NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

E PLURIBUS ANALYSIS: APPLYING A "SUPERFORECASTING" METHODOLOGY TO THE DETECTION OF HOMEGROWN VIOLENCE

by

James G. Huse

March 2018

Thesis Co-Advisors: Robert Simeral
Christopher Bellavita

THIS PAGE INTENTIONALLY LEFT BLANK

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

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE E PLURIBUS ANALYSIS: APPLYING A "SUPERFORECASTING" METHODOLOGY TO THE DETECTION OF HOMEGROWN VIOLENCE	**5. FUNDING NUMBERS**
6. AUTHOR(S) James G. Huse	
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. IRB number NPS.2017.0076-IR-EP7-A.

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

13. ABSTRACT (maximum 200 words)

This thesis examines investigative decision making, cognitive biases, talent sharing, and the relationship between the random nature of lone-actor violence and a set of predefined decision-making protocols. This research included running four simulations using the Monte Carlo technique, which illustrated that with the dedication of additional resources came a concomitant effect of diminishing returns, opportunity cost, and exposure to liability. The simulations also suggested that regardless of an investigative agency's decision-making processes, the outcome relies on the randomness of the event. To demonstrate a prototype for a new method of threat analysis, a "superforecasting" team of analysts participated in an experimental survey. Nine participants reviewed five threat scenarios and assigned a score based on factors including the potential for violence and immediacy of the threat. Analysis in the survey was accurate for four out of five scenarios. Survey participants also answered six prospect theory questions, set in a homeland security context, to assess their decision making under uncertainty. Considered together, the results from the simulations and the two-part survey explain the relative strength of certain threat assessments. They distinguish what may be detectable from what is statistically unpredictable through the use of a collaborative and multidisciplinary method of analysis.

14. SUBJECT TERMS threat assessment, lone actor violence, assassinations, lone wolf terrorism, school shootings, superforecasting, crowdsourcing, collaboration, prospect theory, decision making, Monte Carlo simulation, Fort Hood	**15. NUMBER OF PAGES** 131
	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

Approved for public release. Distribution is unlimited.

E PLURIBUS ANALYSIS: APPLYING A "SUPERFORECASTING" METHODOLOGY TO THE DETECTION OF HOMEGROWN VIOLENCE

James G. Huse
Assistant Special Agent in Charge, Rome Field Office, U.S. Secret Service
B.A., Michigan State University, 1993
M.A., Wayne State University, 1995

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 2018**

Approved by: Robert Simeral
Thesis Co-Advisor

Christopher Bellavita
Thesis Co-Advisor

Erik Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis examines investigative decision making, cognitive biases, talent sharing, and the relationship between the random nature of lone-actor violence and a set of predefined decision-making protocols. This research included running four simulations using the Monte Carlo technique, which illustrated that with the dedication of additional resources came a concomitant effect of diminishing returns, opportunity cost, and exposure to liability. The simulations also suggested that regardless of an investigative agency's decision-making processes, the outcome relies on the randomness of the event. To demonstrate a prototype for a new method of threat analysis, a "superforecasting" team of analysts participated in an experimental survey. Nine participants reviewed five threat scenarios and assigned a score based on factors including the potential for violence and immediacy of the threat. Analysis in the survey was accurate for four out of five scenarios. Survey participants also answered six prospect theory questions, set in a homeland security context, to assess their decision making under uncertainty. Considered together, the results from the simulations and the two-part survey explain the relative strength of certain threat assessments. They distinguish what may be detectable from what is statistically unpredictable through the use of a collaborative and multidisciplinary method of analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1

II. THESIS PROPOSAL....5
- **A. PROBLEM STATEMENT....5**
- **B. RESEARCH QUESTIONS....7**
- **C. LITERATURE REVIEW....8**
  - **1. Current Organizational Models Struggle to Detect Lone Actor Violence....10**
  - **2. Alternative Organizational Models and Methodologies to Detect Targeted Violence....14**
- **D. RESEARCH DESIGN....18**
  - **1. Limits....19**
  - **2. Data Sources....20**
  - **3. Type and Mode of Analysis....20**

III. BACKGROUND....21
- **A. DEFINITION OF LONE ACTOR VIOLENCE....21**
- **B. LONE ATTACKERS AND "ATTACK RELATED BEHAVIOR"—THE DIFFERENCE BETWEEN THE UNPREDICTABLE AND THE UNDETECTABLE....23**
- **C. STATISTICAL ANALYSIS OF LONE ACTOR VIOLENCE IN THE UNITED STATES—THE IMPOSSIBLE TASK OF PREDICTING RANDOMNESS....24**
  - **1. Using a "Runs Test" to Determine a Temporal Pattern in Lone Actor Attacks....24**
  - **2. Time Series and Geospatial Analysis of Incidents over Time and Space....25**
  - **3. Is Lone Actor Violence Detectable?....26**
  - **4. Legal Considerations—What Is a Threat?....28**
  - **5. Decision Making of the Investigator....30**
  - **6. Treatment of Lone Actor Events and Investigative Decision-Making from a Probabilistic Perspective....32**
  - **7. Monte Carlo Simulations....33**

IV. THE SUPERFORECASTING EXPERIMENT....43
- **A. SURVEY AND RESULTS....43**
- **B. SURVEY PART ONE—SCENARIOS....44**
  - **1. Survey Part One—Questions....45**

2. Survey Part One Data—Scoring the Results 45
3. Analysis of the Scenario Results 50
4. Differences between the Disciplines 51
5. The Fort Hood Exception 51
C. SURVEY PART TWO—PROSPECTS AND RISK ASSESSMENT SURVEY 53
1. Survey Part Two—Prospect Theory Questions 53
2. Survey Part Two—Results 54
3. Analysis of the Prospect Theory Responses 57

V. IMPLEMENTATION OF A SUPERFORECASTING NETWORK FOR DETECTING LONE ACTOR VIOLENCE: THE SUPERNETWORK 61
A. WISDOM OF THE CROWD VERSUS EXPERTISE 61
B. ENGAGEMENT OF COMMUNITY LEADERS 62
C. POTENTIAL HAZARDS OF THE SUPERNETWORK 63
D. CIVIL RIGHTS CONSIDERATIONS 63
E. HYPER-VIGILANCE, CONFIRMATION BIAS, AND THE CONTAGION OF PREJUDICE 65
F. CONSIDERING THE NET EFFECTS OF DEPLOYMENT 66

VI. CONCLUSION 67

APPENDIX A. IDEAS FOR FURTHER RESEARCH AND OPEN QUESTIONS 71

APPENDIX B. MODEL SELECTION AND HYPOTHESIS TESTING FOR THE TIME SERIES ANALYSIS AND MONTE CARLO MODELS 81

APPENDIX C. EXPERIMENT SURVEY QUESTIONS 95

LIST OF REFERENCES 105

INITIAL DISTRIBUTION LIST 109

LIST OF FIGURES

Figure 1. Frequency Comparisons of Simulated Casualty Rates from Random Numbers, Random Numbers that are Gamma Distributed, and Actual Casualty Rates.....84

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Runs Test on Lone Actor Attack Time Series 25

Table 2. Monte Carlo Simulation Results—Average over Five Iterations 37

Table 3. Professional Experience of Nine Participants in the Survey 43

Table 4. Brier Scores for All Scenarios 47

Table 5. Scenario 1 Results 47

Table 6. Scenario 2 Results 48

Table 7. Scenario 3 Results 48

Table 8. Scenario 4 Results 49

Table 9. Scenario 5 Results 49

Table 10. Prospect 1 Question and Results 54

Table 11. Prospect 2 Question and Results 55

Table 12. Prospect 3 Question and Results 55

Table 13. Prospect 4 Question and Results 56

Table 14. Prospect 5 Question and Results 56

Table 15. Prospect 6 Question and Results 57

Table 16. Lone Actor Attacks in the United States 85

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CLAT	Countering Lone Actor Terrorism Project
DHS	Department of Homeland Security
DOD	Department of Defense
FBI	Federal Bureau of Investigation
FIG	field intelligence group
JTTF	joint terrorism task force
NTAC	National Threat Assessment Center

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis examines investigative decision making, cognitive biases, talent sharing, and the relationship between the random nature of lone actor violence and a set of predefined decision-making protocols. Targeted violence presents a paradox for the homeland security enterprise. These single-attacker events, whether assassinations, school shootings, or lone-wolf terrorist attacks, are difficult to detect and interdict. In spite of the ephemeral nature of targeted violence, many of the most notorious incidents of targeted violence share a common characteristic: the attackers encountered, or were closely observed by, law enforcement before they attacked.

This thesis is predicated on the assumptions that: 1) in many cases of lone actor violence, the most confounding problem is not detection of the actor but the decision of what to do after the suspect is detected; 2) lone actor violence is a random event that does not follow a predictable pattern over time and space; 3) in spite of the frequency of pre-attack encounters between law enforcement and known lone actors, their actions do not meet the threshold for arrest before they attack; 4) given the other assumptions, when a decision to continue investigation is limited to a single organization, an agency, or task force, the likelihood for a successful outcome is as random as the attacks themselves.

To demonstrate the random nature of lone actor violence, this research uses twotime series statistical techniques. The results of the runs test and the time series analysis indicated that the emergence of these events was random over time and space. This analysis shows that these events are driven by a wide array of motives. These types of attacks are committed by a diverse group of perpetrators, who direct them at a dispersed number of targets. This statistical treatment of the attacks suggests that some detection tools may not be effective and buttresses the case that these events are random and independent.

