization and competition. Such practice naturally reinforces group behavior, membership, and norms amongst a cohort of "trusted" individuals.

[227] Daan Van Knippenberg and Els C. M. Van Schie, "Foci and Correlates of Organizational Identification," *Journal of Occupational and Organizational Psychology* 73, no. 2 (2000): 145, https://doi.org/10.1348/096317900166949.

- Recognize and Reward Contributions: Publicly recognizing and rewarding employees for their contributions reinforces the idea that the organization, the group, values their individual efforts. This recognition can enhance employees' sense of belonging and loyalty to the organization through identification and competition. Further, promoting individuals on their merits can connect workers and management and reinforce dedication to the institutional mission. Conversely, such programs may establish limited-good resources (rewards) within the organization which can result in competition-driven division.
- Cultivate a strong Organizational Identity: When employees categorize their organizational culture as fair and connected to their personal identities, aligning with popular individual values, they may be more likely to develop a positive identification with it.
- Promote Cross-Departmental Collaboration: Encouraging collaboration between different teams and departments can help reduce counter-productive in-group favoritism and out-group discrimination. Cross-functional projects, joint training sessions, and inter-departmental events can facilitate positive interactions and foster a sense of unity across the organization.
- Facilitate Open Communication: Open and transparent communication is essential for reducing misunderstandings and conflicts between different groups within an organization. Regular town hall meetings, feedback sessions, and open-door policies can help ensure that organizations hear their employees and address their concerns.

People are generally aware of their inclinations to be loyal members of groups, the principles of Social Identity Theory have been traditionally applied in team-building and branding efforts across organizations for insider threat mitigation and other business efforts.[228] The presumption is that these efforts provide value to general management and productivity within the business environment and provide additional security value in

[228] Tajfel and Turner, "An Integrative Theory of Intergroup Conflict," 40.

mitigating insider threats. However, a primary concern related to Social Identity Theory in this capacity is the difficulty in precisely evaluating the social effects of Social Identity Theory-supported AIP mitigation. Counting the number of individuals arrested for AIP activity is quite simple. It is much more difficult to determine how many of these individuals would have been interrupted had they identified with their team more. Finally, due to the presumed significance of social relationships and values to insider threat formation and the social presumption that group action portends an individual reaction, insider threat mitigation countermeasures that seek to single out or cleave away individuals from the adversarial group (countermeasures which challenge the values of the group, degrade trust within the group, or establish divisions within the group) would be expected to reduce the insider–organization relationship.

Whereas mitigation efforts more closely aligned to social control can be applied to individuals, Social Identity Theory-based tactics affect groups and rely on predictive social interaction and effects. For example, branding, promotions, and workplace culture programs are advertised and influence individuals and social groups. As another example, many airports, corporations, and critical infrastructure systems provide insider threat awareness and training programs to most employees regularly. AIP are a part of this ecosystem; potential adversaries move through it, breathe the air, drink the water, and hunt within its natural and artificial social constraints. Countermeasures applied to social dynamics are, by their nature, social, visible, and knowable.

C. RATIONAL CHOICE THEMES—IS THIS WORTH THE RISK?

Rational Choice Theory provides a robust framework for understanding how individuals, including AIP, might make decisions and how organizations can influence those decisions through manipulations of risks, rewards, and punishments. This theory addresses the rational aspects of decision-making, specifically how individuals and AIP use perception of risks and rewards to plan and execute illegitimate activity.[229] Rational Choice Theory posits and predicts that individuals decide to maximize their utility by

[229] Serdar Kenan Gül, "An Evaluation of the Rational Choice Theory in Criminology," *Sociology and Applied Sciences* 4, no. 8 (2009): 39.

weighing costs and benefits. It presumes that individuals consider the losses and gains associated with their decisions and seek to optimize their decisions for maximum utility—a traditional economic approach.[230] The theory is an empirical framing of decision-making. Rational Choice Theory would suggest that, when contemplating malicious activity, AIP gather information and conduct a rational calculus wherein they consider the potential rewards of their actions against the associated risks of detection and punishment. After putting their calculator away, AIP would choose the course of action, methods, targets, assets, or information that are most likely to result in the highest utility. By manipulating this calculus, institutions could strategically modify security and support systems to effectively deter adversarial insiders by making the perceived costs of harmful actions clearly outweigh the benefits, thus influencing their decision-making process. Finally, Rational Choice Theory so clearly supports many of the AIP countermeasures discussed and applied to critical infrastructure.

However, real-world cases have demonstrated rapid adaptation to and circumvention of such Rational Choice Theory-based tactics by AIP. Flight attendants (as a tool for AIP), security services, and knowledge of security procedures have been repeatedly leveraged by AIP to circumvent countermeasures and the security system as revealed in the case studies and their analysis. Perhaps measures such as these housed under Rational Choice Theory provide value and reduce the frequency of AIP activity. Perhaps increased alignment to and participation in the critical infrastructure organization will never provide sufficient value to ignore the gains promised by other illicit activities or continued loyalties to other groups. Ultimately, AIP can learn, know, and plan around predictable security procedures. The natural extension of Rational Choice Theory in critical infrastructure protection is that AIP will use their rationality to plan their way through and around such countermeasures to the greatest extent possible. The case studies both support and undermine common AIP countermeasures found in Rational Choice Theory. First, cases 1 and 2 indicate that AIP are compelled to react to countermeasures such as static and planned, mobile screening (checkpoints and canine sweeps) indicating that such

[230] Margaret R. Somers, "Symposium on Historical Sociology and Rational Choice Theory," *American Journal of Sociology* 104, no. 3 (November 1998): 743, https://doi.org/10.1086/210085.

measures wielded generally deterrent power based in economic theory. Ultimately however, these measures and the other layers of security did not ultimately deter illicit activity. Thus, these cases indicate that such countermeasures are not effectively applied in airport environments. In case 2 and 3, AIP directly confronted security measures with conspiratorial confidence. These failures raise at least three very compelling questions:

- Why would people engage in illicit behavior with all the risks inherent to existing countermeasures?
- Will any countermeasures raise the bar sufficiently so that no insider would consider adversarial opportunities?
- Should critical infrastructure managers and regulators require such countermeasures?

Uncertainty, particularly regarding the likelihood of detection and the severity of potential consequences, is an influential factor during decision-making.[231] According to Rational Choice Theory, if an individual is unsure about the likelihood of an outcome, they should consider the expected utility, probabilistic outcome, and scenario. This consideration will result in mathematical calculation and discreet valuation sensitive to risk preference. Within Rational Choice Theory, risk preference may be understood as the willingness for a subject to select options which may result in loss. Preferences are generally a stable psychological trait that are yet somewhat dependent upon problem framing, starting valuations, magnitude and frequency of loss, and other factors which may cause momentary influence.[232] Extending this explanation, problem framing is a term used to describe how the problem is presented to the subject, the AIP.[233] Risk preference plays a critical role in shaping an individual's perception of risk in the context of Rational Choice

[231] Herbert A. Simon, "Bounded Rationality in Social Science: Today and Tomorrow," *Mind & Society* 1, no. 1 (March 2000): 35, https://doi.org/10.1007/BF02512227.

[232] Rui Mata et al., "Risk Preference: A View from Psychology," *Journal of Economic Perspectives* 32, no. 2 (Spring 2018): 156, https://doi.org/10.1257/jep.32.2.155.

[233] Thomas Langer and Martin Weber, "Prospect Theory, Mental Accounting, and Differences in Aggregated and Segregated Evaluation of Lottery Portfolios," *Management Science* 47, no. 5 (May 2001): 730, https://doi.org/10.1287/mnsc.47.5.716.10483.

Theory.[234] The concept of "bounded rationality," which acknowledges that individuals' decision-making processes are limited by the information they have; their cognitive capacities, to include bias; and the finite amount of time available are also important variables within Rational Choice Theory.[235] Different AIP will naturally have different access to information and must operate on unique operational schedules. As discussed elsewhere in this thesis, AIP typically benefit from the luxury of time, access to information, and the initiative to act. Despite these limitations, risk preferences could be influenced by manipulation of AIP's perceptions regarding the probability of being caught, the availability of information, or the nature of the punishment that an AIP might face.

Specifically, the visibility and knowability of certain tactics seem to be important considerations in countermeasure deployment for this purpose. AIP respond to available information in unique ways, but the availability of information itself might be better controlled to elicit favorable reactions, for security. Information is power, and greater knowledge of the security system empowers adversarial problem solving.[236] Insiders operating under uncertainty may not be able to fully assess all possible outcomes or calculate the risks and rewards of their actions, probabilistically, even with their insider advantages. Certainly, completely hidden security measures would have no effect on AIP decision-making, however, by applying or increasing uncertainty toward visible security measures—such as varying the times and methods of observation or the unpredictability of audits—organizations can further limit the ability of insiders to game systems, as seen during the simple games analysis, gather helpful information, and form rational decisions.

Rational Choice Theory posits that individuals make decisions by evaluating the benefits and risks of each decision. Insider threat countermeasures that produce risks or decrease gains in knowable and predictable, even if uncertain, ways theoretically mitigate insider threats by increasing the value threshold to act. This theoretical basis provides a

234 Avinash Dixit, "Entry and Exit Decisions under Uncertainty," *Journal of Political Economy* 97, no. 3 (1989): 621–36, https://www.jstor.org/stable/1830458.

235 Simon, "Bounded Rationality in Social Science," 25.

236 Viale, Gallagher, and Gallese, "Bounded Rationality, Enactive Problem Solving, and the Neuroscience of Social Interaction," 6.

straightforward, simple, and intuitive frame to understand AIP behavior and the effect of countermeasures. Arguably, operational advantages held and enjoyed by AIP should motivate security experts to implement policies that reduce predictability to the greatest extent possible, expand adversarial uncertainty, and manipulate the value propositions of adversarial activity, which also ground these countermeasures in Rational Choice Theory. Organizations currently make use of this theoretical approach by applying several countermeasures:

- Observation/Behavioral monitoring is implemented to monitor employee behavior for deviation from baseline when accessing and moving within institutional systems. The overt nature of this countermeasure makes it visible to some degree. The extent to which it is knowable by AIP is varied given the many methods this countermeasure can be applied.
- Physical Screening is implemented in many critical infrastructure environments to detect and deter the introduction of illicit material into institutional systems and decrease theft from such systems. Physical screening of all kinds is visible.
- Awareness Campaigns are designed to ensure that potential adversaries know the risks associated with adversarial acts. Like social campaigns, this activity is highly visible. The security operators control the exact knowledge supplied to adversaries by such programs, considering the frequency and magnitude of the publicity.[237] Punishment and prosecution fit into this category, as they are also related to the risk of detection.
- Employee Benefit and Development programs are designed and funded in part to increase the value of continued employment. These programs are inherently visible and are designed to provide knowledge to all employees.

This analysis highlights that Rational Choice Theory provides the foundation for several countermeasures. However, these countermeasures are vulnerable to dynamic and

[237] These types of programs appear to be more prevalent in crime control activities such as drug busts, graffiti campaigns, and public shaming campaigns for anti-theft. Direct research into the effectiveness of such campaigns in controlling crime was outside the scope of this analysis.

evolving AIP methods and tactics. Therefore, given this relationship, investment in these countermeasures should be well thought-out for maximum additive or multiplicative effect with other efforts whenever possible while being particularly sensitive to potential deleterious effects such countermeasures may cause a larger insider threat strategy.

D. PROSPECT THEORY—DEGREES OF RATIONALITY

There are alternative decision-making theories to Rational Choice that articulate adversarial decision-making with a more nuanced and descriptive approach. Prospect Theory, developed by Daniel Kahneman and Amos Tversky, lays out a robust and compelling framework for understanding decision-making under risk and advancing the role of uncertainty and how agents consider it during decision-making: Prospect Theory posits that decision-making occurs in two stages and those different perceptions, such as biases and estimations, of the decision are especially important at each stage. Both concepts are relevant to studying insider threats in organizational security and understanding AIP. By manipulating what is known about the system, its countermeasures, and AIP biases (tendencies to improperly evaluate or estimate), organizations may be capable of influencing the decision-making process and dissuading malicious action.

According to Prospect Theory, during the first phase of decision-making, individuals tend to reframe the problem by segregates and accepting information and options for decision.[238] One byproduct of this process is that subjects tend to overestimate the likelihood of low-probability losses, mainly when they are uncertain about the exact likelihood of those events occurring.[239] Individuals ingest information about options and potential gains and losses and then move to consolidate and simplify the values for potential outcomes to drive more efficient decision-making or, more practically, to be capable of very complex decision-making. The simplification phase allows security designers to influence AIP by controlling at least some framing information, bias, and time span. Organizations can capitalize on this bias by cultivating an environment where the

[238] Langer and Weber, "Prospect Theory, Mental Accounting, and Differences in Aggregated and Segregated Evaluation of Lottery Portfolios," 730.

[239] Langer and Weber, 724.

detection mechanisms are perceived by AIP as pervasive and unpredictable. For instance, a fixed closed-circuit television (CCTV) is a form of surveillance that is somewhat knowable and predictable to an adversary. Industry response to deploy dummy CCTV to expand the perception and frequency of surveillance fits neatly within Rational Choice Theory and Prospect Theory frames. However, deploying functional CCTV on a mobile platform would be aligned with Prospect Theory. Driven by Prospect Theory's position regarding the first phase of decision-making, such a modification would likely create a complex and daunting detection probability that cannot be properly estimated by AIP, compressing the area between the bounds of rationality. If AIP believe that the probability of being caught is higher than it is due to strategic ambiguity around security measures, they may be less willing to take risks. Likewise, if AIP are significantly unsure of the risks, they may be more likely to overestimate them when operating in a low information environment. This perception of near-omnipresent surveillance and more-than-mediocre enforcement, even if not entirely accurate, would theoretically reduce the attractiveness illicit activity.