To evaluate different decision-making protocols outside of the narratives of actual attacks, the researcher ran four separate simulations using the Monte Carlo technique. These simulations illustrate that with the dedication of additional investigative resources

comes a concomitant effect of diminishing returns, opportunity cost, and exposure to liability. The simulations also suggest that regardless of the single investigative agency's decision-making process, the outcome relies on the randomness of the event.

These findings suggest that randomness itself may contribute to the decisions investigators make. If an investigator seeks literal "hard" evidence that an attack will occur and does not find it, then there is little wisdom in investigating further if the ultimate goal is arrest, whereby due process obligates a high evidentiary standard. If the decision is framed by the outcomes of earlier investigations, then the lack of evidence can provide an immediate reason to end the investigation they are currently facing. The organizational imperatives of investigative agencies to produce arrests and the consequences of false positives may amplify one another, thus reducing the impetus to commit resources to a less compelling case. These outcomes of these simulations suggest the need for a more precise decision-making model than those used in the Monte Carlo simulations.

The statistical analysis and Monte Carlo simulations of lone actor violence may indicate that these attacks are unpredictable, but they may be detectable. Lacking a defined archetypical "profile" of an attacker renders the search for a definitive predictive model futile; however, identifying behaviors that may indicate a propensity toward violence makes detection of an attacker possible.

To demonstrate a prototype for a new method of threat analysis, a "superforecasting" team of multiorganizational and multidisciplinary analysts participated in an experimental survey. Nine participants reviewed five threat scenarios, and then assigned a score based on various factors such as potential for violence and immediacy of the threat.

Analysis by the experiment participants was highly predictive for three out of five scenarios and better than chance for a fourth scenario. The experiment was too small to claim that a *superforecasting* method is an improvement over single decision makers or investigative squads; however, the success of the analysis from this prototype was promising enough to consider a similar experiment on a larger scale.

The survey also measured participants' risk tolerances under uncertainty based on a prospect theory model. The participants answered six questions to detect risk aversion or risk seeking behavior and the "framing effect." The participants' responses were strongly consistent with prospect theory in some ways and less so in others; however, the pattern that emerged generally favors certain prospects to uncertain ones, despite the greater expected values of alternative choices. A parallel assessment of decision making through scenarios and hypothetical "prospects" presents a possibility for further research to determine the effects of risk tolerance on case study threat assessments.

The model simulations demonstrated that there will always be attacks that are true surprises and that proportion may be large enough to draw the conclusion that many or all lone actor attacks are undetectable. The prototype superforecasting experiment, together with the prospect theory results, may help to explain the relative strength of some certain threat assessments: The results distinguish what may be detectable from what is statistically unpredictable through the use of a collaborative and multidisciplinary method of analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis is dedicated to those who commit their lives to public service.

I am grateful for the support of my wife, Theoni, and my children, Alexi, Niko, Daphne, and Philip. They were supportive and patient, and offered ideas that found their way into the final draft. I am thankful for the encouragement, support, and confidence of my friends and colleagues in the United States Secret Service, who contributed in more ways than I can enumerate here. I am humbled to be a part of the Center for Homeland Defense and Security at the Naval Postgraduate School, which enabled me to synthesize the various experiences of my career and stretch my thinking in unexpected ways. Finally, I am proud to be a part of CHDS Cohorts 1601 and 1602—the members of which represent the very best in public service.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> Facts are stubborn things; and whatever may be our wishes, our inclinations, or the dictates of our passions, they cannot alter the state of facts and evidence.
>
> —John Adams

On November 5, 2009, a man entered a U.S. Army base in Fort Hood, Texas, and killed 13 soldiers. Soon thereafter, the facts about the attack became clear. The shooting was unprovoked, and the victims were unknown to the shooter. The shooter was a soldier, specifically a medical doctor who specialized in psychiatry. The shooter was named Nidal Hasan—an ethnic Palestinian, born in the United States, and a Muslim.

Within days, the image of Hasan came into sharper focus. Before the shooting, Hasan exhibited workplace behavior that concerned his colleagues. Some of this behavior could be characterized as professional negligence; on other occasions, he was increasingly vocal about his religion and his moral crisis over the prospect of serving in an Army that fought predominantly Muslim nations. Most damning to him, and eventually to the Federal Bureau of Investigation, was that Hassan communicated with a "notorious terrorist leader" about a year before the attack. The FBI was aware of the communication, identified Hasan as an Army major, and opened an investigation; however, the investigation closed months before the attack.[1]

After the attack, the public discourse reduced to a basic question: If the government was aware of Hasan's concerning behavior, then why did it fail to stop him? At about the time the information about Hasan's communications was revealed, a

[1] Senate Committee on Homeland Security and Governmental Affairs, *A Ticking Time Bomb: Counterterrorism Lessons from the US Government's Failure to Prevent the Fort Hood Attack* (Washington, DC: Senate Committee on Homeland Security and Governmental Affairs, 2011), https://www.hsgac.senate.gov/imo/media/doc/Fort_Hood/FortHoodReport.pdf, 39.

bipartisan Senate investigation began to examine what the Department of Defense and the FBI knew about Hasan, and why they failed to intervene in spite of that information.

From its inception, the leaders of the Senate investigation fell into now-familiar interpretations of the Hasan story. Chair Joseph Lieberman, a centrist Independent who caucused with the Democrats, felt that the attack indicated that the federal government failed to learn the lessons that the 9/11 Commission identified. Had government agencies shared information across all levels of law enforcement and empowered analysts, the Hasan case would have been resolved more favorably. Senator Susan Collins, a moderate Republican, voiced concern over the government's initial characterization of the attack as workplace violence, and she opined whether "political correctness" influenced the decisions of both the military and the FBI. This debate returned in the aftermath of subsequent attacks and was amplified in the 2016 presidential contest, wherein the Democratic candidate endorsed an "intelligence surge" to combat lone wolf terrorism, while her Republican opponent pointed to political correctness as a root cause for government's failure to do so.[2]

But facts truly are stubborn things, and as the primary sources of information reached the Senate investigative committee members, those facts did not fit neatly into their preconceptions. Lectures Hasan gave during his public health fellowship about Islam in the military did not depict him as a wild-eyed radical. In contrast, although colleagues may have disagreed with the premise of his presentation, but they did not appear outraged from by he said. His performance record during his medical internship indicated he was less the "ticking time bomb," as described in hindsight by his former supervisor, and more of a ticking malpractice suit.[3]

Yet one fact remained the most compelling; the investigation of Hasan came remarkably close to success. The military did not have cause to take significant action against Hasan, which would have disrupted his growing homicidal ideation, nor did the FBI have cause to arrest him. If these separate streams of information within Hasan's

[2] Nolan D. McCaskill, "Clinton Urges 'Intelligence Surge to Counter Terrorist Threat," *Politico*, June 13, 2016, https://www.politico.com/story/2016/06/hillary-clinton-national-security-224267.

[3] Senate Committee on Homeland Security and Governmental Affairs, *A Ticking Time Bomb,* 33–34.

military workplace and the FBI's investigation converged, the threshold for action may have been met.[4] If the totality of available information about Hasan's behavior was placed into one narrative, the Fort Hood attacks may have been prevented.

As a participant in the senate investigation, the question of why this narrative was not synthesized was most salient to me. My role within the investigation was as a staffer, so my questions in that role were often the same as those of the chair, ranking members of the committee, and my colleagues. As a practitioner of threat investigations, my questions were more elemental and circumspect. Was it fair to expect either Hasan's coworkers in the military or the FBI to recognize his behaviors as indicators of emerging violence? Was it fair to expect the FBI investigators to examine Hasan's behavior any further than they did, given their enormous workload?

These questions would reemerge with every subsequent lone actor attack. The Boston Marathon bombers, the Orlando night club shooter, and the White House fence jumper all encountered law enforcement before they attacked yet still were able to commit those attacks. As with Fort Hood, I wondered what information was available to the investigators who encountered these individuals, and how that information influenced the decision they made to close their investigations. The recurring problem appeared to be less about initial detection of the threat, and more about recognizing an individual as a threat.

If story of the Fort Hood is a story of bias in decision making, then the question remains what that bias may be. Law enforcement agencies may have an institutional propensity to close cases that do not present anything but the most compelling evidence. If this is true, the precursors to this bias may include aversion to "owning" the subsequent behavior of a suspect who, lacking any actionable evidence, could not be arrested yet may still commit a crime. Aversion to the risk of violating restrictions on investigative authority may dampen an investigative agency's interest in investigating subjects who have not broken the law. Investigative agencies are also faces with a resource-allocation dilemma and must triage investigative leads, thereby chasing the ones that are more fully

[4] Ibid., 7.

formed. Finally, organizational bias, or *groupthink*, may inculcate investigators with a rigid definition of what a threat is, thereby making them less sensitive to emerging threats that did not resemble that paradigm. The premise of this thesis is that a combination of cognitive and decision-making biases contribute to the missed opportunities to intervene before lone actor violence occurs. The research within this thesis explores a method to counter those biases.

II. THESIS PROPOSAL

A. PROBLEM STATEMENT

Targeted violence presents a paradox for the homeland security enterprise. These single-attacker events, whether assassinations, school shootings or lone wolf terrorist attacks, are difficult to detect and interdict. Lone actors do not respond to foreign command and control apparatuses, do not rely on elaborate support networks or detectable money trails, and often select targets that are difficult to anticipate and defend.

In spite of the ephemeral nature of targeted violence, many of the most notorious incidents of targeted violence share a common characteristic: the attackers encountered or were closely observed by law enforcement before they attacked. For instance, Nidal Hasan, the perpetrator of the 2009 Fort Hood shooting, was investigated by two FBI Joint Terrorism Task Forces before he attacked.[5] Omar Mateen was investigated twice by the FBI before he attacked the Pulse Nightclub in Orlando.[6] The Tsurneyev family was the subject of intelligence and law enforcement inquiries both abroad and in the United States before the 2011 Boston Marathon attacks.[7] Ahmad Khan Rahami, who was arrested for the 2016 New York and New Jersey bombings, was reported to the FBI by his father prior to the attacks.[8] Finally, in 2014, Omar Gonzalez was investigated by the U.S. Secret Service before he jumped the north fenceline of the White House.[9]

The police and federal investigators encountered the attackers because of actions the attackers took that indicated, in retrospect, they were in the midst of pre-attack

---

[5] Ibid., 35–40.

[6] Mark Mazzetti, Eric Lichtblau, and Alan Blinder, "Omar Mateen, Twice Scrutinized by F.B.I., Shows Threat of Lone Terrorists," *New York Times,* June 13, 2016.

[7] Scott Shane, Michael S. Schmidt, and Eric Schmitt, "Russia's Warning on Bombings Suspect Sets off a Debate," *New York Times,* April 25, 2013.

[8] Marc Santora and Adam Goldman, "Ahmad Khan Rahami Was Inspired by Bin Laden, Charges Say," *New York Times,* September 20, 2016.

[9] U.S. Department of Homeland Security, Office of the Inspector General, *2014 White House Fence Jumping Incident (Redacted)* (DHS-OIG Report OIG 16-64) (Washington, DC: U.S. Department of Homeland Security, Office of the Inspector General, 2016), https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-64-Apr16.pdf, 53.

behavior. Research by the National Threat Assessment Center (NTAC) of the U.S. Secret Service indicates that certain behaviors foreshadow targeted violence. A study of 12 years of attacks against government facilities and officials by NTAC found that about three quarters of the perpetrators had contact with the judicial system, an educational system, one or more employers, or law enforcement prior to their attacks.[10]

Why, given the concerns presented to investigators, have they repeatedly closed these cases? The answer may be found in the intersection between four fundamental components of the investigation: the investigator, the suspect, the investigative agency, and society itself. Characteristics of investigators, such as the methodologies they employ, their experience, and cognitive biases, may increase or reduce their propensity to investigate a lead further. Characteristics of suspects, particularly the behaviors they exhibit and the ones that are not obvious to investigators, will also affect the propensity to investigate. Finally, the imperatives of an investigative agency, the way it arrays it resources to counter a threat, and the methodologies it uses will influence the decision to move and investigation forward or not.

Society provides the policies, laws, and social norms in which the other three components anchor their decision making. The investigators assess the behavior of a suspect relative to the baseline behaviors of the community. The actions the investigators take are also bound to the public's expectations for safety on one end and the restrictions of police power on the other. As members of a community, the attackers may select their targets and the method of attack based on societal influences, even when the purpose of the attack is only apparent to the attackers themselves. An investigative agency is strongly influenced by society in the resources it receives to fulfill its mission, and it shapes and prioritizes aspects of that mission based on what matters most to society, using only those powers society deems appropriate.

These four components represent separate forces, which like vectors, may align and amplify one another toward an obvious decision, or they may align in a countervailing manner, wherein the appropriate decision is less apparent. Exploring all of

[10] National Threat Assessment Center, *Attacks on Federal Government 2001–2013: Threat Assessment Considerations* (Washington, DC: United States Secret Service, 2015), 2.

these aspects comprehensively is beyond the scope of a single thesis; however, they must all be considered when examining what is often the most critical decision in an investigation—whether to carry the case further. That decision is the watershed of those separate forces; therefore, the question of how that decision is made and how that decision can be improved forms the basis of this thesis.

This thesis tests whether a new method of threat analysis, using a "superforecasting" method engaging a diverse group of analysts, will produce an accurate assessment of targeted violence. Crowdsourcing analysis would take individual threat assessments, distill them into a brief synopsis, and send the synopsis to a large number of vetted analysts. Those analysts could include local and federal investigators, intelligence analysts, social scientists, teachers, health care professionals, faith leaders, and any other field that may have a nexus into targeted violence investigations. These analysts would assign each brief a score based on various factors, such as potential for violence and immediacy of the threat. These analyses would then be aggregated, and a combined score would assist case management decisions, such as whether to close a case or investigate a threat further.

This thesis is an examination of decision-making, cognitive biases, and the relationship between organizational form and function. This new approach is intended to stimulate interagency and multidisciplinary cooperation through a less centralized, networked environment. The end goal of this method is an evolution of information sharing into talent sharing.

B. RESEARCH QUESTIONS

The primary question of this thesis is whether a "superforecasting" team of multi-organizational and multidisciplinary analysts, produce more accurate and predictive analysis of potential lone actor threats than analysis from a single organization? A team of superforecasters, who are loosely networked in a way that transcended organizational boundaries and distributed across a broad cross-section of society, may better detect the ephemeral threats that lone actors present. An experiment that simulates this technique will indicate whether the superforecasting method is effective for detecting lone actors.

An additional question this thesis explores is if the repeating pattern wherein perpetrators of targeted violence are investigated by law enforcement, but are left to commit their attacks, a consequence of organizational and methodological inadequacies? In spite of the trend in law enforcement and intelligence to form multiagency task forces, the work of an individual case is often conducted by a very small number of investigators. One example is the investigation of Nidal Hasan by the FBI in 2008 and 2009 before he attacked in Fort Hood, Texas. This case was investigated by two FBI joint terrorism task forces (JTTFs), which are comprised of investigators and analysts from a wide array of agencies; however, the case itself was investigated in depth by only three people—an analyst and an FBI agent in one JTTF and Defense Criminal Investigative Service agent who was detailed to a second JTTF. In spite of their initial success in identifying Hasan, they did not extend their inquiry beyond the confines of the JTTFs, thereby missing an opportunity to put Hasan's radicalization into context.[11]

C. LITERATURE REVIEW

The detection of single actor and small group attacks is inherently challenging to investigative agencies. It must be acknowledged that single actor attacks are a very small phenomenon in comparison to other criminal trends. The problem of identifying potential targeted violence and intervening appropriately can be found in recent statistics. However, different researchers have yielded different tallies of these attacks. For example, a PBS *Frontline* report stated that there were 115 single-actor, or "lone wolf," attacks in the United States between 1940 and 2016. [12] A report by the FBI and Texas State University counted 160 active shooter incidents between 2000 and 2013, which killed 486, and wounded 557. The data used later in this thesis counted 190 lone actor attacks between 1982 and 2017, and three additional attacks occurred in the month since that analysis concluded. Regardless of which method is used, when compared to the

[11] Senate Committee on Homeland Security and Governmental Affairs, *A Ticking Time Bomb*, 35–39.

[12] Katie Worth, "Lone Wolf Attacks Are Becoming More Common—And More Deadly" *Frontline*, July 14, 2016, http://www.pbs.org/wgbh/frontline/article/lone wolf-attacks-are-becoming-more-common-and-more-deadly/.

number of murders in the United States in 2015, 15,696 in total, it can be asserted that acts of targeted violence are rare, and the total casualties are relatively small.[13]

According to the FBI-Texas State study, all but two of the targeted attacks involved a single shooter.[14] The 20 deadliest attacks since September 11, 2001 were perpetrated by individual actors or small groups. Seventeen involved an individual or pair of attackers using firearms, and the remaining three used vehicles, explosives, or biological weapons against their targets.[15]

The statistics indicate that targeted violence may be "black swan" events, which Nassim Taleb defines as an event that is an outlier, carries extreme impact, and that human nature is compelled to explain after the fact.[16] The October 2017 Las Vegas shooting, resulting in 58 deaths and the injury of many others, exemplifies this definition. The attack emerged without any apparent foreshadowing, and the nation that bore witness to the attack struggled to explain the meaning of the crime. To date, the killer's motives for attacking remain unknown and stand in relief to the many other details since revealed about him.

In a critical examination of the performance of investigators, it is also important to consider Taleb's thought experiment in *The Black Swan*, which contemplates an alternate reality wherein a legislator successfully passes a law mandating locked cockpit doors just before the September 11, 2001 attacks. Taleb contends that if this law had passed, and the 9/11 attacks were thwarted, the legislator would likely go unheralded. This is what Taleb describes as "Black Swan blindness," wherein successes go unheralded, and conversely, failures after a significant event are salient.[17]

---

[13] "Latest Crime Statistics Released," Federal Bureau of Investigation, September 26, 2016, https://www.fbi.gov/news/stories/latest-crime-statistics-released.

[14] J. Pete Blair and Katherine W. Schweit, *A Study of Active Shooter Incidents, 2000—2013* (Washington DC: Texas State University and Federal Bureau of Investigation, 2014), https://www.fbi.gov/file-repository/active-shooter-study-2000-2013-1.pdf, 6–7.

[15] Global Terrorism Database (queried using Country: United States / Time 2001—2016), accessed June 27, 2017, https://www.start.umd.edu/gtd.

[16] Nassim Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2007), xvii–xviii.

[17] Ibid., xxiii.

In their defense, law enforcement leaders often posit an argument similar to Taleb's and buttress it arguing, that given the facts that were presented to them, they did not have cause to arrest, much less prosecute. However, the idea that arrest is the only resolution for these cases may be part of the problem. In these cases, police and federal investigators encountered the attackers because they were engaged in pre-attack behavior, which if properly analyzed, could have prompted interventions short of arrest, but still preventative in nature.