Prospect Theory also builds on the concept of loss aversion, suggesting that individuals uniquely experience losses more intensely than gains of the same magnitude: every person will experience these losses and gains differently, but people tend to experience losses more intensely.[240] Thus, risk-aversion is a quality that varies, and it changes given the scenario and agent. Arguably, uncertainly enhances risk aversion in any scenario.[241] Organizations might find a new capability to exploit this bias and discourage malicious behavior by heightening AIP's perceived uncertainty around detection and punishment. For example, increasing the unpredictability of monitoring and surveillance measures can create an environment where insiders are unsure about when and how their actions might be detected, thus amplifying their fear of loss and reducing their likelihood

[240] Peter Sokol-Hessner and Robb B. Rutledge, "The Psychological and Neural Basis of Loss Aversion," *Current Directions in Psychological Science* 28, no. 1 (2019): 20, https://doi.org/10.1177/0963721418806510.

[241] Kahneman and Tversky, "Prospect Theory," 21; Glenn W. Harrison and E. Elisabet Rutström, "Risk Aversion in the Laboratory," in *Research in Experimental Economics*, vol. 12 (Bingley, UK: Emerald, 2008), 41–44, https://doi.org/10.1016/S0193-2306(08)00003-3.

of engaging in harmful activities. Such logic seems evident in decisions to deploy random and/or unpredictable screening in some environments such as passenger screening or border checkpoints.

Prospect Theory features another critical insight in the context of insider threat mitigation, which might be used by critical infrastructure operators to influence adversarial decision-making: framing effects and a phased decision process. How experimental design frames choices significantly impacts how the payoffs for each choice are perceived and evaluated by the agent. Levin, Schneider, and Gath have proposed that framing effects can be categorized as risky choice-framing, attribute-framing, or goal-framing and that these frames demonstrate significantly consistent qualities—risky choice-framing is more effective at shifting opinions with positive frames, attributes are perceived positively when labeled positively, and losses tend to sway decisions under goal-framing.[242] These insights are still applied to important modern decision-making, such as work to guide more effective conversations regarding Flu, Covid-19, and other vaccinations.[243] In such applications the framing of risks associated with illnesses were evaluated for effectiveness using various communication styles to align with or conversely confront personally held beliefs and social membership norms. Such considerations have also been applied to anti-drug campaigns to reduce illicit drug use.[244]

In the case of insider threats, the way in which critical infrastructure Operators frame potential outcomes as either potential gains or losses would influence insiders' decisions. For instance, framing the consequences of getting caught not merely as a loss of employment but as a substantial personal and professional disaster (e.g., legal repercussions, public disgrace, and long-term career damage) may increase the psychological weight of these losses. Further, framing the consequences of insider activity

[242] Irwin P. Levin, Sandra L. Schneider, and Gary J. Gaeth, "All Frames Are Not Created Equal: A Typology and Critical Analysis of Framing Effects," *Organizational Behavior and Human Decision Processes* 76, no. 2 (November 1998): 150, 181, https://doi.org/10.1006/obhd.1998.2804.

[243] Nehama Lewis and Erga Atad, "Effects of Message Framing and Narrative Format on Promoting Persuasive Conversations with Others About the Flu Vaccine," *Health Communication* 39, no. 10 (August 23, 2024): 2111, 2118, https://doi.org/10.1080/10410236.2023.2257427.

[244] Lewis and Atad, 2117.

in terms of the effects on individuals related to and associated with the actor might have a tremendous impact on decision-making. When coupled with uncertainty about the exact method consequences, this framing can create a powerful deterrent effect, making the decision to engage in malicious activities less appealing by further decreasing the perceived payoff.

Moreover, manipulating uncertainty can disrupt the adversarial insider's confidence in evading detection. Overconfidence is a common cognitive bias where individuals overestimate their capabilities and the likelihood of success.[245] Organizations can undermine this confidence by introducing elements of uncertainty into the environment, such as random security checks, unpredictable auditing processes, and ambiguous communication about monitoring technologies. When AIP are unsure about their ability to avoid detection, it is likely that AIP will overestimate the effectiveness of such measures. This uncertainty could, therefore, force AIP to reconsider, reframe, and even overestimate the risks associated with their actions, leading AIP to shift or abstain.[246] Organizations may deter AIP by creating an environment where the outcomes of adversarial actions are perceived as highly uncertain and severe.

Critical infrastructure institutions have long applied insider threat countermeasures supported by Prospect Theory. For instance, the effectiveness of screening methods is a closely guarded secret in many security systems. The U.S. Government has stipulated the effectiveness of screening methods as sensitive in its regulation; it takes measures to protect precisely how effective these measures are.[247] Further, the Transportation Security Administration has required that some airports implement random inspection of aviation workers (insiders) and recently issued requirements to airports that establish a baseline or

[245] Tamar Kugler et al., eds., "Improving and Measuring the Effectiveness of Decision Analysis: Linking Decision Analysis and Behavioral Decision Research," in *Decision Modeling and Behavior in Complex and Uncertain Environments*, vol. 21, Springer Optimization and Its Applications (New York: Springer New York, 2008), 6, https://doi.org/10.1007/978-0-387-77131-1.

[246] Buttenheim, Moffitt, and Beatty, *Behavioral Economics*, 3–4, 185–87.

[247] ABC News, "TSA Fails Most Tests in Latest Undercover Operation at U.S. Airports," ABC News, 11/09/20217, https://abcnews.go.com/US/tsa-fails-tests-latest-undercover-operation-us-airports/story?id=51022188; Transportation Security Administration, *49 CFR 1520 – The SSI Federal Regulation* (Washington, DC: Department of Homeland Security), accessed September 22, 2024, https://www.tsa.gov/sites/default/files/49_cfr_part_1520.pdf.

minimum amount of random physical screening for aviation workers with access to security-restricted areas at some airports. Suppose this baseline establishes an expectation among AIP that screening could occur using any normal pathway. In that case, adversaries may overestimate the likelihood of being caught while attempting to smuggle illicit goods through such pathways.[248] Thus, according to Prospect Theory, shielding the actual effectiveness, frequency, and locations of screening procedures likely increases adversarial uncertainty and decreases insider threat.

Prospect Theory also provides the most relevant theoretical underpinnings for other deployed countermeasures. When designing security systems, the landscape itself, virtual or physical, is fertile ground for exploitation. An example is the positioning of high-value aircraft in specific security programs—it has been argued that some airlines and airports will vary gate approach, gate assignment, and gate configuration to improve security and decrease the information horizon for adversaries.[249] This concept could be applied to physical spaces, wherein the location of high-value assets, physical security systems, and transportation methods may be varied from time to time to reduce AIP's confidence in planning and executing illicit activity. For instance, the rotation of security personnel involved in internal affairs and insider threat programming is helpful to ensure that relationships are not compromised or leveraged by external handlers. Though these arguments are admittedly underdeveloped, such Prospect Theory-founded tactics can be considered more broadly for countering AIP. For instance, the rotation of access points and pathways presents a low-cost opportunity to increase uncertainty, complexity, and decision cost under Prospect Theory. The clear thread is that countermeasures under Prospect Theory would effectively accomplish these tasks.

E. A NOVEL DECISION CONTROL FRAMEWORK

The work expanding the knowledge of insider threat mitigation proceeding this thesis has generally argued for comprehensive solutions to the problem of insider threats.

[248] Buttenheim, Moffitt, and Beatty, *Behavioral Economics*, 174.

[249] Jaummer, "El Al's Legendary Security," FlyerTalk Forums, December 5, 2001, https://www.flyertalk.com/forum/el-al-matmid/61931-el-al-s-legendary-security.html.

Understanding the nature and relationship of these fundamental theoretical underpinnings for each countermeasure permits a new frame around mitigation decisions that place the adversary in the middle as the object of mitigation and permits security to be built around them. This approach spotlights every aspect of AIP while recognizing each as a human being with typical human psychological consideration. Recognizing and communicating with security specialists the complex nature of adversaries and how countermeasures most effectively reach potential AIP can enhance the application of each countermeasure. Further, this insight will better inform critical infrastructure strategic planning and design. This section will synthesize these insights and observations to propose a new DCF for Insider Threat Mitigation selection to potentially facilitate security system design by evaluating the balanced and comprehensive qualities of countermeasure selection.

A theoretical understanding of an AIP's motivation and frames which describe how AIP come to be are not new. The common characteristics of all AIP as they have been discussed in this thesis, are that they are individuals, have a social identity, are motivated to act against the interest and social norms meant to protect an organization by opportunities to gain, and act in a way that is outside and counter to the organization.[250] Shaw and Lenzenweger proposed a *similar* framework for *identifying* potential insider threats and assessing infrastructure risk in 2022, describing a "critical pathway" to becoming a threat can be understood through personality, stressors, behavior, and organizational response.[251] This thesis proposes a frame that could sit alongside theirs, expanding the focus from understanding and identifying AIP to mitigation; and further, extending an understanding of either "organized" or "maladaptive" countermeasures. Like the characteristics composing the critical pathway, AIP's characteristics should be considered as opportunities for intervention clarified by the dominant theory of the day. Finally, this framework provides a tool to make sense of recommendations for comprehensive intervention and the unique slate of challenges for any airport. Framing

[250] Gains are not always monetary though they are often described in such quantifiable methods.

[251] "The Critical Pathway to Insider Risk Model," 8.

these characteristics provides a valuable means to assess and organize tactics and the AIP mitigation strategy.

The first step in outlining the DCF is the aggregation of countermeasures in relation to their theoretical families. As discussed above, when reviewing and analyzing the dominant theories influencing insider threat mitigation, proposed and applied countermeasures are found to reflect specific aspects of prominent behavioral theories. The categorization of these countermeasures is not perfectly exclusive. As these theories exhibit some overlapping concepts, so do the groupings of countermeasures according to these theories. For instance, Rational Choice Theory and Prospect Theory seek to better describe and advance the understanding of human deliberation and choice. However, each theory has an affinity and a central theme. A central theme likewise drives each countermeasure and the philosophy of its application. While the application of countermeasures has not been demonstrated to be contradictory or exclusive in this research, a push-and-pull relationship between countermeasures is anticipated given their diverse theoretical underpinnings. While each countermeasure may draw from more than one theoretical family, this analysis proposes that each countermeasure and theoretical family exhibit core themes sufficient to categorize them by their unique affinity to each other.

For instance, countermeasures such as integrity-testing may interfere with training and employee reporting programs due to their effect on the relationship between employees and the organization. Testing, punishment, and publication programs are categorized under Rational Choice Theory, as they are intended to increase the loss or perception of loss associated with adversarial activity. From the adversarial perspective, such programs appear to demonstrate effectiveness and increase the probability of being caught—such perceptions modify the decision calculus for engaging in counter-organizational behavior. However, the broader population of insiders would view such activity differently. Such countermeasures potentially create divisions within the organization, degrade trust, and reduce social control by the group. There is no evidence to suggest that this effect is critical – a test and punishment of an adversary, a violator of organization goals, a.k.a. an outsider, will not likely override a well-established culture. However, repeated testing, or perhaps consistent screening of the entire insider population, could gradually reduce the quality of

the relationship between employee and employer while degrading the social fabric that Social Identity Theory countermeasures conceptually rely upon for their effectiveness.

It can also be understood from this framing that certain countermeasures may be applied via methods that contradict their theoretical foundation. As seen in the cases studied, random search activity, related to Prospect Theory and Rational Choice Theory, is not frequently observed. AIP in the DFW smuggling case (2018) obtained information regarding scheduled, quais-random searches prior to planning and engaging in illicit activity.[252] In the JFK aircrew smuggling case (2024), the known identity and low-frequency, predictable screening activity were insufficient to deter AIP's activity.[253] Similarly, adversarial agents were able to weigh the likelihood of random encounter at access points in attacker-defender games analysis. These observations indicate that activity must be random in the AIP's perspective and that they must approach some threshold of effectiveness. Too often, nominal ideas of randomization are countered through good surveillance and planning. It is easy to assume that visible random screening increases the intuitive deterrence value of an activity. Random screening in the open elevates employee and public awareness of the activity—often designated as a good thing for security. However, random screening is not random if it can be learned and/or manipulated by AIP (the target of the activity). Prospect Theory informs that such activity is wasted if it can be known and planned around by AIP. What use is a high awareness of screening activities if the screening activity is easily predicted and countered by AIP?

Grouping countermeasures by theoretical family provides insight into each countermeasure's conceptual effect on AIP and employee host populations, providing two values: application to specific aspects of AIP pathways and cooperation among countermeasures. Comprehensive insider threat programs and their supporters strive to create a network of mitigation measures that touch all aspects of AIP in all parts of the adversarial life cycle.[254] Consistent with leading recommendations for the integration of

[252] Krauss, "DFW Airport Drug-Smuggling Crew That Offered to Fly Explosives Admits Guilt."

[253] U.S. Attorney's Office, Southern District of New York, "Flight Attendants Charged in Connection with Smuggling Drug Money to the Dominican Republic."

[254] Lenzenweger and Shaw, "The Critical Pathway to Insider Risk Model," 8.

insider threat programs, to accomplish this goal, it is crucial to select countermeasures that best fit the organization and its security strategy to reduce the impact, shift organizational risk, increase the perception of adversarial risk.[255] As an example, consider that not every organization experiences the same level of social cohesion. Further, consider that not every subgroup within an organization will match the overall social temperature. Maintaining group identity and cohesion is an essential aspect of strong groups under Social Identity Theory.[256] In an organization with high group cohesion, insider threat awareness and training are intuitively indicated, whereas for socially isolated or unique subgroups, more sophisticated vetting and testing are more applicable. Conversely, training and awareness programs that rely upon strong social norms may not be the correct countermeasure to apply to organizations that already experience low cohesion. Such a program may be better indicated and more successful if and once the underlying social conditions are resolved through corporate identity and inclusion programs. Such an organization, armed with this understanding, may instead deploy a reporting program as an integrated feature of an extensive organizational identity improvement project.

The validation and quantification of this proposition present fertile research ground. Aggregating and organizing countermeasures by theoretical family advances an understanding of how these countermeasures are founded and interrelated and illustrates new ways to consider countermeasures when implementing and enhancing insider threat mitigation strategies. Based on the analysis above, common countermeasures are categorized in Table 8.

255 Grizzle, *Insider Threat Mitigation at Airports*, 12, 20, 30.

256 Marlene E. Turner et al., "Threat, Cohesion, and Group Effectiveness: Testing a Social Identity Maintenance Perspective on Groupthink," *Journal of Personality and Social Psychology* 63, no. 5 (November 1992): 794, https://doi.org/10.1037/0022-3514.63.5.781.

Table 8. Countermeasures by Theoretical Family

Theoretical Family	Underlying Mechanisms & Concepts	Reflection of Existing Countermeasures
Self and Social Control Theories	• Social Bonds • Socialization • Commitment to Conventional Institutions • Norms vs. Deviance	• Consequence Awareness Programs • Identification and Intervention • Mental Health Benefits • Challenge Programs
Social Identity Theory	• Social Identity • Social Categorization • In Group Favoritism • Self-Esteem • Group Dynamics/Social Mobility	• Insider Vetting • Insider Threat Awareness • AIP Awareness and Reporting • Cultural Alignment Programs
Rational Choice	• Expected value vs. relative loss • Perception/Frames • Estimations	• Physical Screening • Surveillance and Observation Programs • Testing, Reward, & Awareness Campaigns • Punishment / Prosecution • Employee Development & Relations
Prospect Theory	• Two-step decision-making process. • Biases and framing result in efficient, though imprecise, risk-reward decision-making.	• Veiled effectiveness of security procedures • Randomized screening activity • Obscured vetting processes • Variable Landscaping

The DCF organizes and assess tactics axially along two lines: their interaction with AIP's decision-making and social effects between AIP and the larger insider population as derived from Rational-Prospect and Control-Social Identity Theory Theories, respectively, Figure 6. In such a frame, researchers and practitioners could evaluate each countermeasure

in terms of its security effect in each of the four theoretical areas, demonstrating its individual contribution and effect across the system. These values could be summative, multiplicative, or exponentially influential. This influence is treated as summative for the purposes of this research to retain some simplicity.

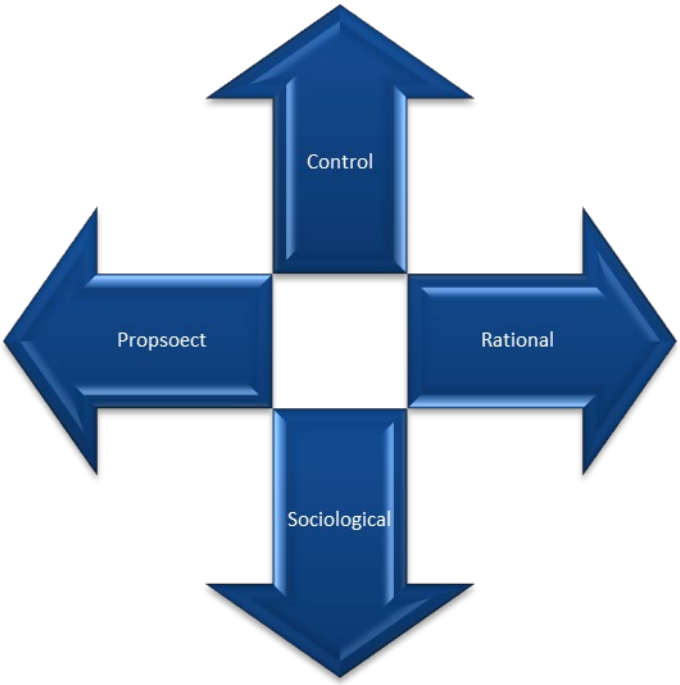

Figure 6. DCF: Axial Organization of Theoretical Families

The relationship of the countermeasure to the adversary is critically important and defined by the potential for an adversary to see and know the countermeasure. Not every countermeasure is accessible to AIP. For example, the intricacies of vetting and the secretive nature of surveillance make some countermeasures difficult to study. Similarly, unpredictable security measures, by definition, are difficult to know, though easy to see. Conversely, other countermeasures are inherently visible and knowable, such as employee screening checkpoints, awareness training, reporting programs, access control measures, challenge programs, CCTV, and direct observation activities. Invisible countermeasures also allow system agents to *selectively* make information regarding certain security activities more available to AIP. For instance, it is a security decision to release the results

of surveillance activity. While not necessary, reporting and advertising activity related to otherwise invisible security operations may have a strategic deterrent value. Security strategists should consider using this frame through which the relationship of countermeasures to each other and the AIP mitigation strategy can be assessed in terms of visibility and knowability, as these factors determine how the security information is received by or hidden from AIP (and all employees).

An airport or regulatory agency could implement this frame to advance its understanding of active and relevant policies. Using DCF and drawing from the discussion above, the following Insider Threat Mitigation Strategy for a large airport may be hypothetically constructed and assessed. Drawing further from the previous case studies, a composite airport with a security-restricted area and some number of aircraft is conceived with five access points to the secured area. The airport has 5,000 employees with unescorted access to the security-restricted area. The airport has a neutral assessment of its current social cohesion and notes its aviation worker population is also composed of many sub-groups. The airport selects eleven countermeasures to deploy in its strategy, represented in Table 9. This table documents a quantified representation, assessing the affinity of each countermeasure [from -10 to 10]: the negative portion of the range demonstrates conflict with the categorical column. By contrast, the positive portion of the range demonstrates cross-categorical support.

Table 9. Countermeasure Evaluation

Category	Countermeasure	Visibility	Knowability	Control	Rational	Social	Prospect
RCT	Routine Canine Sweep of Employee Lockers	10	5	0	6	-5	0
PT	High Frequency - Randomized Physical Screening in Secured Area	10	3	0	3	-4	9
PT	Recurrent Vetting of Employees	0	0	4	0	10	0
PT	Rotation of High Value Asset Locations	2	2	0	2	0	8
Control	Low Frquency Challenge Program	4	4	1	0	1	0
Control	Consequence Awareness Program	5	5	5	10	5	-4
Control	Mental Health Support	1	0	8	0	0	0
SIT	Initial Vetting	5	4	2	0	8	0
SIT	Routine Pen Testing	1	2	0	4	-2	0
RCT	Full Employee Screening	5	5	1	0	-6	0
RCT	Employee Relations Program Improvements	2	1	9	0	0	0

Evaluating a countermeasure follows a subjective, though simple, path through each of the theoretical bases to establish a valuation of its visibility and knowability. Full aviation worker screening, for instance, is highly knowable and visible. It takes place at access points to security-restricted areas, even at a centralized screening location. On its own, AIP may participate in, observe, and learn the effectiveness, vulnerabilities, times, locations, and agents involved in such activities. The screening itself has no effect on individual control of their own actions. However, for the population it serves as a litmus for control in the population—higher find rates indicate lower self-control or organizational communication. Similarly, as the countermeasure is highly visible and well known, it has no value from a rational choice perspective. AIP are free to simply consider other pathways and create effective solutions to circumvent the countermeasures. The countermeasure creates no additional risk to the adversary, as they have the initiative to act. The countermeasure can be ascribed a negative social score, as the screening creates specialized populations of exempt (such as some management and law enforcement) and non-exempt individuals (aviation workers as a whole) creating division and generally creating an optic of distrust based on social tendencies toward social categorization and competition. Thus, full aviation worker screening would be scored as: 5, 5, 1, 0, -6, as reflected on Table 9.

The DCF, assessing strategic security decisions in this socio-economic matrix, can also quantify the cumulative effect and illustrate organizational effort across theoretical families, Figure 7 and Figure 8. The DCF also identifies that this hypothetical strategy aggressively reinforces individual responsibility and traditional security measures with a secondary focus on prospective rationales. However, the strategy may demonstrate weakness in building a social fabric that inhibits and prevents insider threat formation and subsequent activity.

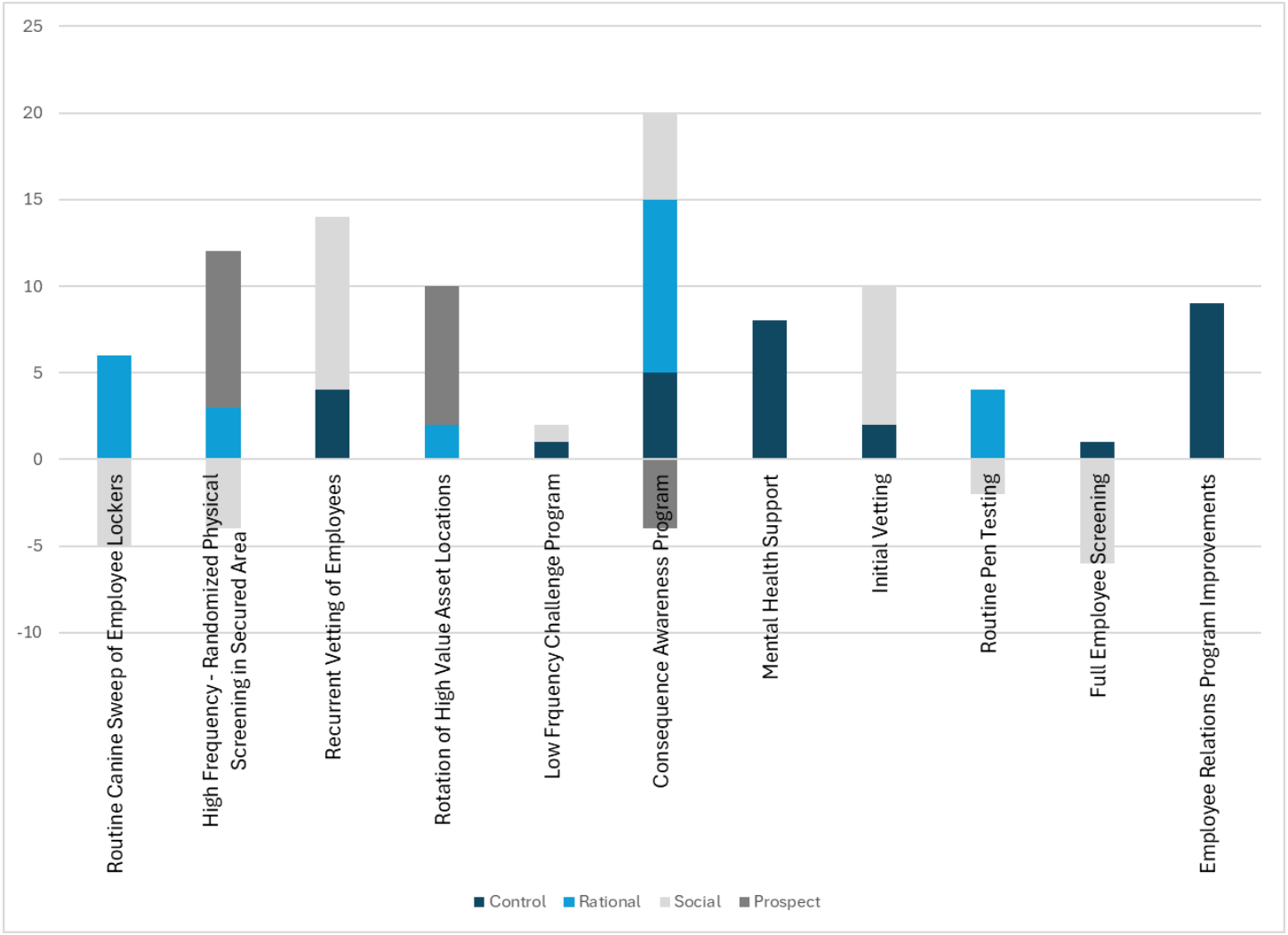

Figure 7. DCF Illustrated Influence of Countermeasure According to Valuation

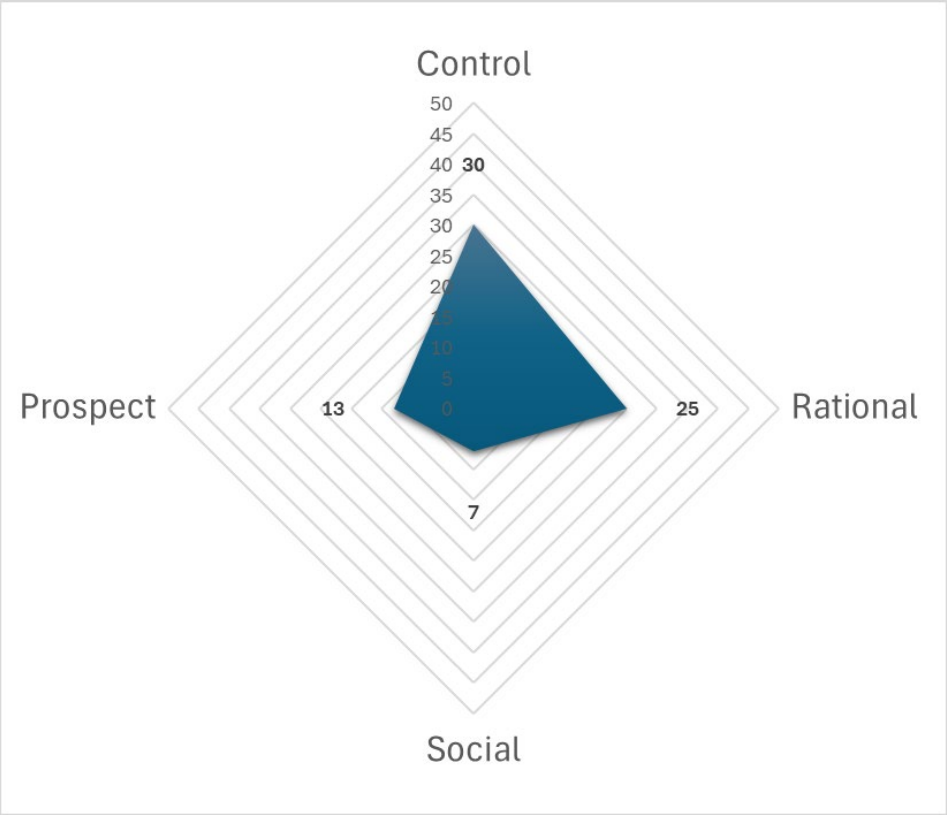

Figure 8. DCF: Illustration of Focus Areas—Comprehensive Mitigation Evaluation

F. CONCLUSION

Research reviewed by this thesis has consistently demonstrated that insider threat mitigation programs should consider all aspects of the AIP life cycle and that such strategies should draw from multiple disciplines. Existing countermeasures are based on prominent behavioral economics and psychological theories. Therefore, while these theories are not necessarily mature enough to apply in focused countermeasure development, they are promising lenses through which strategic decisions and existing insider threat mitigation efforts may be reviewed and assessed. This thesis has determined that organizations, including regulatory authorities, should consider the theoretical concepts from which each countermeasure proceeds and, absent precise and validated matrices illustrating cooperative affinity, can subjectively assess tactics and select those

most likely to cooperate and provide additive value when constructing comprehensive insider threat mitigation strategies.