Research indicates that certain concerning behaviors foreshadow targeted violence. The NTAC's study of 12 years of attacks against government facilities and officials found that about three quarters of the perpetrators had contact with the judicial system, an educational system, one or more employers, or law enforcement.[18]

1. Current Organizational Models Struggle to Detect Lone Actor Violence

Beginning in the late twentieth century, faced with threats that were increasingly multijurisdictional and networked, law enforcement and intelligence agencies countered with the development of task forces. Task forces represented a significant organizational innovation in a profession where organizations were traditionally insular and guarded information jealously. There is little available literature analyzing the performance of investigative task forces. This deficit may be from the difficulty of researchers to access and observe task forces or a general sense that these groups, as the best representation of the multiagency and multitiered solutions that were envisioned after the 9/11 terrorist attacks, are unimpeachable. It remains that task forces have not been subjected to the same scrutiny that their controlling agencies have.

Given the deficit of research, an examination of task forces must begin with research and oversight reports of their parent agencies and then continue with research and theory into the decision making of small groups. The study of decision making, organizations and social network analysis provides a framework to venture into an

[18] National Threat Assessment Center, *Attacks on Federal Government*, 2.

examination of task forces, and research an alternative design that may better serve threat analysis.

Examining the performance of task forces and fusion centers has been limited to congressional committees and the agencies themselves. Although not academic, each has its advantages and disadvantages. Congressional reports may be skewed or amplified from political agendas, but the investigative mandate of Congress provides exceptional access to data in this secretive field. Agencies always trumpet their programs, but much can be deduced from what an agency emphasizes and what it does not. In *Spying Blind*, Amy Zegart examines organizational problems within the homeland security enterprise; however, even she dedicated an entire chapter, titled "Crossing an Academic No-Man's Land,"[19] to the scarcity of existing research on agency adaptation failure.

Zegart crosses this no-man's land by blending organizational theory and political science to assess why intelligence agencies could not adapt to the changing threats they faced before 9/11, and why were resistant to change in spite of the imperatives of post-9/11 reforms. Her argument is that the nature of organizations, self-interest of political officials, and the fragmented nature of the federal government all militate against reform.[20]

The premise that cultural and bureaucratic barriers between intelligence and investigative agencies were two precursors of the failures of imagination before 9/11 has been evinced by many studies in Congress, academia, and the press. Most convincingly, the eleventh chapter of the *9/11 Commission Report* details examples of how "institutionalizing imagination" could have synthesized the disparate leads and strings of available data that may have revealed the 9/11 plot.[21]

Congress responded to these findings with a massive reorganization of government that yielded the Department of Homeland Security (DHS), the Office of the

---

[19] Amy Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton, NJ: Princeton University Press, 2007), 43.

[20] Ibid., 9.

[21] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: National Commission on Terrorist Attacks upon the United States, 2004).

Director of National Intelligence, and a FBI that quadrupled the number of multiagency JTTFs under its supervision.[22]

Advocates of these changes credit the recast *homeland security enterprise*, which realigned agencies under these new organizational structures and emphasized information sharing, for the absence of a large-scale terrorist attack within the United States since 2001. Critics have cited the recent emergence of homegrown terror and a concomitant failure of the homeland security enterprise to thwart these lone wolf attacks, as indicators that even these reorganized entities remain one step behind contemporary threats.

A 2011 U.S. Senate report took direct aim at the FBI's JTTFs for their inability to disrupt the terrorist attack at Fort Hood Army base in Texas. The committee's account of the FBI's "superficial inquiry" of the attacker, Nidal Hassan, recommended that the FBI accelerate its transformation into an intelligence-driven agency, integrate its field offices, fully utilize intelligence analysts, update its tradecraft, and that JTTFs ultimately "fulfill the FBI's aspiration for them to become interagency information-sharing and operational coordination mechanisms."[23]

Critical to the Fort Hood failure was that in spite of the colocation of investigators and analysts within the JTTFs, interagency divisions persisted. Non-FBI participants in the JTTFs were prohibited complete access to critical databases and essential training, nor could they share information with their parent organizations. In essence, the JTTFs were acting as "appendages of the FBI."[24]

Criticism of the JTTFs has persisted after Fort Hood. For instance, a RAND report of a 2014 seminar on domestic intelligence collation and information sharing observed that JTTFs are the primary conduit for intelligence to move from local to federal law enforcement; however, intelligence did not flow in the opposite direction.[25]

---

[22] "Joint Terrorism Task Forces," Federal Bureau of Investigation, accessed October 15, 2016, https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces.

[23] Senate Committee on Homeland Security and Governmental Affairs, *A Ticking Time Bomb*, 45.

[24] Ibid., 74.

[25] Brian Michael Jenkins, Andrew Liepman, and Henry H. Willis, *Identifying Enemies among Us: Evolving Threats and the Continuing Challenges of Domestic Intelligence* (Santa Monica, CA: RAND Corporation, 2014), 9–10.

In spite of this, the report acknowledged that the JTTF system works, albeit imperfectly, and remains the primary conduit between federal and local law enforcement.[26]

Fusion centers have been an alternative conduit between federal agencies and their state and local counterparts to share and collectively analyze information. These centers, and their mission, are often confused with JTTFs. This confusion, and sometimes criticism, is frequent enough that DHS posts a webpage that carefully distinguishes the respective missions and characteristics and missions of fusion centers and the JTTFs.[27] According to DHS, the fundamental distinction between them is that fusion centers are vigilant concerning all-hazards, including terrorism, while JTTFs focus on counterterrorism exclusively.

In a separate but closely linked website, DHS also distinguishes between fusion centers and FBI-led field intelligence groups (FIGs).[28] Here too, DHS contrasts the all-hazard posture of fusion centers against the FIGs' purpose of supporting all FBI investigative efforts. The distinctions within these websites are clear, as it is on three other DHS websites that distinguish the purpose of fusion centers from other federal-local partnerships.[29] However, the effort these websites make to distinguish these groups also begs the question, does DHS protest too much?

A 2012 report from the Senate Permanent Subcommittee on Investigations appears to think so. The report painstakingly details deficiencies of fusion centers, describing outdated and uninformative reporting, a muddled chain-of-command structure,

---

[26] Ibid.

[27] "Fusion Centers and Joint Terrorism Task Forces," U.S. Department of Homeland Security, accessed October 15, 2016, https://www.dhs.gov/fusion-centers-and-joint-terrorism-task-forces.

[28] Ibid.

[29] "FBI Field Intelligence Groups and Fusion Centers," U.S. Department of Homeland Security, accessed December 1, 2016, https://www.dhs.gov/building-law-enforcement-and-homeland-security-partnerships.

and wasteful spending. The final chapter of the report goes so far as to consider that fusion centers may have hindered, rather than aided, federal counterterrorism efforts.[30]

Senate Permanent Subcommittee on Investigations certainly had a political axe to grind; subcommittee ranking-member, Republican Tom Coburn, proudly carried the moniker "Dr. No" for his reputation as a fiscal "hawk" who paid particular attention to duplicative and inefficient federal programs. Furthermore, the report itself admits that it focused on the utility of fusion centers to the federal government and counterterrorism and that it did not examine the utility of the centers to state and locals nor their ability to analyze other types of threats.[31] Yet the report is another indication that in spite of intentions, multiagency task forces and fusion centers are imperfect mechanisms for producing coordinated threat analysis.

2. Alternative Organizational Models and Methodologies to Detect Targeted Violence

The examinations such as those by Zegart, Congress, and watchdog groups are helpful, but they tend to direct their focus toward agencies, while this thesis looks at the more discrete behavior within those agencies. The actions of agencies and policymakers certainly influence the decision making of investigators, but the story seems incomplete. What is deduced from the available evidence is that task forces and fusion centers are top-down constructs seeking to have their participants conform to a rigid framework. It is that imposed design that causes these entities, which are intended to transcend bureaucratic fault lines, to act like bureaucracies themselves.

Social network analysis (SNA) speaks to the weakness of the top-down, centrally-controlled design of collaboration vice *autonomy* in which independent actors volunteer to come together. Ted Lewis writes that autonomy leads to *bottom-up evolution*, in which

---

[30] Senate Permanent Subcommittee on Investigations, *Federal Support for and Involvement in State and Local Fusion Centers—Majority and Minority Staff Report* (Washington, DC: Senate Permanent Subcommittee on Investigations, 2012), https://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers, 101–104.

[31] Ibid., 9.

networks grow and evolve based on local rules.[32] SNA is a promising method to evaluate both the vulnerability of single-agency and task force approaches to threat analysis and the potential of an emergent system that evaluates threats over a multiplicity of evaluators. Lewis writes that with networks, function follows form. This means that real-world phenomena behave the way they do because of their network structure.[33]

SNA also speaks to the value of a widely distributed and loosely -connected network of analysts as an alternative to the regimented design of the investigative squad, field office, or task force. Mark Granovetter researched social networks and emphasized the importance of those on the periphery of a network, which he called "weak ties" to adhere disparate, tightly-bound groups into a broad community.[34] Paradoxically, strong social ties within groups may inhibit community organization; when groups become tightly bound at the expense of weaker social ties, the community organizes into unaligned cliques.[35]

Granovetter considers earlier research examining whether innovators are generally marginal within a social network. In comparison to those who are more central and strongly linked to the group, those on the margins are less bound by convention.[36] Granovetter is equivocal about this question; however, more recent research takes this argument a step further. In combining the mathematics of networks and methodologies applied to linguistics, researchers Vittorio Loretto et al. theorize that the potential for innovation is more likely when ideas are arrayed in a networked structure. The authors apply the concept from biology of the *adjacent possible* to explain how unanticipated knowledge can emerge from centrality in a network of known evidence.[37]

---

[32] Ted G. Lewis, *Network Science: Theory and Practice* (Hoboken, NJ: John Wiley & Sons, 2009), 1-244, 299–430.