- The analysis of behavioral economics in the form of Rational Choice Theory and Prospect Theory and how each is applied in critical infrastructure environments presently indicates that despite their promising value, more work is needed to understand the broad effect such security activity could have on workplace culture and its constituents.
- While analysis has indicated that each countermeasure and its theoretical basis must have a relationship with other countermeasures and some affinity defined by this relationship, a thorough review demonstrates that insufficient research exists to permit organizations, or this thesis, to quantify these values precisely.
- Despite a lack of precise information describing how countermeasures relate to each other, the DCF provides illustrative value in understanding how a slate of countermeasures is expected to deliver a comprehensive insider threat mitigation environment and permits evaluation of proposed changes to such strategies in a novel and holistic manner.

The proposed DCF offers a new method of potential research, a whisper of more informative planning, and the promise of a new way to think about and assess insider threat mitigation strategies, extending the well-formed arguments for comprehensive insider threat mitigation programs.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

The threat posed by adversarial insider personnel (AIP) in critical infrastructure environments, particularly aviation, is a pressing issue that continues to challenge traditional security strategies as demonstrated by recent events, headlines, and incidents. This research has explored the complex dynamic qualities of insider threats, the economics related to AIP countermeasures, including the decision-making processes of AIP, and the relationships of mitigation strategies through a multidisciplinary lens. The goal of this thesis is to assess to what extent concepts from behavioral economics should be considered for more effective insider threat mitigation. Current literature indicates that further research must be conducted to precisely tune behavioral economic models and theories to adversarial decision-making. This thesis extends and focuses such observations on AIP. This research further extends calls for comprehensive insider threat mitigation by proposing a novel frame through which current and proposed AIP mitigation measures may be understood through behavioral economics lenses, from the AIP's perspective and through theoretical socio-economic lenses. The proposed Decision Control Framework (DCF) may enhance and inform strategic selection of AIP countermeasures through structured consideration of an organization's AIP mitigation strategy in relation to selected socio-economic theories.

A. KEY FINDINGS AND SYNTHESIS

This conclusion synthesizes the key findings, practical recommendations, and limitations while shining a torch toward future inquiry and action.

1. Insider Threat Dynamics

Insider threats in aviation are driven by a confluence of factors that make them both persistent and challenging to address. AIP exploit their legitimate access to sensitive environments to bypass traditional security measures, often with devastating consequences. The motivations behind such adversarial behavior can be categorized into five main drivers: financial gain, ideological conflict, personal grievances, psychological disturbance, and the pursuit of power. Each of these factors interacts dynamically with the

individual's environment contributing to the adaptability of AIP and AIP resistance to conventional deterrence measures. The evolution of insider threats has revealed a troubling adaptability among adversaries. Case studies highlight specific efforts on the part of AIP to adjust their methods in response to enhanced security protocols. For instance, the smuggling operation at Dallas/Fort Worth International Airport (DFW) demonstrated the deliberate exploitation of procedural gaps and insider access to bypass security. Similarly, the bombing of Daallo Airlines Flight 159 illustrated the collaboration between AIP and external actors to subvert physical security measures and surveillance. These cases underscore the importance of understanding AIP as active agents capable of learning, adapting, and evolving.

2. Strategic and Tactical Insights

Efforts to mitigate insider threats have yielded an array of tactics and strategies that may lack coordination and strategic integration. From an operational perspective, the literature highlights the role of organizational culture and trust in shaping employee behavior. AIP often emerge in environments where trust is either excessively granted or systematically undermined. Building a culture of accountability, transparency, and mutual respect can serve as a powerful deterrent against insider threats. However, the challenge lies in balancing trust with verification, a tension that is evident in the resistance of aviation stakeholders to more intrusive security measures, and supported by competing socio-economic theory belying all AIP countermeasures.

The number of pathways to security assets is a factor that can be controlled to a large degree by institutions. Most importantly, placing security activity on these paths and within each unique system is an important advantage. Conducting security at access points and other chokepoints within critical infrastructure environments provides an efficient means of exposure. This is a valuable aspect of risk-shifting when countering an external threat with limited options for penetration, but less effective for countering AIP as demonstrated by analysis of the cases and attacker-defender games. However, due to the systematic nature of airport environments, such configurations also provide predictable deployment patterns. If there are only three places where security is taking place, then

anywhere and everywhere else becomes an opportunity for illicit activity. Therefore, all the spaces and times in which employees have access and trust should be considered for security activities. For instance, the TSA recently improved its vetting so that it is no longer done just at entry to employment, but recurrently. Taking this a step further, physical screening should not be considered just a checkpoint or access point activity.

Finally, visibility matters. Adversaries learn, and so much of the case analysis deals with what motivation and information can accomplish when combined. Human beings are generally visual creatures. One method by which to consider security countermeasures is by assessing them based on their desired effect and capacity to be seen and known by an adversary. A passenger screening checkpoint, for example, is a very visible security layer. Random security need not be visible and arguably should occur with no visible methodology. Therefore, the number of people receiving random re-vetting or physical screening is less likely as important as the AIP's knowledge that such activity is occurring. Whereas surveillance activity should only exist to AIP as a whisper and provide almost no footprint whatsoever. Given the varied menu of security countermeasures, knowledge and visibility become important factors during countermeasure selection and strategic review. Inversely, critical infrastructure reliance on highly visible security features intending to deter AIP may unfortunately serve only to bandage an incomplete and maladapted security system – a dark, hospitable environment for corruption of the insider population.

3. Theoretical Contributions

Behavioral economics, social psychology, and game theory offer valuable insights for insider threat mitigation by addressing the psychological, social, and strategic drivers of adversarial behavior. Behavioral economics, through Prospect Theory and Rational Choice Theory, highlight cognitive biases such as loss aversion and risk perception, enabling security professionals to design countermeasures that exploit these factors. Social Identity Theory and Self/Social Control Theories emphasize the impact of organizational culture, inclusion, and social bonds in deterring adversarial actions by fostering accountability, respect, and strong group identities. Additionally, game theory, including Mechanism Design Theory (MDT) and adversarial security games, provide a framework

for aligning security policies with organizational incentives and understanding adversarial decision-making in response to countermeasures, making these approaches integral to enhancing and studying insider threat prevention strategies.

B. RECOMMENDATIONS

To address the challenges of mitigating adversarial insider threats, this section proposes a set of comprehensive and actionable recommendations. These recommendations draw from interdisciplinary insights and are structured to inform security professionals, policymakers, regulators, and industry stakeholders in designing and implementing effective strategies.

1. Policy and Engagement

AIP have portable skills and can choose the weakest links in critical infrastructure systems, particularly in transportation. Policy efforts should:

- Encourage cross-sector partnerships with industries facing similar challenges, such as banking, critical infrastructure, and corrections, to identify transferable strategies and lessons learned.
- Advance Regulatory Reforms for Standardization: Enhance minimum baseline for security measures, such as comprehensive, or preferably, dynamic employee screening and continuous behavioral monitoring. Ensure transparent cost-benefit analyses, at the system level, to support policy decisions, ensuring that security investments are both effective and economically viable.
- Consider the proposed DCF or other novel frames capable of evaluating and illustrating potential countermeasures simultaneously from the perspective of AIP and from broad socio-economic perspectives to align future AIP mitigation strategies to previously described insider threat life cycles and motivators. This tool can integrate with insider threat programming and processes to effectively enhance and unify the contributions of otherwise disparate leadership efforts. It does not replace tools and processes used for risk assessment.

2. Implement Economic Incentives to Drive Security Investment

Mechanism Design Theory (MDT) reveals that financial disincentives and lack of clear rewards generally discourage investment in additional security measures above and beyond requirements. Markets may be leveraged to improve investment in security initiatives:

- Instead of rulemaking and regulations, alternatively consider the introduction of subsidization programs, such as tax-and-credit or government grant programs to encourage independent airport and critical infrastructure investment for AIP mitigation and other security concerns consistent with the observations of airport investment decision-making.
- Encourage public-private partnerships to share the financial burden of implementing large-scale, regional, and systematic security enhancements, particularly at smaller airports and infrastructure operators with limited budgets.

3. Operational Enhancements

The adaptability of adversarial insiders necessitates dynamic security measures informed by real-time data and predictive analytics. Operational enhancements could include:

- Strengthening real-time intelligence capabilities by deploying advanced mobile surveillance and behavioral monitoring technologies, such as algorithm-driven anomaly detection, to identify unusual employee behavior and operational irregularities.
- Employing adaptive security layers; static security measures are easily learned and circumvented by motivated adversaries. Augmenting visible security measures with covert security measures would create uncertainty for potential adversaries. For instance, supplement physical screening with unobservable and/ or mobile surveillance techniques.

- If physical screening is deployed, implement randomized inspections at varying times *and* locations *throughout security-restricted areas* to prevent predictability in security routines.
- Importantly, consider privileged populations such as privileged employees and customer populations (quasi-insider) as more vulnerable to manipulation and temptation given their ascribed status. Frequent and unpredictable security measures such as surveillance and physical screening are more strongly indicated given the case studies and games analysis.

C. LIMITATIONS AND AMBIGUITIES

While comprehensive in its interdisciplinary approach to understanding and mitigating AIP, this research has limitations. A primary constraint lies in the reliance on its analysis of case studies and theoretical material to draw conclusions. While this analysis provides valuable insights into historical incidents and theoretical frameworks, they inherently lack granularity and validated data. The absence of empirically validated data on insider threat activity, such as behavioral cues or decision-making processes collected during actual events, limits the ability to validate the proposed models and recommendations fully. Additionally, the counterfactual analyses used to evaluate hypothetical responses to enhanced security measures are speculative by nature and may not account for the full complexity of AIP adaptation and influencing factors. Further, quantifying the influence of countermeasures as proposed by the Decision Control Framework (DCF) is not validated. Presently, the use of the DCF would be informative but subjective without a precise understanding of how each countermeasure influences security values in other areas of the frame.

While the aviation sector represents critical infrastructure, another limitation to this research stems from the focus on aviation-specific contexts which may inhibit generalization of these findings to other sectors of critical infrastructure. The unique regulatory environment, technological infrastructure, and organizational cultures of airports may not fully align with other industries facing insider threats, such as finance, energy, or corrections. For instance, while Mechanism Design Theory and game theory

models are highly relevant to regulated airport markets, their application may differ significantly in less regulated or differently structured sectors. Finally, even in aviation environments, the parameters applied to both sets of games are hypothetical. The actual scenarios, payoff structures, countermeasures, and particularly agent strategies may not apply to any individual airport, though this thesis has made efforts to make such scenarios as broadly applicable and relevant as possible. This sector-specific focus risks overlooking broader insights that could enhance cross-industry strategies for mitigating insider threats. This has led to the recommendation that any future work with the DCF includes efforts to engage with insider threat programming from multiple sectors.

Finally, the research's theoretical reliance on behavioral economics and psychological models introduces potential biases related to the abstraction of human behavior. While frameworks like Prospect Theory and Social Identity Theory offer robust explanations for insider decision-making, they may oversimplify the dynamic interplay of personal, social, and organizational factors. These theories often assume idealized conditions, such as clear cognitive biases or predictable group behaviors, which may not fully capture the nuances of real-world AIP scenarios. Furthermore, the absence of longitudinal data limits the exploration of how insider threat behaviors and mitigation measures evolve over time, leaving critical gaps in understanding long-term effectiveness and unintended consequences of proposed interventions. This framework is not restricted to the use of these theories, nor is it limited to the four theoretical families applied – rather the DCF offers a new manner to think about, evaluate, and document organizational and regulatory insider threat mitigation strategies. In its current limited form, it also offers practical advantages to otherwise unstructured strategic discussion and decision-making processes surrounding mitigation selection, deployment, and regulatory efforts.

D. FUTURE RESEARCH AND TECHNOLOGICAL INNOVATION

This thesis focused on the assessment of behavioral economics in AIP mitigation and resulted in a broad review and critique of AIP mitigation strategies which was often hampered by gaps in research which would otherwise indicate why particular countermeasures are and are not effective. Future research in insider threat mitigation is

needed to deepen the understanding of how Prospect Theory, Rational Choice Theory, Social Control Theory, and Social Identity Theory intersect in shaping the decision-making processes of potential insider threats. Specifically, the proposed DCF offers a method for AIP and AIP countermeasure evaluation, however, existing research does not provide sufficient material to adequately ascribe and evaluate countermeasures in a standard manner within each theory. The proposed DCF may enhance future research in this area. A more refined version of the DCF may prove useful to the process of designing new interventions and systematic strategies that are both theoretically robust and operationally effective.