[33] Ibid., 9.

[34] Mark Granovetter, "The Strength of Weak Ties," *American Journal of Sociology* 78, no. 6 (1973): 1364–1366, https://doi.org/10.1086/225469.

[35] Ibid., 1373–1374.

[36] Ibid., 1367–1368.

[37] Vittorio Loreto et al., "Dynamics of Expanding Spaces: Modelling the Emergence of Novelties," in *Creativity and Universality in Language*, Lecture Notes in Morphogenesis Series, ed. Mirko Degli Esposti, Eduardo G. Altmann, and François Pachet, 59–83 (Cham, Switzerland: Springer International, 2016).

In a more narrative sense, in *Change by Design*, Tim Brown describes how the emergence of an idea, or in this case good decision making, is encouraged through effective organizational design. In describing the concept of design thinking, Brown points out that a self-propagating idea changes behavior, perceptions, and attitudes; however, he also recognizes that this approach militates against top-down authority and centralized administration.[38] In approaching an investigation as a type of innovation, wherein the unanticipated is revealed through the networked propagation of ideas, it is not difficult to imagine how threat analysis may benefit from a more distributed and networked approach.

Other academic treatments of SNA observe how information can spread through a network like a contagion; this is what marketers call "going viral." The homeland security enterprise was purposely built to facilitate information sharing; however, the deleterious effects of networked information need to be considered. Nicholas Christakis and James Fowler present the ominous observation that "the wisdom of crowds can quickly turn to folly."[39] Recent media coverage of "fake news" and the influence of social media on the 2016 presidential election may reinforce this point. If a certain network may produce better analysis, that same network under different conditions may reinforce or amplify falsehoods or bias.

A method designed by Philip Tetlock, Dan Gardner and the Good Judgement Project may provide a way to balance broader strategic goals organizational imperatives. In *Superforecasting: The Art and Science of Prediction* and its underlying research, Tetlock and Gardner found that dispersed teams of untrained, nonprofessionals could predict the outcomes of strategic-level questions better than colocated and cohesive

[38] Tim Brown, *Change by Design: How Design Thinking Transforms Organizations and Inspires Innovation* (New York: Harper Collins, 2009), 138.

[39] Nicholas A. Christakis and James H. Fowler, *Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives* (New York: Little Brown and Co., 2009), 140.

professional analysts.[40] Amateur forecasters who used this method outperformed professional intelligence analysts by 30 percent.[41]

The competition described in *Superforecasting* may point to the wisdom of crowds unto itself as a reason for the superior analysis of the amateur forecasters. These teams were comprised of talented individuals in their own fields, and it is possible that their collective knowledge eclipsed that of the agency-sponsored subject matter experts. Also, the networked structure of these teams may extend to sources of information that were more predictive than the classified information the agency teams used. The authors suspect that other forces also contributed to this success. Referencing the works of Amos Tversky and Daniel Kahneman on availability heuristics, the *Superforecasting* authors argue that the agglomeration of intelligence in a particular field does not necessarily contribute to accurate prediction.[42]

Superforecasting also refers to the seminal work on groupthink by Irving Janis to contemplate the vulnerability of small groups. Janis states, "members of any small cohesive group tend to maintain esprit de corps by unconsciously developing a number of shared illusions and related norms that interfere with critical thinking and reality testing."[43] This tendency for what Janis calls "concurrence seeking behavior" in groups may explain the susceptibility of task forces to poor decision making.[44] Without deliberate steps to counter it, such as predesigned dissent and debate and the introduction of outside opinion, cohesive groups will fall into the trap of groupthink. In this sense, Janis echoes the insights of Granovetter in his examination of social networks, but he sees a more insidious consequence from a group that eschews outside influences. According to Janis,

---

[40] Philip Tetlock and Dan Gardner, *Superforecasting: The Art and Science of Prediction* (New York: Crown, 2016), 94–99.

[41] David Ignatius, "More Chatter Than Needed," *Washington Post*, November 1, 2013.

[42] Tetlock and Gardner, *Superforecasting,* 51–52, 109.

[43] Irving Janis, *Victims of Groupthink: A Psychological Study of Foreign-Policy Decisions and Fiascoes* (Boston: Houghton Mifflin, 1972), 20, quoted in Philip Tetlock and Dan Gardner, *Superforecasting: The Art and Science of Prediction* (New York: Crown, 2016), 196.

[44] Tetlock and Gardner, *Superforecasting*, 9.

> Groupthink refers to a deterioration of mental efficiency, reality testing, and moral judgment that results from in-group pressures. . .[The consequences of bad decision making from groupthink] deserved to be fiascoes because of the grossly inadequate way the policymakers carried out decision-making tasks.[45]

Task forces, by name and design, assemble subject matter experts together to address a specific challenge, but the insights of Janis, Tversky and Kahneman, and their intellectual progeny—Tetlock and Gardner—indicate that the deep expertise of task forces makes them less able to adapt when their intended task changes. A networked approach may favor better threat analysis, but it also signals a break from recommendations of Zegart and the Senate's Fort Hood report to centralize the FBI. This illuminates the paradox of teams and centralized control—they can amass an array of talents, but they can also impose consensus to the point where the benefits from that diversity of thought are eclipsed by central control. Where the appropriate balance lies goes to the heart of this research.

This thesis tests the accuracy of superforecasting with threat analysis. It examines whether a networked method, which in *Superforecasting* trained the collective analysis of the crowd toward large-scale longitudinal questions, will be effective when applied to situations that are ephemeral and immediate.

D. RESEARCH DESIGN

This thesis examines whether a networked "crowdsourcing" method of threat analysis produces a more complete and accurate assessment of targeted violence suspects than current methods that are compartmentalized within a single organization. Crowdsourcing analysis would take individual threat assessments, then distill that assessment into a very brief synopsis, which would be sent to a large number of vetted analysts. These analysts could be local and federal investigators, intelligence analysts, social scientists, teachers, health care professionals, and any other field that may have a nexus into targeted violence investigations. If the results of this technique are similar to

[45] Ibid., 9–10.

those described in *Superforecasting*,[46] the diversity of the analytical group and their strength in numbers would analyze threat cases with improved fidelity compared to a single-agency method.

In superforecasting competitions, analysts and amateur teams registered probabilities that hypothetical scenarios would occur within the span of the competition. These probabilities were then scored not only on their binary accuracy (i.e., it happened or it did not) but on their precision. This meant that a forecaster who gave a 75 percent probability for an event that ultimately occurred would receive a higher score than somebody who gave that outcome a 60 percent probability. Conversely, if the event did not occur, the forecaster who predicted 75 percent in favor would endure a larger penalty than the forecaster who predicted 60 percent.[47]

This competition could be replicated for the thesis using past cases of targeted violence. Information for most of these cases is publically available through agency case studies, and databases such as the National Consortium for the Study of Terrorism and Responses to Terrorism's Global Terrorism Database. Additional descriptive data may be found through the NTAC. Research subjects could then analyze these cases studies and score them.

1. Limits

The scope of this thesis was to test the hypothesis that a superforecasting methodology will produce more thorough, accurate, and predictive analysis than that of a single organization. The research was framed by the assumption that lone actor violence detectable and actionable, even when the subject of an investigation has not yet violated the law.

A second assumption was that missed opportunities to stop acts of violence were the result of inherent institutional and cognitive vulnerabilities. These failures were not the consequence of inadequate information about the subject or individual failings of an

[46] Ibid.

[47] Ibid., 92–93.

investigator, rather, they were the consequence of detecting a randomly occurring and complex event with a single organization, Whether the organization was an agency or task force, the critical decision to investigate further was limited to a single entity, thereby creating a single point of failure. To address this single point of failure, the researcher assumed that a broadly networked array of agencies and organizations, which engages a multiplicity of talents and perspectives, would produce better analysis and intervention strategies than the current single agency and task force models.

2. Data Sources

Data for the statistical analysis of lone actor attacks and an experimental superforecasting survey derived from unclassified, publically available case studies, the START Global Terrorism Database, and news accounts of targeted violence incidents. I then distilled the cases into synopses that form the bases for data collection. Analysts then analyzed and scored the synopses.

3. Type and Mode of Analysis

The thesis analyzed data through quantitative analysis of past lone actor events, a Monte Carlo simulation, and a survey simulating the superforecasting methodology. The quantitative analysis detected any patterns in the time series data, or in the absence of such patterns, established the randomness of lone actor attacks. The Monte Carlo simulations tested different decision-making protocols against a randomly occurring series of events.

In addition to the quantitative analysis of attack data, this research also includes an experimental survey. The survey evaluated the superforecasting methodology through the analysis of scores participants gave to threat synopses. A Brier score evaluated the precision of participant scoring of the survey threat scenarios. This score enabled a test of the hypothesis that the networked interagency analysts produce results that are significantly different than the investigative agencies or chance. Additional questions within the survey produced output that illustrated how analysts reached decisions, what within the scenarios interested them, and why. In this sense, it presents an opportunity to analyze the analysts.