The case studies analyzed in this research offer practical insights into the limitations of existing security measures and the potential for innovative solutions. Synthesizing these cases reveals a central theme: insider threats thrive in environments where static security measures are the norm, reinforcing the need for dynamic security. Adaptive and layered approaches that integrate behavioral, technological, and procedural innovations are essential to counter these evolving threats and represent a niche for ongoing and future research.[257] Blockchain technology, which ensures tamper-proof activity logs, can support Prospect Theory by creating a clear and transparent record of actions, thus re-framing potential risks in ways that deter harmful behaviors. Additionally, augmented reality (AR) tools for training personnel might enhance their ability to identify subtle behavioral anomalies in their social circles. Future research should explore the efficacy and ethical implications of these technologies in operational contexts.

To address the behavioral and economic drivers of insider threat activities, future studies should conduct analyses of organizational dynamics and their impact on employee behaviors. This aligns with Social Identity Theory by considering how workplace culture and changes influence group affiliations and motivations. Behavioral interventions such as stress management programs and counseling merit exploration to assess their impact on reducing insider threat ideation, incorporating insights from Social Control and Rational

[257] Robert L Scott, "Protecting the Perimeter: Unmanned Aircraft Systems Enhance National Airport Security" (master's thesis, Naval Postgraduate School, 2023), 48–49, https://hdl.handle.net/10945/72602.

Choice theories. Simultaneously, cost-benefit analyses of combining behavioral and economic deterrents can optimize resource allocation, ensuring that investments in security yield the greatest impact. Finally, the relationship between automation, social strain, and labor response appears to be a ripe area for research given the increasing reach of these technologies into the labor market. These studies will be essential in tailoring mitigation strategies that address both the human and systemic elements of AIP prevention and mitigation.

Finally, more complex and illustrative games are called for to adequately understand market forces and decision-making which surround the problem of insider threats. The games presented by Kunreuther and Heal assessed the willingness of airlines to invest in additional security measures to protect baggage-handling systems from terrorist threats.[258] The games presented in this thesis were extended to airports and the issue of insider threats. There is a significant opportunity to define more elaborate games to determine if the results are consistent for more complex markets. There is also an opportunity to attune the attacker-defender games to account for risk perception and other concepts in Prospect Theory.

E. CLOSING REMARKS

Much of the literature discussed random security features. It is often posited that elements of randomness are crucial to effective security. These cases, and the subsequent analysis, suggest that beyond randomness, a return to unpredictability, from the adversarial perspective, is required. These concepts are, unfortunately, not the same. Countermeasures should be designed and implemented to limit possible in-advance communication and knowledge. In addition to time, location should be used as a random factor to the greatest extent possible for when security measures would take place for insider populations. For instance, the creation of schedules for surveillance, observation, challenge campaigns, and screening can more closely coincide with deployment. Developing recommendations on these fronts would require insight and unique knowledge of the airport, or critical

[258] Kunreuther and Heal, "Interdependent Security," 2–16.

infrastructure assets being protected. Unfortunately, such dynamic security activities would also make management and oversight more difficult. However, without a balance of these perspectives, security efforts run the risk of being made obsolete by effective adversarial preparation. No leader, regardless of their role, wants their efforts and the efforts of their team to be made obsolete.

Insider threats to aviation security are multifaceted and evolving. This challenge demands innovative, interdisciplinary solutions. Additionally, insider threats are an old problem, and organizations have implemented countermeasures that predate even the simplest scientific understanding of human behavior. This research highlights the critical importance of understanding AIP as adaptive actors and designing countermeasures that are equally dynamic and multifaceted, representative of modern scientific theory. By integrating insights from game theory, behavioral economics, and social psychology, security may move beyond reactive measures toward proactive systemic solutions.

The path forward requires collaboration, innovation, and an unwavering commitment to public safety and economic resilience. As the aviation industry and other vulnerable infrastructure sectors continue to navigate the complexities of mitigating insider threats, the arguments and ideas proposed herein offer a blueprint for building a more secure and resilient future.

LIST OF REFERENCES

ABC News. "TSA Fails Most Tests in Latest Undercover Operation at U.S. Airports." ABC News, 11/09/20217. https://abcnews.go.com/US/tsa-fails-tests-latest-undercover-operation-us-airports/story?id=51022188.

Abdellaoui, Mohammed. "Rational Choice under Uncertainty." In *Cognitive Economics: An Interdisciplinary Approach*, edited by Paul Bourgine and Jean-Pierre Nadal, 15–32. Berlin, Heidelberg: Springer, 2004. https://doi.org/10.1007/978-3-540-24708-1_2.

Agrawal, Ajay, Carlos Rosell, and Timothy S Simcoe. "Tax Credits and Small Firm R&D Spending." Working Paper, National Bureau of Economic Research, 2019.

Airports Council International. "ACI-NA Position on TSA's Aviation Worker Screening National Amendment." Washington, DC: Airports Council International, August 2, 2023. https://airportscouncil.org/wp-content/uploads/2023/08/ACI-NA-USPC-Position-on-TSA-Aviation-Worker-Screening-Mandate.pdf.

Airways Staff. "Airways Top 10 Largest Passenger Aircraft in Service." *Airways Magazine – Airlines*, May 18, 2024. https://airwaysmag.com/new-post/top-10-largest-passenger-aircraft.

Alterman, Steve. *Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control*. Washington, DC: Aviation Security Advisory Committee, 2015. https://www.tsa.gov/sites/default/files/asac-employee-screening-working-group-04-15.pdf.

Anman, Molly, Karie Gibson, Mathew Bowlin, Sarah Griffin, Leslie Buckles, Kirk Kennedy, Kevin Burton, Cari Robins, and Kimberly Brunnel. *Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks*. Washington, DC: U.S. Department of Justice, 2017.

Apau, Mohd Nazer, Muliati Sedek, and Rabiah Ahmad. "Inclination of Insider Threats' Mitigation and Implementation: Concurrence View from Malaysian Employees." In *Knowledge Management in Organizations*, edited by Lorna Uden, Branislav Hadzima, and I-Hsien Ting, 877:340–52. Communications in Computer and Information Science. Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-95204-8_29.

Arneklev, Bruce J, Lori Elis, and Sandra Medlicott. "Testing the General Theory of Crime: Comparing the Effects of 'Imprudent Behavior' and an Attitudinal Indicator of 'Low Self-Control.'" *Western Criminology Review* 7, no. 3 (2006): 41–55.

Ashforth, Blake, and Fred Mael. "Social Identity Theory and Organization." *The Academy of Management Review* 14, no. 1 (1989): 20–39. https://doi.org/10.5465/AMR.1989.4278999.

A. Zoumpouli, Garyfalia, Fernanda Siqueira Souza, Bruce Petrie, Liliana Amaral Féris, Barbara Kasprzyk-Hordern, and Jannis Wenk. "Simultaneous Ozonation of 90 Organic Micropollutants Including Illicit Drugs and Their Metabolites in Different Water Matrices." *Environmental Science: Water Research & Technology* 6, no. 9 (2020): 2465–78. https://doi.org/10.1039/D0EW00260G.

Baum, Phillip. "Daallo Airlines Bombing: Interview with Captain Vladimir Vodopivec." *Aviation Security International*, February 2017, 21–29. https://www.avsec.com/media/files/int01.pdf.

Baumeister, Roy F., and Kathleen D. Vohs, eds. *Handbook of Self-Regulation: Research, Theory, and Applications*. New York: Guilford Press, 2004.

Bean, Brian S. "Mitigating Insider Threats in the Domestic Aviation System: Policy Options for the Transportation Security Administration." Master's thesis, Naval Postgraduate School, 2017. https://hdl.handle.net/10945/56861.

Becker, Megan. "Four Charged in Chillicothe after Drug Search." *Chillicothe Gazette*, June 23, 2022. https://www.chillicothegazette.com/story/news/2022/06/23/four-charged-chillicothe-after-drug-search/7710872001/.

Beers, Rand. *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*. Washington, DC: Department of Homeland Security, 2011.

Beitsch, Rebecca. "House Approves Contentious FISA Bill in Bipartisan Vote." The Hill, April 12, 2024. https://www.aol.com/house-approves-contentious-fisa-bill-171241728.html.

Bergemann, Dirk, and Juuso Välimäki. "Dynamic Mechanism Design: An Introduction." *Journal of Economic Literature* 57, no. 2 (June 2019): 235–74. https://doi.org/10.1257/jel.20180892.

Beynon, Steve. "Green Beret in Las Vegas Bombing and New Orleans Attacker Had Brief Overlap in Military Careers." Military, January 6, 2025. https://www.military.com/daily-news/2025/01/06/green-beret-las-vegas-bombing-and-new-orleans-attacker-had-brief-overlap-military-careers.html.

Biase, Nicholas, and Shelby Wratchford. "Four Flight Attendants Plead Guilty to Smuggling Drug Money to the Dominican Republic." United States Department of Justice Southern District of New York, August 14, 2024. https://www.justice.gov/usao-sdny/pr/four-flight-attendants-plead-guilty-smuggling-drug-money-dominican-republic.

Bishop, Matt, Sophie Engle, Deborah A. Frincke, Carrie Gates, Frank L. Greitzer, Sean Peisert, and Sean Whalen. "A Risk Management Approach to the 'Insider Threat.'" In *Insider Threats in Cyber Security*, edited by Christian W. Probst, Jeffrey Hunker, Dieter Gollmann, and Matt Bishop, 115–37. Boston, MA: Springer U.S., 2010. https://doi.org/10.1007/978-1-4419-7133-3_6.

Black, Alan. "Managing the Aviation Insider Threat." Master's thesis, Naval Postgraduate School, 2010. https://hdl.handle.net/10945/5039.

Booth, Charles. "Does History Matter in Strategy? The Possibilities and Problems of Counterfactual Analysis." *Management Decision* 41, no. 1 (2003): 96–104. https://doi.org/10.1108/00251740310445545.

Brook, Jack, Stephen Smith, and Sara Cline. "FBI Says Driver behind New Year's Truck Attack Visited New Orleans Twice before." PBS News – Nation, January 5, 2025. https://www.pbs.org/newshour/nation/fbi-says-driver-behind-new-years-truck-attack-visited-new-orleans-twice-before.

Brown Jr, Michael S. "Tell Me How This Begins: Insurgency in the United States." Master's thesis, Naval Postgraduate School, 03/23. https://hdl.handle.net/10945/72065.

Bulhof, Johannes. "What If? Modality and History." *History and Theory* 38, no. 2 (1999): 145–68. https://www.jstor.org/stable/2505660.

Burke, Kevin. "Airports Council Releases Statement on Rodney Scott Nomination to Serve as Customs and Border Protection Commissioner." Airports Council International – North America, December 9, 2024. https://airportscouncil.org/press_release/airports-council-releases-statement-on-rodney-scott-nomination-to-serve-as-customs-and-border-protection-commissioner/.

Buttenheim, Alison, Robert Moffitt, and Alexandra Beatty, eds. *Behavioral Economics: Policy Impact and Future Directions*. Washington, DC: National Academies Press, 2023. https://doi.org/10.17226/26874.

Cao, Sissi. "Amazon Unveils AI Worker Monitoring for Social Distancing, Worrying Privacy Advocates." *Observer*, June 16, 2020, sec. Technology. https://observer.com/2020/06/amazon-artificial-intelligence-monitor-warehouse-worker-social-distancing-coronavirus/.

Catrantzos, Nick. "Insider Threat: Applying No Dark Corners Defenses." Master's thesis, Naval Postgraduate School, 2018. https://hdl.handle.net/10945/4656.

Caves Jr., John P. "Fentanyl as a Chemical Weapon." In *Proceedings*. National Defense University: CSWMD, 2019. https://wmdcenter.ndu.edu/Portals/97/CSWMD%20Proceedings%20Dec%202019.pdf.

Chamberlain, Colleen, and Brian Kalish. "AAAE Aviation Security Summit." American Association of Airport Executives. Accessed January 14, 2025. https://aaae.org/securitysummit.

Chremos, Ioannis Vasileios, and Andreas A. Malikopoulos. "Mechanism Design Theory in Control Engineering: A Tutorial and Overview of Applications in Communication, Power Grid, Transportation, and Security Systems." *IEEE Control Systems* 44, no. 1 (February 2024): 20–45. https://doi.org/10.1109/MCS.2023.3329919.

Cibulsky, Susan M., Timo Wille, Renée Funk, Danny Sokolowski, Christine Gagnon, Marc Lafontaine, Carol Brevett et al. "Public Health and Medical Preparedness for Mass Casualties from the Deliberate Release of Synthetic Opioids." *Frontiers in Public Health* 11 (May 12, 2023): 1–9. https://doi.org/10.3389/fpubh.2023.1158479.

Citiguard. "How Much Does It Cost to Hire a Security Guard?" Citiguard, February 15, 2024. https://www.mysecurityguards.com/blog/how-much-does-it-cost-to-hire-a-security-guard/.

Costello, Barbara J., and John H. Laub. "Social Control Theory: The Legacy of Travis Hirschi's *Causes of Delinquency*." *Annual Review of Criminology* 3, no. 1 (2020): 21–41. https://doi.org/10.1146/annurev-criminol-011419-041527.

Craig, Megan. "Fentanyl Could Be Weaponized and Used for Terroristic Mass Poisoning." News Medical, June 1, 2023. https://www.news-medical.net/news/20230601/Fentanyl-could-be-weaponized-and-used-for-terroristic-mass-poisoning.aspx.

Cruickshank, Paul, and Robyn Kriel. "Source: 'Sophisticated' Laptop Bomb on Somali Plane Got through X-Ray Machine." CNN, February 11, 2016. https://www.cnn.com/2016/02/11/africa/somalia-plane-bomb/index.html.

Cybersecurity and Infrastructure Security Agency. "Defining Insider Threats." America's Cyber Defense Agency. Accessed October 30, 2023. https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats.

Daines, Steve and Zinke, Ryan. "Letter to TSA Regarding Aviation Worker-Screening Rule," August 23, 2023. https://www.daines.senate.gov/wp-content/uploads/2023/08/2023.08.23_Letter-to-TSA-re-Aviation-Worker-Screening-Rule.pdf.

De Valk, Giliam. "On Screening and the Insider Threat – A Methodological Exploration." *National Security and the Future* 20, no. 1–2 (January 9, 2020): 35–50. https://doi.org/10.37458/nstf.20.1-2.5.

Department of Homeland Security. "View Rule: 1652-AA70." Office of Information and Regulatory Affairs, November 2018. https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201810&RIN=1652-AA70.

Department of Homeland Security, Homeland Security Investigations. "Flight Attendants Charged with Smuggling Drug Money into Dominican Republic." Homeland Security Investigations, May 2024. https://www.dhs.gov/hsi/news/2024/05/08/flight-attendants-charged-smuggling-drug-money-dominican-republic.

Department of Homeland Security, Office of Science and Technology. "Master Question List (MQL) for Synthetic Opioids." Washington, DC: Department of Homeland Security, Office of Science and Technology, September 2021. https://www.dhs.gov/sites/default/files/publications/21_1110_st_csac_mql_synthetic_opioids_30sep2021_pr_508.pdf.

Dixit, Avinash. "Entry and Exit Decisions under Uncertainty." *Journal of Political Economy* 97, no. 3 (1989): 620–38. https://www.jstor.org/stable/1830458.

Drug Enforcement Agency. "Facts about Fentanyl." United States Drug Enforcement Agency, 2023. https://www.dea.gov/resources/facts-about-fentanyl.

Elias, Bart. *Strange Occurrences Highlight Insider Threat to Aviation Security*. CRS Report No. IN10954. Washington, DC: Congressional Research Service, 2018. https://crsreports.congress.gov/product/pdf/IN/IN10954/2.

Engineering News-Record. "LAX People Mover Passes Construction Milestone." Transportation, May 11, 2022. https://www.enr.com/articles/54095-lax-people-mover-passes-construction-milestone.

Erkki, Koskela, and Ollikainen Markku. "Optimal Design of Forest Taxation with Multiple-Use Characteristics of Forest Stands." *Environmental and Resource Economics* 10, no. 1 (July 1997): 41–62. https://doi.org/10.1023/A:1026472622826.

Estrella, Timothy. "Airplane Water and Wastewater Systems." Aerospace and Defense, May 2021. https://insights.globalspec.com/article/16509/airplane-water-and-wastewater-systems.

Evains, Tyler. "LAX Transformation More than Halfway Done, Last Phase Underway." *Daily Breeze*, January 28, 2023, Electronic edition, sec. News. https://www.dailybreeze.com/2023/01/28/lax-transformation-more-than-halfway-done-last-phase-underway/.

Fant, Christopher. "United States v. Hernandez, 24 Cr. 447 (RA) (S.D.N.Y. Jul. 26, 2024); Sealed Complaint." Department of Justice, April 30, 2024. https://www.justice.gov/usao-sdny/media/1351111/dl.

Farahmand, Fariborz, and Eugene H. Spafford. "Understanding Insiders: An Analysis of Risk-Taking Behavior." *Information Systems Frontiers* 15, no. 1 (March 2013): 5–15. https://doi.org/10.1007/s10796-010-9265-x.

Fein, Robert A., Bryan Vossekuil, and Gwen A. Holden. "Threat Assessment: An Approach to Prevent Targeted Violence." *Research in Action*, July 1995, 1–7. https://doi.org/10.1037/e517592006-001.

Ferguson, Naill. *Virtual History: Alternatives and Counterfactuals*. London: Macmillan, 1997.

Fong, Philip. "Police Open Fire at Paris Train Station on Woman Making 'Threats.'" *Digital Journal*, October 31, 2023, sec. World. https://www.digitaljournal.com/world/police-open-fire-at-paris-train-station-on-woman-making-threats/article.

Gambler, Rebecca. *CBP Should Update Policies and Enhance Analysis of Inspections*. GAO-19-658. Washington, DC: Government Accountability Office, 2019. https://www.gao.gov/assets/710/700787.pdf.

Gates, Megan. "Insider Threat: The Shift from Report to Support." *Security Management*, September 1, 2021. http://www.asisonline.org/security-management-magazine/articles/2021/09/insider-threat-the-shift-from-report-to-support/.

Glimcher, Paul W., and Ernst Fehr. *Neuroeconomics: Decision Making and the Brain*. 2nd ed. Boston, MA: Academic Press, 2014.

Gramlich, John. "Federal Criminal Prosecutions Fall to Lowest Level in Nearly Two Decades." Pew Research Center, March 28, 2017. https://www.pewresearch.org/short-reads/2017/03/28/federal-criminal-prosecutions-fall-to-lowest-level-in-nearly-two-decades/.

Grizzle, Jessica. *Insider Threat Mitigation at Airports*. Louisville, TN: National Safe Skies Alliance, Inc., 2021. https://www.sskies.org/images/uploads/subpage/PARAS_0026_InsiderThreatMitigation.FinalReport_.pdf.

Gül, Serdar Kenan. "An Evaluation of the Rational Choice Theory in Criminology." *Sociology and Applied Sciences* 4, no. 8 (2009): 36–44.

Harrison, Glenn W., and E. Elisabet Rutström. "Risk Aversion in the Laboratory." In *Research in Experimental Economics*, 12:41–196. Bingley, UK: Emerald, 2008. https://doi.org/10.1016/S0193-2306(08)00003-3.

Hay, Carter, and Walter Forrest. "The Development of Self-Control: Examining Self-Control Theory's Stability Thesis." *Criminology* 44, no. 4 (November 2006): 739–74. https://doi.org/10.1111/j.1745-9125.2006.00062.x.

Hirschi, Travis. *Causes of Delinquency*. New Brunswick, NJ: Transaction Publishers, 2002.

Hoffman, Bruce. *Inside Terrorism*. 3rd ed. New York: Columbia University Press, 2017.

Holler, Manfred J. "Classical, Modern and New Game Theory." Working paper, Yale Law School, August 2001. https://law.yale.edu/sites/default/files/documents/pdf/holler.pdf.

Homeland Security & Government Affairs. "Chairman Johnson Asks TSA for Solutions on Passenger Screening and Insider Threats." Majority News, June 7, 2016. https://www.hsgac.senate.gov/media/reps/icymi-chairman-johnson-asks-tsa-for-solutions-on-passenger-screening-and-insider-threats/.

Hsu, Andrea. "Strike Ends for Dockworkers." NPR All Things Considered, October 4, 2024. https://www.npr.org/2024/10/03/nx-s1-5139450/dockworkers-port-strike-deal.

Huang, Linan, and Quanyan Zhu. "Duplicity Games for Deception Design with an Application to Insider Threat Mitigation." *IEEE Transactions on Information Forensics and Security* 16 (2021): 4843–56. https://doi.org/10.1109/TIFS.2021.3118886.

Hubbard, Douglas W. *The Failure of Risk Management: Why It's Broken and How to Fix It*. 2nd ed. Hoboken, NJ: Wiley, 2020.

Humphrey, Adam. "Do Innovative Thinkers Pose an Increased Insider Threat?: A Preliminary Analysis." Master's thesis, Naval Postgraduate School, 2019. https://calhoun.nps.edu/bitstream/handle/10945/62735/19Jun_Humphrey_Adam.pdf.

Husband, Charles, and Yunis Alam. *Social Cohesion and Counter-Terrorism: A Policy Contradiction?* Portland, OR: Policy Press, 2011.

Infrastructure Management Programme and Airports Council International. *State of Airport Economics*. Montreal, Canada: International Civil Aviation Organization, 2015. https://www.icao.int/sustainability/airport_economics/state%20of%20airport%20economics.pdf.

International Civil Aviation Organization. *ICAO Pamphlet: Managing Insider Risks*. 1st ed. Montreal, Canada: ICAO Aviation Security, 2022. https://www.icao.int/Security/Security-Culture/State%20and%20Industry%20Promotional%20Material/ICAO%20Pamphlet%20Managing%20Insider%20Risks.pdf.

International Civil Aviation Organization, Aviation Security. *Managing Insider Risks*. 01 ed. Montréal: ICAO HQ, 2022. https://www.icao.int/Security/Security-Culture/State%20and%20Industry%20Promotional%20Material/ICAO%20Pamphlet%20Managing%20Insider%20Risks.pdf.

Jackie Brown. Crime, Drama, Thriller. Miramax, A Band Apart, Lawrence Bender Productions, 1997.

Jackson, Matthew O. "Mechanism Theory." Working paper, California Institute of Technology, 2003. http://www.ssrn.com/abstract=2542983.

Jaummer. "El Al's Legendary Security." FlyerTalk Forums, December 5, 2001. https://www.flyertalk.com/forum/el-al-matmid/61931-el-al-s-legendary-security.html.

Jet, Johnny. "You Probably Won't Be Drinking the Water, Coffee or Tea on Airplanes After Reading This." Johnny Jet, May 7, 2024. https://johnnyjet.com/you-probably-wont-be-drinking-the-water-coffee-or-tea-on-airplanes-after-reading-this/.

Kahneman, Daniel, and Amos Tversky. "Prospect Theory: An Analysis of Decision Under Risk." *Econometrica* 47, no. 2 (March 1979): 263–91. https://doi.org/10.2307/1914185.

Kearns, Michael, Mallesh M. Pai, Aaron Roth, and Jonathan Ullman. "Mechanism Design in Large Games: Incentives and Privacy." *American Economic Review* 104, no. 5 (May 2014): 431–35. https://doi.org/10.1257/aer.104.5.431.

Keightley, Mark P. *Why Subsidize Homeownership? A Review of the Rationales*. CRS Report No. IF11305. Washington, DC: Congressional Research Service, 2019.

Keller, Elena, Jade E. Newman, Andreas Ortmann, Louisa R. Jorm, and Georgina M. Chambers. "How Much Is a Human Life Worth? A Systematic Review." *Value in Health* 24, no. 10 (October 2021): 1531–41. https://doi.org/10.1016/j.jval.2021.04.003.

Keshner, Andrew, and Thomas Tracy. "Woman Busted at JFK Airport Smuggling Cocaine in Motorized Wheelchair's Cushion." *Daily News*, June 13, 2017, Online edition, sec. New York News. https://www.cclec.org/enforcement/woman-busted-at-jfk-airport-smuggling-cocaine-in-motorized-wheelchairs-cushion/.

Kirkpatrick, Shelley. "Refining Insider Threat Profiles." *Security Magazine* 45, no. 9 (September 2008): 56–63.

Krauss, Kevin. "DFW Airport Drug-Smuggling Crew That Offered to Fly Explosives Admits Guilt." *Dallas News*, May 10, 2019, sec. Crime. https://www.dallasnews.com/news/crime/2019/05/10/dfw-airport-drug-smuggling-crew-that-offered-to-fly-explosives-admits-guilt/.

Kriel, Robyn, and Faith Karimi. "Airport Workers Seen with Laptop in Somalia Jet Blast." CNN, February 8, 2016. https://www.cnn.com/2016/02/07/africa/somalia-airplane-explosion-video/index.html.

Krishnan, Vik, Shannon Peloquin, Aprameya Rao, and Bill Swelbar. "Turning on the Revenue Tap: How U.S. Airports Could Make the Most of Additional Liquidity." Business and Lobby Group. Mckinsey, February 8, 2022. https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/turning-on-the-revenue-tap-how-us-airports-could-make-the-most-of-additional-liquidity.

Kugler, Tamar, J. Cole Smith, Terry Connolly, and Young-Jun Son, eds. "Improving and Measuring the Effectiveness of Decision Analysis: Linking Decision Analysis and Behavioral Decision Research." In *Decision Modeling and Behavior in Complex and Uncertain Environments*, Vol. 21. Springer Optimization and Its Applications. New York: Springer New York, 2008. https://doi.org/10.1007/978-0-387-77131-1.

Kuhn, Steven T. "Reflections on Ethics and Game Theory." *Synthese* 141, no. 1 (July 2004): 1–44. https://doi.org/10.1023/B:SYNT.0000035846.91195.cb.

Kunreuther, Howard, and Geoffrey Heal. "Interdependent Security." *Journal of Risk and Uncertainty* 26, no. 2 (May 2003): 231–49. https://www.jstor.org/stable/41755017.

LaGrave, Katherine. "How TSA's 'Quiet Skies' Program Tracks U.S. Passengers." Condé Nast Traveler, July 2018. https://www.cntraveler.com/story/how-tsa-quiet-skies-program-tracks-us-passengers.

Lam, Oiwan, and Eunsoo Lee. "Can Childbirth Subsidies Solve South Korea's Low Birth Rate?" Global Voices Online, May 20, 2024. https://globalvoices.org/2024/05/20/can-childbirth-subsidies-solve-south-koreas-low-birth-rate/.

Langer, Thomas, and Martin Weber. "Prospect Theory, Mental Accounting, and Differences in Aggregated and Segregated Evaluation of Lottery Portfolios." *Management Science* 47, no. 5 (May 2001): 716–33. https://doi.org/10.1287/mnsc.47.5.716.10483.

Lenzenweger, Mark F., and Eric D. Shaw. "The Critical Pathway to Insider Risk Model: Brief Overview and Future Directions." *Counter-Insider Threat Research and Practice* 1, no. 1 (August 2, 2022). https://citrap.scholasticahq.com/article/36186.