III. BACKGROUND

A. DEFINITION OF LONE ACTOR VIOLENCE

Defining of lone actor violence is a challenging task for the researcher and practitioner alike. Conflating acts such as "lone wolf terrorist," "mass shooter," and "assassin" may risk a disregard of the different tactics, targets, and motives of these attacks. However, to consider each too distinctly may draw the boundaries too close, thereby leading practitioners to disregard concerning precursors that do not conform to their definition, or a legal and jurisdictional one, of who is a terrorist, a mass shooter, or an assassin. To make such distinctions ignores some commonalities that may be shared across these different acts, regardless of the stated motive of the attacker.

This debate continues among policymakers and the public. In the case of Nidal Hassan, in many ways the prototypical American lone-wolf terrorist, this question was the topic of fierce debate within Congress and between Congress and the Executive Branch. Some policymakers and pundits characterized Hassan's attack at Fort Hood as workplace violence, a case of "going postal" with an Islamist veneer, while others impugned the workplace violence characterization as "political correctness" and extended that argument to imply that by not characterizing Hassan's behavior properly, his colleagues and investigators failed to recognize an emerging terrorist in their midst.

This debate may have been a distinction without a difference: Hassan behaved in a manner concerning to his colleagues and communicated with a known terrorist. These behaviors alone should have elicited curiosity from either his colleagues or investigators, as they were unusual for an Army officer. For his colleagues to frame his behavior as: "are these things which should warrant discipline?" or for investigators to frame it as: "are these things that indicate he is a terrorist?" prohibited either from recognizing that Hassan was rapidly becoming untethered from his life and may have been on the path to commit violence.

The debate over the label of "terrorist" in the context of lone actors also illustrates the hazard of reverse causation. With Hassan and subsequent attackers proclaiming an

affiliation with a terrorist group, there is an associated assumption that those groups assisted, or at least encouraged, the attacker; however, evidence of such encouragement is sparse in American lone wolves. Instead, these appear to be actors who develop an urge to kill first and then seek a purpose for the killing afterwards.

Similar debates have followed attempted and successful presidential assassinations. Although the story of the first presidential assassin, John Wilkes Booth, positions him as the center of a wider Confederate conspiracy, and James Garfield's assassin, Charles Guiteau, is assumed to have been mentally ill, the motives of the two twentieth century assassins are less clear. William McKinley's assassin Leon Czolgosz is consistently described as an anarchist, and he also had a history of mental illness.[48] The killing of Lee Harvey Oswald two days after he assassinated John F. Kennedy destroyed any possibility of hearing his account for his motives; however, his avowed belief in Marxism and the meandering path of his life produced ample material for countless theories that try to ascribe a conspiratorial motive for the assassination.

The attribution of "domestic terrorists" to a larger movement is less strong. The motives of school shooters are even less so, possibly by nature of their youth. However, the description of the motives attributed to many of the more notorious actors in both groups often alludes to philosophy that is often framed as the cause, rather than a consequence, of their pathos.

Considered in their entirety, lone wolf terrorists, assassins, domestic terrorists, and school shooters share common characteristics in their respective paths to violence; it is their ascribed motive of the attack that distinguishes them. These commonalities form the basis of the definition, used by this thesis, which derives from the NTAC's study of targeted violence, "Targeted violence is an incident of violence where a known or knowable attacker selects a particular target prior to their violent attack."[49]

---

[48] "Leon Czogolsz and the Trial," University of Buffalo, accessed September 27, 2017, http://library.buffalo.edu/pan-am/exposition/law/czolgosz/#who.

[49] Robert Fein, Bryan Vossekuil, and Gwen A. Holden, "Threat Assessment: An Approach to Prevent Targeted Violence," *Research in Action*, NCJ 155000 (July 1995), https://www.ncjrs.gov/pdffiles/threat.pdf.

For the purposes of this analysis, this definition is expanded and defined in the following way:

- **The actor attacked in a targeted manner**. In accordance with the NTAC definition, the attack was not sudden nor was it impulsive.[50]
- **The attack involved one or a few actors and was not directed or supported by an outside group**. Although the literal use of "lone actor" may be inaccurate, the term is kept to remain consistent with the literature and for the sake of concision.
- **The actor was detectable**. The actor encountered law enforcement or another institution before the attack or was reported by a close associate before the attack.

B. LONE ATTACKERS AND "ATTACK RELATED BEHAVIOR"—THE DIFFERENCE BETWEEN THE UNPREDICTABLE AND THE UNDETECTABLE

An observer may perceive that single-actor violence is random, and an examination of related data may support that perception; however, it is important to distinguish between what is unpredictable and undetectable. The random nature of time series data on lone actor events analyzed in this chapter implies that these events are statistically independent, which means that the occurrence of an event is not the consequence of similar events that preceded it. In the context of lone actor investigations, this implies that the essential questions of who, where, and when cannot be extrapolated from earlier events attacks.

Undetectable is a separate and distinct condition that is more forbidding for an investigator than the predictable. The next attack may not derive (in a statistical sense, at least) from earlier attacks; however, there may be common characteristics of past attacks and attacker that foretell the next one.

---

[50] Robert Fein and Bryan Vossekuil, *Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials* (Washington: National Institute for Justice, 2000), https://www.ncjrs.gov/pdffiles1/nij/179981.pdf, 16.

C. STATISTICAL ANALYSIS OF LONE ACTOR VIOLENCE IN THE UNITED STATES—THE IMPOSSIBLE TASK OF PREDICTING RANDOMNESS

It may be argued that lone actor violence is random. To affirm the random character of lone actor violence, this thesis reviews and tests data on these attacks. The source of the data was the Global Terrorism Database, which is compiled by the National Consortium for the Study of Terrorism and Responses to Terrorism (START).[51] This data included attacks that involved three or fewer perpetrators and occurred in the United States between 1982–2017. An additional data set was compiled by *Mother Jones* magazine and then hand-filtered to exclude duplicates or events that were committed by groups. This combined set accounted for 190 incidents over 13030 days.[52]

1. Using a "Runs Test" to Determine a Temporal Pattern in Lone Actor Attacks

Once collected, the next step was to analyze the lone wolf data a statistical technique called the "runs test." The runs test reviews a series of events with two distinct outcomes over time and determines whether that series exhibits a pattern.[53] Any consecutive sequence where the same event occurs is considered a "run." For example, if a fair coin was tossed five times, resulting in HHHTT, there would be two runs. The first run is three sequential flips of heads; the second is two sequential flips of tails. The total numbers of runs for either event is then counted, as is the number of individual times the either event occurred at all. Using these numbers one can determine a mean and variance and run a statistical "Z" test against the null hypothesis that the sample mean is not significantly different from the mean of a times series that is random.[54] If the Z score is

---

[51] National Consortium for the Study of Terrorism and Responses to Terrorism, Global Terrorism Database [Data file], accessed November 5, 2017, https://www.start.umd.edu/gtd.

[52] Mark Follman, Gavin Aronsen, and Deanna Pan, *Mother Jones*, November 15, 2017, http://www.motherjones.com/politics/2012/12/mass-shootings-mother-jones-full-data/.

[53] National Institute of Standards and Technology, "Runs Test for Detecting Non-Randomness," in *Engineering Statistics Handbook* [online], last updated October 30, 2013, http://www.itl.nist.gov/div898/handbook/eda/section3/eda35d.htm.

[54] A Z score test is described in "Hypothesis Testing," Pennsylvania State University, accessed October 15, 2017, http://sites.stat.psu.edu/~ajw13/stat200_notes/09_hypoth/03_hypoth_proportion.htm.

sufficiently far from the mean (this is ± 1.96 at the 95 percent confidence level) then the null hypothesis (H_o) is rejected.

Table 1. Runs Test on Lone Actor Attack Time Series

Runs Test for Daily Attacks 1/28/1982—10/1/2017

Runs			
n+ (incident)	189	mean	373.5175
n- (no incident)	12,842	var	10.6214
Runs (incident)	180	Z score=	-1.36682
Runs (no incident)	179	Accept H_o	

The Z score of the test in Table 1 is within the confidence interval of ± 1.96, which suggests the null hypothesis is acceptable. By extension, this result supports that the onset of lone actor attacks within the tested time series follows a random pattern. This indicates that lone actors' attacks are unlikely to follow a pattern that is predictable through quantitative analysis, and they are likely independent events.

2. Time Series and Geospatial Analysis of Incidents over Time and Space

Time series analysis determined whether there were any correlations between an incident and a period up to 365 days in the past. The result confirmed there was no statistically significant correlation between any day and a day 1 to 365 days prior. (See Appendix B for this analysis). This indicates that it is highly unlikely that a lone wolf attack has a statistical relationship with previous attacks within a year-long span.

A similar analysis of the locations of events between 2013 and 2016 was the only span for which a complete data set on latitude and longitude of the events was available. As with the analysis of incidents over time, there was no statistical correlation on the latitudinal and longitudinal series. This indicates that the location of an attack does not predict the location of later attacks within this time frame.

Considered together, the results of the runs test and the time series analysis indicates that lone wolf attacks between 1982 and 2017 were random over both time and

space. It is likely that one could intuit this argument without the use of statistical techniques. A cursory review of lone actor events shows that these events are driven by a wide array of motives, committed by a diverse group of perpetrators, and directed toward a dispersed number of targets. However, it is useful to attempt statistical treatment of the attacks, albeit simple ones, to eliminate potential detection tools and to buttress the case that these events are random and independent.