Levin, Irwin P., Sandra L. Schneider, and Gary J. Gaeth. "All Frames Are Not Created Equal: A Typology and Critical Analysis of Framing Effects." *Organizational Behavior and Human Decision Processes* 76, no. 2 (November 1998): 149–88. https://doi.org/10.1006/obhd.1998.2804.

Levine, David I., Michael W. Toffel, and Matthew S. Johnson. "Randomized Government Safety Inspections Reduce Worker Injuries with No Detectable Job Loss." *Science* 336, no. 6083 (2012): 907–11. https://www.jstor.org/stable/41584864.

Lewis, Nehama, and Erga Atad. "Effects of Message Framing and Narrative Format on Promoting Persuasive Conversations with Others About the Flu Vaccine." *Health Communication* 39, no. 10 (August 23, 2024): 2110–22. https://doi.org/10.1080/10410236.2023.2257427.

Loffi, Jon M., and Ryan J. Wallace. "The Unmitigated Insider Threat to Aviation (Part 1): A Qualitative Analysis of Risks." *Journal of Transportation Security* 7 (2014): 289–305. https://doi.org/10.1007/s12198-014-0144-4.

Lom, Ionut Valentin. "Current Global Trends of Aviation Insurance." *INCAS BULLETIN* 14, no. 4 (December 2, 2022): 195–200. https://doi.org/10.13111/2066-8201.2022.14.4.16.

Los Angeles World Airports. *Fiscal Year 2023–2024 Proposed Budget*. Los Angeles: Los Angeles World Airports Board of Airport Commissioners, 2023. https://www.lawa.org/-/media/lawa-web/lawa-investor-relations/files/lawa-annual-budget/2023/lawa-annual-budget-fy-2024.ashx.

Lowers & Associates. "The Impact of Workplace Violence." Risk Management Blog, May 19, 2016. http://www.lowersriskgroup.com/blog/2016/05/19/infographic-impact-workplace-violence/.

Ludwig Institute for Shared Economic Prosperity. "True Rate of Unemployment," October 2024. https://www.lisep.org/tru.

Maley, Kim, Kate Sanders, Shaun Cardiff, and Jonathan Webster. "Effective Workplace Culture: The Attributes, Enabling Factors and Consequences of a New Concept." *International Practice Development Journal* 1, no. 2 (October 2011): 1–29. https://www.fons.org/wp-content/uploads/2024/03/IPDJ_0102_01.pdf.

Manancourt, Vincent. "'Millions of People's Data Is at Risk' — Amazon Insiders Sound Alarm over Security." Politico, February 24, 2021. https://www.politico.eu/article/data-at-risk-amazon-security-threat/.

Mas-Colell, Andreu, Michael Dennis Whinston, and Jerry R. Green. *Microeconomic Theory*. New York: Oxford University Press, 1995.

Mata, Rui, Renato Frey, David Richter, Jürgen Schupp, and Ralph Hertwig. "Risk Preference: A View from Psychology." *Journal of Economic Perspectives* 32, no. 2 (Spring 2018): 155–72. https://doi.org/10.1257/jep.32.2.155.

Mathew, Taj. "Insider Threat: A Constant Problem with a Continuous Approach." Master's thesis, Naval Postgraduate School, 2023. https://hdl.handle.net/10945/71985.

Mayorkas, Alejandro. *DHS Agency Financial Report FY2022*. Washington, DC: Department of Homeland Security, 2022. https://www.dhs.gov/sites/default/files/2022-11/dhs_agency_financial_report_fy2022.pdf.

McMasters, Michael. "Societal Polarization: An Evolving Threat to U.S. Homeland Security." Master's thesis, Naval Postgraduate School, 2023. https://hdl.handle.net/10945/72572.

McMunn, Andrew. "Man Arrested at JFK Airport after 40 Lbs. of Cocaine Found in Bags of Jumbo Shrimp, Federal Officials Say." WLBT3, January 21, 2024. https://www.wlbt.com/2024/01/21/man-arrested-jfk-airport-after-40-lbs-cocaine-found-bags-jumbo-shrimp-federal-officials-say/.

McNeil, Triana. *Airport Worker Screening: TSA Could Further Strengthen Its Approach to Estimating Costs and Feasibility of Security Measures*. GAO-21-273. Washington, DC: United States Government Accountability Office, 2021. https://www.gao.gov/assets/gao-21-273.pdf.

———. *Aviation Security: TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals*. GAO-20-275. Washington, DC: Government Accountability Office, 2020. https://www.gao.gov/assets/gao-20-275.pdf.

Miller, Rod, and John E. Wetzel. "Jail Vulnerability Assessment: A Systems Approach to Improve Safety and Security." Working draft. Washington, DC, December 2008. https://correction.org/wp-content/uploads/2014/10/Jail-Vulnerability-Assessment-JVA-Final-Draft.pdf.

Mookherjee, Dilip, and Masatoshi Tsumagari. "Mechanism Design with Communication Constraints." *Journal of Political Economy* 122, no. 5 (October 2014): 1094–1129. https://doi.org/10.1086/676931.

Nash, John F. "Equilibrium Points in N-Person Games." *Proceedings of the National Academy of Sciences of the United States of America* 36, no. 1 (1950): 48–49. http://www.jstor.org/stable/88031.

National Research Council. *Review of the Department of Homeland Security's Approach to Risk Analysis*. Washington, DC: National Academies Press, 2010. https://doi.org/10.17226/12972.

Navon, Aviad, Gefen Ben Yosef, Ram Machlev, Shmuel Shapira, Nilanjan Roy Chowdhury, Juri Belikov, Ariel Orda, and Yoash Levron. "Applications of Game Theory to Design and Operation of Modern Power Systems: A Comprehensive Review." *Energies* 13, no. 15 (January 2020): 3982. https://doi.org/10.3390/en13153982.

Nelu, Clarisa. "Exploitation of Generative AI by Terrorist Groups." International Centre for Counter-Terrorism – ICCT, June 10, 2024. https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

Newburn, Tim. "The Inevitable Fallibility of Policing." *Policing and Society* 32, no. 3 (2022): 434–50. https://doi.org/10.1080/10439463.2022.2037557.

Office of the Inspector General. *Audit of Access to Airport Secured Areas (Unclassified Summary)*. OIG-07-35. Washington, DC: Department of Homeland Security, 2007. https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/OIG_07-35_Mar07.pdf.

Omar, Feisal, and Abdi Sheikh. "Somalia Sentences Two to Life in Prison for February Airline Blast." Reuters, May 30, 2016. https://www.reuters.com/article/idUSKCN0YL1DJ/.

Paramount Business Jets. "Airbus A320 Charter – Rental Cost and Hourly Rate." Accessed July 12, 2024. https://www.paramountbusinessjets.com/private-jet-charter/aircraft/airbus-a320.

Pascale, Jordan. "What You Need to Know About Taking the Silver Line to Dulles." DCist. Accessed January 15, 2025. https://dcist.com/story/22/11/02/what-you-need-to-know-about-taking-the-silver-line-to-dulles/.

Pekoske, David. "2023 TSA Year in Review." Transportation Security Administration, 2024. https://www.tsa.gov/sites/default/files/17228_info_tsa_2023_year_in_review.pdf.

———. "2023 Year in Review: TSA Highlights a Year of Innovation and Improvements to Security Effectiveness, Efficiency and the Passenger Experience." Transportation Security Administration, January 12, 2024. https://www.tsa.gov/news/press/releases/2024/01/12/2023-year-review-tsa-highlights-year-innovation-and-improvements.

Peltz, Jennifer. "'Finch-Smuggling Kingpin' Gets Prison Time for Sneaking Birds Into NY for Competitions." NBC New York, February 10, 2023. https://www.nbcnewyork.com/news/local/crime-and-courts/finch-smuggling-kingpin-gets-prison-time-for-sneaking-birds-into-ny-for-competitions/4096768/.

Persico, Nicola, and Petra E. Todd. "Passenger Profiling, Imperfect Screening, and Airport Security." *The American Economic Review* 95, no. 2 (2005): 127–31. https://www.jstor.org/stable/4132803.

Phillips, Peter J., and Gabriela Pohl. "Prospect Theory and Terrorist Choice." *Journal of Applied Economics* 17, no. 1 (May 2014): 139–60. https://doi.org/10.1016/S1514-0326(14)60006-4.

Piraveenan, Mahendra. "Applications of Game Theory in Project Management: A Structured Review and Analysis." *Mathematics* 7, no. 9 (2019): 858. https://doi.org/10.3390/math7090858.

Ponemon Institute. *Ponemon Insider Threats Global Report – 2022*. Traverse City, MI: Ponemon Institute, 2023. https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-the-cost-of-insider-threats-ponemon-report.pdf.

Potapov, Serge, and Philip Kaplan. *Privacy Impact Assessment for the Insider Threat Unit Database*. Washington, DC: Department of Homeland Security, 2018. https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa048-april2018.pdf.

Pratt, Travis C. "A Self-Control/Life-Course Theory of Criminal Behavior." *European Journal of Criminology* 13, no. 1 (2016): 129–46. https://doi.org/10.1177/1477370815587771.

Proctor, Michael S. "The Deterrent Effect of the Death Penalty: A Rational Choice Case Study." PhD diss., University of Arizona Global Campus, 2021. https://www.proquest.com/docview/2566283818.

Propper, David. "American Airlines Mechanic Convicted of Stashing $320K of Cocaine under Cockpit of Plane." *New York Post*, May 3, 2023, Electronic edition. https://nypost.com/2023/05/03/american-airlines-mechanic-convicted-of-stashing-320k-of-cocaine-under-cockpit-of-plane/.

Quinn, Rob. "Feds: Flight Attendants Smuggled $8M in Drug Money." Newser, May 9, 2024. https://www.newser.com/story/350095/4-flight-attendants-accused-of-smuggling-drug-money.html.

Reitstetter, Raven, and Travis Losser. "The Synthetic Opioid Fentanyl Is Degraded by Temperature and Ultraviolet Irradiation in the Environment." Environmental Protection Agency, January 2017. https://www.epa.gov/sites/default/files/2018-11/documents/decon_poster_099.pdf.

Rennhack, Michael D. "Unescorted Access vs. Security Clearance." NukeWorker Forum, October 2013. https://www.nukeworker.com/forum/index.php?topic=37139.0.

Republic of Somaliland. "Department of Civil Aviation and Regulation." Accessed November 7, 2024. https://caaa.govsomaliland.org/article/department-civil-aviation-and-regulation.

Risk Management Group. "General Liability Insurance for Airport Service Providers." Risk Management Group. Accessed December 8, 2024. https://trmg.net/policies/airport-service-liability/.

Ritchey, Diane. "See It, Say It, Spread the Message in Las Vegas." *Security Magazine: Security and Business Resilience*, June 6, 2011. https://www.securitymagazine.com/articles/82102-see-it-say-it-spread-the-message-in-las-vegas.

Rivers, Martin. "Learning the Lessons of a Lucky Escape." Air Transport, September 15, 2016. https://www.timesaerospace.aero/features/air-transport/learning-the-lessons-of-a-lucky-escape.

Roberts, Harrison. "Airline Employee, Heading DFW Airport Drug-Smuggling Ring, Sentenced to 16 Years in Prison." KCBD, December 6, 2019. https://www.kcbd.com/2019/12/06/airline-employee-heading-dfw-airport-drug-smuggling-ring-sentenced-years-prison/.

Rose, Adam, Misak Avetisyan, Heather Rosoff, William J. Burns, Paul Slovic, and Oswin Chan. "The Role of Behavioral Responses in the Total Economic Consequences of Terrorist Attacks on U.S. Air Travel Targets." *Risk Analysis* 37, no. 7 (2017): 1403–18. https://doi.org/10.1111/risa.12727.

Sanou, Hanneke. "Police Arrest Six Airport Workers for Drug Smuggling." *Dutch News*, May 31, 2024. https://www.dutchnews.nl/2024/05/police-arrest-six-airport-workers-for-drug-smuggling/.

Sarr, Hamet, Mohamed Ali Bchir, and François CoChard. "Is the 'Average Pigouvian Tax' Robust to the Size of the Group of Polluters?" *Review of Agricultural, Food and Environmental Studies* 102, no. 3 (September 2021): 285–95. https://doi.org/10.1007/s41130-021-00145-z.

Scott, Robert L. "Protecting the Perimeter: Unmanned Aircraft Systems Enhance National Airport Security." Master's thesis, Naval Postgraduate School, 2023. https://hdl.handle.net/10945/72602.

Scroxton, Alex. "Calls for Clarity over Amazon Insider Breach." *ComputerWeekly*, October 27, 2020. https://www.computerweekly.com/news/252491142/Calls-for-clarity-over-Amazon-insider-breach.

Serrato, Gerardo H. "Defund or Unbundle the Police? A Strategy to Enhance the Reputation and Morale of Law Enforcement Agencies in The United States." Master's thesis, Naval Postgraduate School, 2022.

Shaw, Eric, Keven Ruby, and Jerrold Post. *The Insider Threat to Information Systems*. Vol. 2–98. Washington, DC: Department of Defense Security Institute, 1998. https://homes.cerias.purdue.edu/~mkr/sab.pdf.

Shea, Tom. "Man Caught at JFK Airport Trying to Smuggle Fentanyl Inside Candles from Mexico." News Source. 4NBC New York, April 12, 2023. https://www.nbcnewyork.com/news/local/crime-and-courts/man-caught-at-jfk-airport-trying-to-smuggle-fentanyl-inside-candles-from-mexico/4235727/.

Simon, Herbert A. "Bounded Rationality." In *Utility and Probability*, edited by John Eatwell, Murray Milgate, and Peter Newman, 15–18. London: Palgrave Macmillan UK, 1990. https://doi.org/10.1007/978-1-349-20568-4_5.