3. Is Lone Actor Violence Detectable?

In 1997, the United States Secret Service and the National Institute of Justice studied the histories of 83 people known to have attacked, or approached with intent to attack, a prominent person of public status in the United States from as early as 1949.[55] This Exceptional Case Study Project examined the traditional profile-based approach to these incidents and refuted that approach; however, the project asserted that assassination was the "end result of a discernable process of thinking and behavior."[56] In a subsequent report, Fein and Vosskuil explain that

> There are no accurate—or useful—descriptive, demographic, or psychological "profiles" of American assassins, attackers, and near-lethal approachers. …[The attackers studied] were both male and female, and ranged across ages, educational backgrounds, employment histories, marital status, and other demographic and background characteristics.[57]

This distinction encapsulates the difference between a phenomenon that is unpredictable and one that is undetectable. Lacking a defined archetypical "profile" of an attacker renders the search for a definitive predictive model futile; however, identifying behaviors that may indicate a propensity toward violence makes detection of an attacker possible.

The Exceptional Case Study Project also dismissed the prevailing wisdom that attackers were generally mentally ill, going so far as to state that "[a focus] on mental

---

[55] Robert Fein and Bryan Vossekuil, *Preventing Assassination: Secret Service Exceptional Case Study Project* (Washington, DC: National Institute for Justice, 1997), https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=167224, 1.

[56] Ibid., 41–44.

[57] Ibid., 1.

illness is not useful for those with responsibilities to prevent attacks."[58] The study suggests that this characterization derives from the logic that attacking a political leader is irrational because that leader can be removed from office peacefully through elections, and the leader operates in a system succession where the her or his replacement would be ideologically similar. In addition, the study distinguishes here between behavior that may be socially repugnant, as assassination is, and behavior that is clinically pathological.[59]

In the context of counterterrorism, other researchers have added to this premise. A 2017 analysis of terrorist writings determined that terrorists are rarely emotionally or cognitively impaired; rather, they generally exhibit a high level of negative emotions, anger, and cognitive flexibility.[60] In an earlier study of 98 lone actor terrorists in Europe by the Countering Lone Actor Terrorism Project (CLAT), 35 percent of subjects exhibited mental health issues compared to a World Health Organization estimate of 27 percent for the population at large. [61]

The more recent research on terrorism and the *Exceptional Case Study* agree that the perpetrators of lone actor violence do not share a consistent profile and eschew the assumption that such violence is, *per se,* a consequence of mental health issues. However, none of these studies describe the emergence of lone actor violence as undetectable. The *Exceptional Case Study* describes a "downward spiral" in the lives of many attackers but asserts that planning and undertaking an attack was the consequence of rational behavior.[62] The more recent linguistic study of lone actor terrorists describes their communications as representative of sophisticated but highly angry, categorical, and causally-integrated.[63] The final characteristic means that attackers often assessed a causal

---

[58] Ibid., 71.

[59] Ibid.

[60] Stephane Baele, "Lone Actor Terrorist's Emotions and Cognition: An Evaluation Beyond Stereotypes," *Political Psychology* 38, no. 3 (2017): 449, doi: 10.1111/pops.12365.

[61] Jeanine de Roy van Zuijdewijn and Edwin Bakker, "Analyzing Personal Characteristics of Lone-Actor Terrorists: Research Findings and Recommendations," *Perspectives on Terrorism* 10, no. 2 (2016): 45, https://openaccess.leidenuniv.nl/bitstream/handle/1887/44250/PersonalCharacteristics-PoT.pdf?sequence=1.

[62] Fein and Vosskuil, *Preventing Assassination*, 48, 75.

[63] Baele "Lone Actor Terrorists," 465.

linkage between the object of their anger and their own grief—what is colloquially referred to as "conspiracy theories."

None of these studies discard the idea that terrorism can be detected, but the consistency of their findings demonstrates the hazards of stereotyping. Attackers derive from a full range of backgrounds, are male and female, are young and old, and are motivated by ideas that may originate from a broader public movement but can also derive from personal grievances. Yet across this diversity of profiles, attackers do consistently demonstrate actions and thoughts that signal their intentions. A companion analysis of the 2016 CLAT study noted that changes in behavior prior to the attack, including "leakage behavior," wherein the perpetrator would express extreme views or an intention to commit violence to a third party.[64]

4. Legal Considerations—What Is a Threat?

When investigating potential lone actor violence, law enforcement agencies are faced with several legal obstacles. By definition, the lone actor does not rely on a larger conspiracy, and as such, the ultimate act of violence is not supported with other predicate crimes such as money laundering, arms trafficking, possession of banned substances, or other illegal acts. Confounding this further is that some of the actions a lone actor takes in preparation for a violent act are legal and constitutionally protected, such as endorsing certain beliefs or owning a firearm. Instead, investigators must rely on the expression of intent through a threat to arrest, and falling short of that, they must seek other methods to intervene. Threats in this context are unique in that they must be communicated; therefore, an investigator or prosecutor must discern where Frist Amendment protected freedom of speech ends and the crime begins.

The federal laws most germane to targeted violence are 18 U.S.C. § 871, Threats Against the President and Successors to the Presidency, which forbids "any threat to take the life of, to kidnap, or to inflict bodily harm upon the President of the United States, the

[64] Clare Ellis et al., "Analyzing the Process of Lone Actor Terrorism: Research Findings," *Perspectives on Terrorism* 10, no. 2 (2016): 36–37, https://openaccess.leidenuniv.nl/handle/1887/44254.

President-elect."[65] Additionally, 18 U.S.C. § 875(c) Interstate Communications, forbids "any communication containing any threat to kidnap any person or any threat to injure the person of another."[66]

Application of these laws has sometimes relied on the assumption that the communication, unto itself, was the crime. A 2015 Supreme Court decision Elonis v. United States rejected this assumption. The petitioner, Anthony Douglas Elonis, was arrested after posting a Facebook threat where he declared he would shoot his estranged wife and "slit her throat."[67] Elonis admitted to making the declaration but claimed that it was an imitation of a rapper who he admired. In an 8–1 decision, the court decided in favor of Elonis, determining that a threat required not only the communication but the intent to do harm.

In the majority opinion, Chief Justice John Roberts wrote,

> [C]ommunicating *something* is not what makes the conduct "wrongful." Here [quoting an earlier case] "the crucial element separating legal innocence from wrongful conduct" is the threatening nature of the communication. The mental state requirement must therefore apply to the fact that the communication contains a threat.[68]

Roberts's opinion relied on three definitions of threat to frame this argument: 1) "to declare (usually conditionally) one's intention of inflicting injury upon;" "an expression of an intention to inflict loss or harm on another by illegal means;" and "[a] communicated intent to inflict harm or loss on another".[69] Application of 18 U.S.C. § 871 is similarly challenging. When a celebrity performs a mock execution, holding the head of the president in the manner of a terrorist propaganda video and disseminates it broadly online, it is regarded as provocative to everyone who views it, offensive to many, and potentially illegal to a few. Even fewer may regard the celebrity as a physical threat to the world leader, even though the images are a graphic imitation of a murder.

---

[65] 18 U.S.C. § 871.

[66] 18 U.S.C. § 875(c).

[67] Elonis v. United States, 575 S. Ct. 983 (2015).

[68] Ibid.

[69] Ibid.

Considered alone, the physical threat to the world leader may be small, but the investigator must also consider the precedent set if the case is disregarded. The investigator must consider how the same communication would be perceived and the risk it presents if a heretofore-unknown person made it. The history of the celebrity might be publically available, allowing the investigator to put the communication into context with other controversial statements that person may have made. It would also be difficult to imagine a celebrity gaining the necessary access to the leader to kill him or her without being recognized. It is easier to consider the performance as provocative speech and nothing more. The unknown subject who performs the mock beheading lacks that mitigating context. Reaching the decision to investigate a case further involves a difficult triangulation between common sense, fairness, and public credibility.

5. Decision Making of the Investigator

Targeted violence may be detectible, but it is random and unpredictable. Lone actor attacks are salient to the public, but the legal definition of a threat is particular and prohibitive of law enforcement intervention. Given these circumstances, it is not difficult to be sympathetic toward the investigator who is faced with a decision of whether to move forward with a prolonged investigation or to close the case and move on.

To the law enforcement agency, this decision is not trivial. Any decision to move forward in an investigation carries the cost of time and other resources, an investment that comes at the opportunity cost of dedicating those scarce resources elsewhere. Continuing with a case also carries the risk of allegations that the investigative agency has violated the suspect's civil rights. From a purely probabilistic standpoint, this risk may be greater than the risk of the attack itself. Indicators of an impending threat include language that may indicate violence and access to weapons; however, these behaviors abut constitutionally protected rights. More often than not, a person who utters threatening speech does not commit violence, and a person who stockpiles weapons may not ever turn them on another person.

These narrow boundaries may inhibit investigators' propensity to investigate further unto themselves, but the steady stream of false leads may amplify these effects. In

emergency medicine, this is commonly called *alarm fatigue*, whereby the steady feedback of alarms that are not urgent can numb the reaction time of a caregiver.[70] It may be that the investigators, faced with the steady stream of false positives, will slowly reduce their vigilance toward future threats.

The possibility of previous outcomes affecting decision-making is further supported by Bayesian confirmation theory. Bayes's theorem proposes that the final probability of a hypothesis (in this case that a case in present time warrants further investigation) is a dividend of a probability presented by an initial hypothesis by the probability presented by additional evidence (every preceding investigation that is perceived to be either valid or not).[71] In his *Treatise on Probability*, Keynes explains the effect of evidence on an initial estimate of probability further, stating:

> In ordinary language we may assert that, according to our rule, the addition to our evidence of a single fact always has a definite bearing on our conclusion. It either leaves its probability unaffected and is irrelevant, or it has a definitely favourable or unfavourable bearing, being favourably or unfavourably relevant.[72]

Given these approaches to probability, it may be that an investigator's vigilance toward new threats steadily decomposes after a lengthy stream of false leads.