———. "Bounded Rationality in Social Science: Today and Tomorrow." *Mind & Society* 1, no. 1 (March 2000): 25–39. https://doi.org/10.1007/BF02512227.

"Social Identity Theory." Accessed September 12, 2023. https://www.age-of-the-sage.org/psychology/social/social_identity_theory.htm.

Software Engineering Institute. *Common Sense Guide to Mitigating Insider Threats*. 7th ed. Pittsburg, PA: Carnegie Mellon University, 2022. https://insights.sei.cmu.edu/documents/5777/5692_CSG_Book_20-optimized.pdf.

Sokol-Hessner, Peter, and Robb B. Rutledge. "The Psychological and Neural Basis of Loss Aversion." *Current Directions in Psychological Science* 28, no. 1 (2019): 20–27. https://doi.org/10.1177/0963721418806510.

Somers, Margaret R. "Symposium on Historical Sociology and Rational Choice Theory." *American Journal of Sociology* 104, no. 3 (November 1998): 722–84. https://doi.org/10.1086/210085.

Sommerfeld-Klatta, Karina, Wiktoria Jiers, Magdalena Łukasik-Głębocka, Artur Tezyk, Klaudia Dolińska-Kaczmarek, Kamil Walter, Paweł Świderski, Szymon Rzepczyk, Barbara Zielińska-Psuja, and Czesław Żaba. "Severe and Fatal Fentanyl Poisonings from Transdermal Systems after On-Skin and Ingestion Application." *Toxics* 11, no. 10 (2023): 1–10. https://doi.org/10.3390/toxics11100872.

Souza, W.A.V., and M. C. Malavazi. "Game Theory: An Approach Through History and Its Applications." *Scientific Electronic Archives* 12, no. 1 (February 2019): 138–47. https://doi.org/10.36560/1212019642.

Stana, Richard. *Customs and INS: Random Inspection Programs Can Be Strengthened*. GAO-02-215R. Washington, DC: Government Accountability Office, 2001. https://www.gao.gov/assets/gao-02-215r.pdf.

Stanley, Jay. "How the TSA's Facial Recognition Plan Will Go Far Beyond the Airport." American Civil Liberties Union: News and Commentary, October 22, 2018. https://www.aclu.org/news/privacy-technology/how-tsas-facial-recognition-plan-will-go-far.

Strand, Jon. *Importer and Producer Petroleum Taxation: A Geo-Political Model*. Vol. 2008. Washington, DC: International Monetary Fund, 2008. https://www.elibrary.imf.org/view/journals/001/2008/035/article-A001-en.xml.

Strindberg, Anders. "Social Identity Theory and the Study of Terrorism and Violent Extremism." Research. Totalförsvarets forskningsinstitut (Total Defense Research Institute), December 2020. https://www.foi.se/rest-api/report/FOI-R--5062--SE.

Stronghold Engineering. "Air Operations Area Perimeter Fence Project." Stronghold Engineering, September 21, 2012. https://www.strongholdengineering.com/projects/air-operations-area-perimeter-fence-project/.

Sunset Aviation Insurance. "Airport Liability Insurance." Sunset Aviation Insurance, Persistent and Undated. https://sunsetais.com/airport-liability-insurance/.

Tajfel, Henri, and John Turner. "An Integrative Theory of Intergroup Conflict." In *Organizational Identity*, edited by Mary Jo Hatch and Majken Schultz, 56–65. Oxford, UK: Oxford University Press, 2000. https://doi.org/10.1093/oso/9780199269464.003.0005.

Tamir, Christine. "Key Findings about Black Immigrants in the U.S." Pew Research Center, January 27, 2022. https://www.pewresearch.org/short-reads/2022/01/27/key-findings-about-black-immigrants-in-the-u-s/.

Tamman, Maurice, Laura Gottesdiener, and Stephen Eisenhammer. "We Bought What's Needed to Make Millions of Fentanyl Pills–for $3,600." Reuters, July 25, 2024. https://www.reuters.com/investigates/special-report/drugs-fentanyl-supplychain/.

Taquechel, Eric F. and Ted G. Lewis. "More Options for Quantifying Deterrence and Reducing Critical Infrastructure Risk: Cognitive Biases." *Homeland Security Affairs* XII (September 2016): Article 3. https://www.hsaj.org/articles/12007.

Taquechel, Eric, and Ted G. Lewis. "Risk, Deterrence, and Prospect Theory: Decision Bias Influence on Quantifiable Deterrence Efficacy in Reducing Risk." *Homeland Security Affairs* XVIII (November 2022). https://www.hsaj.org/articles/21639.

Thai, Tuyet-Quan. "TSA Can Improve Aviation Worker Vetting." GAO Report. Washington, DC: Department of Homeland Security Office of the Inspector General, June 2014. https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/2015/OIG_15-98_Jun15.pdf.

The Flight Attendant. Comedy, Drama, Mystery. Warner Bros. Television, Berlanti Productions, Yes, Norman Productions, 2020.

Tilo, Dexter. "Amazon Fined for 'excessive' Employee Monitoring." Human Resources Director, January 24, 2024. https://www.hcamag.com/us/specialization/employment-law/amazon-fined-for-excessive-employee-monitoring/474239.

Transportation Security Administration. *49 CFR 1520 – The SSI Federal Regulation*. Washington, DC: Department of Homeland Security. Accessed September 22, 2024. https://www.tsa.gov/sites/default/files/49_cfr_part_1520.pdf.

———. "Sensitive Security Information." Transportation Security Administration, June 2023. https://www.tsa.gov/for-industry/sensitive-security-information.

———. *SSI Best Practices Guide*. Washington, DC: Transportation Security Administration, 2023. https://www.tsa.gov/sites/default/files/ssi_best_practices_guide_for_non-dhs_employees.pdf.

———. "The TSA Workforce Has Adapted to the Changing Threat Environment, Remains Steadfast and Committed to Securing the Nation's Transportation Systems." Statements, October 27, 2022. https://www.tsa.gov/news/press/statements/2022/10/27/tsa-workforce-has-adapted-changing-threat-environment-remains.

———. "TSA Detects 6,737 Firearms at Airport Security Checkpoints in 2023." Transportation Security Administration. Accessed January 12, 2025. https://www.tsa.gov/news/press/releases/2024/01/10/tsa-detects-6737-firearms-airport-security-checkpoints-2023.

———. "TSA Insider Threat Awareness." Symposium Briefing. Montreal, Canada: International Civil Aviation Organization, November 2018. https://www.icao.int/Meetings/AVSEC2018/Documents/TSA%20Insider%20Threat.pdf#search=employee%20screening.

———. "TWIC." Transportation Security Administration, 2024. https://www.tsa.gov/twic.

Turner, J. C., R. J. Brown, and H. Tajfel. "Social Comparison and Group Interest in Ingroup Favouritism." *European Journal of Social Psychology* 9, no. 2 (1979): 187–204. https://doi.org/10.1002/ejsp.2420090207.

Turner, Marlene E., Anthony R. Pratkanis, Preston Probasco, and Craig Leve. "Threat, Cohesion, and Group Effectiveness: Testing a Social Identity Maintenance Perspective on Groupthink." *Journal of Personality and Social Psychology* 63, no. 5 (November 1992): 781–96. https://doi.org/10.1037/0022-3514.63.5.781.

Tversky, Amos, and Daniel Kahneman. "Advances in Prospect Theory: Cumulative Representation of Uncertainty." *Journal of Risk & Uncertainty* 5, no. 4 (October 1992): 297–323. https://doi.org/10.1007/BF00122574.

United Nations Office on Drugs and Crime. *Handbook on Dynamic Security and Prison Intelligence*. Vienna: United Nations, 2015. https://www.unodc.org/documents/justice-and-prison-reform/UNODC_Handbook_on_Dynamic_Security_and_Prison_Intelligence.pdf.

U.S. Attorney's Office, Northern District of Texas. "Lead Defendant in DFW Airport Drug-Smuggling Ring Sentenced to 16+ Years." United States Department of Justice Northern District of Texas, December 6, 2019. https://www.justice.gov/usao-ndtx/pr/lead-defendant-dfw-airport-drug-smuggling-ring-sentenced-16-years.

U.S. Attorney's Office, Southern District of New York. "Flight Attendants Charged in Connection with Smuggling Drug Money to the Dominican Republic." United States Department of Justice Southern District of New York, May 8, 2024. https://www.justice.gov/usao-sdny/pr/flight-attendants-charged-connection-smuggling-drug-money-dominican-republic.

U.S. Immigration and Customs Enforcement. "HSI Special Agents at JFK International Airport Work 'To Catch a Smuggler,'" February 10, 2023. https://www.ice.gov/news/releases/hsi-special-agents-jfk-international-airport-work-catch-smuggler.

Van Knippenberg, Daan, and Els C. M. Van Schie. "Foci and Correlates of Organizational Identification." *Journal of Occupational and Organizational Psychology* 73, no. 2 (2000): 137–47. https://doi.org/10.1348/096317900166949.

Vergun, David. "All DoD Personnel Now Receive Continuous Security Vetting." DoD News, October 5, 2021. https://www.defense.gov/News/News-Stories/Article/Article/2800381/all-dod-personnel-now-receive-continuous-security-vetting/.

Vespa, Jonathan, Armstrong, David, and Medina, Lauren. "Demographic Turning Points for the United States: Population Projections for 2020 to 2060." U.S. Census Bureau, March 2018.

Viale, Riccardo, Shaun Gallagher, and Vittorio Gallese. "Bounded Rationality, Enactive Problem Solving, and the Neuroscience of Social Interaction." *Frontiers in Psychology* 14 (2023): 1–9. https://doi.org/10.3389/fpsyg.2023.1152866.

Wallace, Ryan J., and Jon M. Loffi. "The Unmitigated Insider Threat to Aviation (Part 2): An Analysis of Countermeasures." *Journal of Transportation Security* 7 (2014): 307–31. https://doi.org/10.1007/s12198-014-0150-6.

Walter, Karla, and Aurelia Glass. "Airport Service Workers Deserve Good Jobs." Center for American Progress, March 7, 2023. https://www.americanprogress.org/article/airport-service-workers-deserve-good-jobs/.

Whitty, Monica T. "Developing a Conceptual Model for Insider Threat." *Journal of Management and Organization* 27, no. 5 (2021): 911–29. https://doi.org/10.1017/jmo.2018.57.

Wichter, Zach. "Is Airplane Coffee and Tea Safe to Drink?" *USA Today*, August 2023, Online edition, sec. Cruising Altitude. https://www.usatoday.com/story/travel/columnist/2023/08/23/airplane-coffee-tea-safe-drink/70653256007/.

Willison, Robert, and Merrill Warkentin. "Beyond Deterrence: An Expanded View of Employee Computer Abuse." *MIS Quarterly* 37, no. 1 (March 2013): 1–20. https://doi.org/10.25300/MISQ/2013/37.1.01.

Wisconsin Department of Health Services. "Dose of Reality: Get the Facts on Opioids." Wisconsin Department of Health Services, January 30, 2022. https://www.dhs.wisconsin.gov/opioids/facts.htm.

Wooldredge, John. "Prison Culture, Management, and In-Prison Violence." *Annual Review of Criminology* 3 (2020): 165–88. https://doi.org/10.1146/annurev-criminol-011419-041359.

World Economic Forum. *Global Risks Report 2023*. Zurich: World Economic Forum, 2024. https://www.weforum.org/reports/globalrisks-report-2023/.

Wright, George. "Brussels Shooting: 'Europe Shaken' after Two Swedes Shot Dead." BBC News, October 16, 2023. https://www.bbc.com/news/world-europe-67129117.

WSYX Staff. "Chillicothe SWAT Team Seizes 38 Grams of Fentanyl in Drug Bust." WSYX, June 23, 2022. https://cwcolumbus.com/news/local/chillicothe-swat-team-seizes-28-grams-of-fentanyl-in-drug-bust-detective-division-search-warrant-crack-cocaine-paraphernalia-charges-jefferson-avenue.

Xue, Gui, Chuansheng Chen, Zhong-Lin Lu, and Qi Dong. "Brain Imaging Techniques and Their Applications in Decision-Making Research." *Acta Psychologica Sinica* 42, no. 1 (2010): 120–37. https://doi.org/10.3724/SP.J.1041.2010.00120.

Yahoo News. "Brussels Shooting: Man Arrested on Suspicion of Supplying Gun to Assailant in Deadly Attack," October 26, 2023. https://news.yahoo.com/brussels-shooting-man-arrested-suspicion-182722591.html.

Zahidi, Saadia. *Future of Jobs Report 2025*. Geneva: World Economic Forum, 2025. https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf.

Zamost, Scott, and Morgan Brennan. "Take a First-Ever Look at How LAX Airport Targets Threats from Airport Workers." Airlines, September 7, 2017. https://www.cnbc.com/2017/09/07/inside-lax-airport-security-as-it-targets-insider-threats.html.

Zeballos, Melina, Carla Sophie Fumagalli, Signe Maria Ghelfi, and Adrian Schwaninger. "Why and How Unpredictability Is Implemented in Aviation Security – A First Qualitative Study." *Heliyon* 9 (2023): 1–13. https://doi.org/10.1016/j.heliyon.2023.e13822.

Zeigler, Zachary D. "Leveraging DHS Assets: Potential for the Transportation Security Administration to Enhance U.S. Government Intelligence Capabilities." Master's thesis, Naval Postgraduate School, 2021. https://hdl.handle.net/10945/68400.

ZipRecruiter. "$16-$37/Hr Airport Security Screener Jobs in Los Angeles." ZipRecruiter. Accessed December 8, 2024. https://www.ziprecruiter.com/Jobs/Airport-Security-Screener/-in-Los-Angeles,CA.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California