Other research asserts that people are, in fact, poor judges of probability. Abias researchers call the *gambler's fallacy* describes the tendency of decision makers, such as mortgage adjusters, baseball umpires, and gamblers themselves, to misjudge the probability of a future event based on the outcome of recent events. According to the research, this effect is most pronounced when an event is assumed to be random, such as

---

[70] Mike Mitka, "Joint Commission Warns of Alarm Fatigue: Multitude of Alarms from Monitoring Devices Problematic," *JAMA* 309, no. 22 (2013): 2315–2316, doi:10.1001.

[71] William Talbott, "Bayesian Epistemology," in *Stanford Encyclopedia of Philosophy*, winter 2016 ed., https://plato.stanford.edu/archives/win2016/entries/epistemology-bayesian, 8–9; James Joyce, "Bayes' Theorem," in *Stanford Encyclopedia of* Philosophy, Winter 2016 ed., https://plato.stanford.edu/archives/win2016/entries/bayes-theorem/, 2–4.

[72] John Maynard Keynes, *A Treatise on Probability: Full Text of 1921 Edition* (London: Macmillan and Co., 1921), Kindle ed., Chapter VI, location 1971.

a coin toss. [73] When a series of many tosses produce the same result, such as when that coin lands on "heads" several times in a row, the gamblers fallacy predicts that an observer will adjust his or her estimate of the next outcome in the *other* direction, believing that the run of previous events foretells such an adjustment.[74] This research detected the effect in decision making, quantifying a five percent difference in decisions as varied as whether an undocumented immigrant would receive asylum, whether an applicant would receive a loan, or a Major League batter received a called strike or a ball.[75] Although this behavior may appear to counter the concept of alarm fatigue and possibly Bayesian thinking generally, it is consistent with the idea that previous outcomes will affect future decisions.

6. Treatment of Lone Actor Events and Investigative Decision-Making from a Probabilistic Perspective

Approaching both lone actor events and the decision to investigate as a purely probabilistic phenomenon permits a contrast to the more complex motives and decision making extant with both. It is highly unlikely that either the attacker or investigator approach their actions as roll of the dice; however, a purely probabilistic examination illustrates the scale of the problem, provides a means to bench test different decision-making processes, and provides a baseline from which to contrast the actual decisions that are taking place.

The research on lone actor violence, which illustrates that there is no consistent profile or motive for a lone actor to attack, further validates a probabilistic approach. The time series and geospatial examination of lone actor violence adds evidence that the emergence of an attack is stochastic. By modeling the onset of an attack in a purely probabilistic way, the challenge to an investigator can be illustrated and quantified.

---

[73] Daniel Chen, Tobias J. Moskowitz, and Kelly Shue, "Decision-making under the Gambler's Fallacy: Evidence from Asylum Judges, Loan Officers, and Baseball Umpires" (working paper, NBER Working Paper Series, National Bureau of Economic Research, Washington, DC, 2016), http://www.nber.org/papers/w22026.pdf, 1.

[74] Ibid.

[75] Ibid.

From the investigator's perspective, the propensity to investigate can be modeled in different ways and compared to one another. For example, a model where a certain proportion of leads are investigated can be considered against other formulas that model both an alarm fatigue and a gambler's fallacy scenario. In the latter models, the decision to investigate or not would begin at one hundred percent and with rise or fall based on preceding outcomes.

Together, these decision-making processes were simulated using the Monte Carlo method. A Monte Carlo model simulated the occurrence of attacks at random intervals over time. Coinciding with the simulated onset of attacks was a simulated detection of that threat. Finally, the model applied different decision-making protocols to determine how many times an attack emerged, was detected, and ultimately, investigated.

7. Monte Carlo Simulations

Using a Microsoft Excel spreadsheet produced three decision making models. The intension of this sheet modeled a time period similar in length, 13030 days, to the time series analyzed earlier in this section (January 22, 1982 through October 1, 2017). The simulation used a random number generating formula within Excel. The researcher considered any random number that that was less than or equal to the specified probability for the event an "attack" and assigned the value 1. The researcher considered any event that exceeded the probability a non-event and assigned the value 0. This combined set accounted for 190 incidents over 13030 days; therefore, probability for an attack, on any given day, was set at 190/13030 = P_{attack} = .01458. This probability was used for all models for the attack side of the simulation.

Probability for detection was 0.7 (70 percent). The basis of this probability derives from the NTAC observation that 74 percent of lone actor attackers encountered law enforcement or other institutions before they attacked; however, not all of the encounters could be construed as related to the attack.[76] To account for this the NTAC statistic was deflated to 70 percent.

[76] National Threat Assessment Center, *Attacks on Federal Government*, 24.

Four separate simulations tested different decision-making dynamics. The first simulation, titled "Rapidly Diminishing Vigilance," was based on the assumption that an investigator's perception of a lead at time *t* is determined by her or his perception the previous day *t*-1 and the ratio of events to non-events. This probability began at 100 percent at day one. On subsequent days, the probability adjusted based on an average of the probability the day before and the ratio of outcomes where an attack occurred to outcomes where it did not.

Rapidly diminishing probability formula: [77]

1) Let t = the days in this simulation = $(1, 2, 3, \ldots 13{,}030)$
2) $Let\ a_t = an\ attack\ at\ time\ t\ and\ a'_t = a\ non-attack$
[Equation 1]: $Let\ P_t = \ the\ probability\ at\ time\ t\ where\ P_t = \frac{P_{t-1}}{2} + \frac{1}{2}\left(\sum_1^t \frac{a_{t-1}}{a'_{t-1}}\right)$

The second simulation, titled "Reactive Vigilance," builds upon the assumptions of the "Rapidly Diminishing" equation but adds an assumption that investigators will increase their vigilance and their propensity to open an investigation after an attack has occurred. With this assumption in mind, the probability will rise after an attack, then diminish, in a wave-like plot.

Reactive vigilance equation:[78]

[Equation 2]: $If\ a_{t-1} = 1\ then\ P_t = 1; if\ a_{t-1} \neq 1\ then\ P_t = \frac{P_{t-1}}{2} + \frac{1}{2}\left(\sum_1^t \frac{a_{t-1}}{a'_{t-1}}\right)$

The third simulation, titled "Gambler's Fallacy," adjusts the investigators decision-making whenever there is a sequence of five or more previous decisions to not investigate. The research of Chen et al. estimated that the decision makers they studied were five percent more likely than chance to change their decision in the opposite direction following a sequence of the same decision.[79] Using this five percent estimate, the "Gambler's Fallacy" is a two-step equation: the first is Equation 1, the second is an increase of 1.05 for every decision that follows until the decision changes.

---

[77] The function is represented as an Excel formula like this (assuming it is within row# 3, representing Day 2, and looking back at row#2, representing Day 1):
G2/2+((COUNTIF(C$2:C2,1)/COUNTIF(C$2:C2,0))/2).

[78] The function is represented as an Excel formula like this (assuming it is within row# 3, representing Day 2, and looking back at row#2, representing Day 1):IF(C2=1,1,G2/2+(I$1*(COUNTIF(C$2:C2,1)/COUNTIF(C$2:C2,0))/2)).

[79] Chen, Moskowitz, and Shue, "Decision-making under the Gambler's Fallacy," 1.

The fourth simulation is the simplest, “Investigate Everything that is Detected.” This simulation assumes the investigators will open a following investigation for every investigative lead they receive.

The Monte Carlo simulation estimated a cost statistic for outcomes with an attack, which yielded a cost, or detection and an investigation, which yielded a benefit (or negative cost). Additionally, a causality statistic was estimated any time an attack occurred. Like the occurrence of attacks, detections, and investigations, the number of casualties and associated economic costs were based on random number generators within the model; however, the distributions of the random numbers were different for the casualties and costs. The random numbers for the attacks, detections, and investigations were evenly distributed, which means that any number between zero and one was equally likely. Using an even distribution was appropriate because the likelihood of any of those events relied on their underlying probability. The casualties from actual lone actor attacks vary widely, with many attacks that have small numbers of casualties and fewer attacks with large numbers of casualties. This means the distribution of casualties is not even, where an equal number of attacks result in any number of casualties, nor are they normal, where attacks most frequently result in the mean number of casualties and an equal number of attacks with casualties that are higher or lower than the mean occur less frequently. Given this skewness, the random numbers that the model generated for casualties was adjusted so, like the actual attacks, many small casualty attacks and occasional mass casualty attacks occurred.

To determine the appropriate degree of skewness in the simulated casualties, the researcher derived mean and standard deviations from the historical data for fatalities and non-fatal injuries over 190 incidents. A histogram for these statistics showed a positive (rightward) skew, and thus, did not have a normal distribution. This is explained by a cursory review of the casualty rates. Attacks were most frequent in the low single-digits (1 to 5 for fatalities), yet there were several attacks with fatalities as high as 58. This leads to a frequency distribution that is “tall” in the low number but has a long, “fat” tail. Analysis of nonfatal injuries followed a similar pattern. To simulate casualties that would most often generate casualties that reflected this skewed distribution—many events with

single-digit results and occasional events with large results—a gamma distribution was applied to the random numbers associated with the fatality and non-fatal injury statistics.

A random number generator using these skewed distributions generated the consequences of these events. For any occasion where there was an attack but no investigation, the simulation multiplied the number of fatalities by $7 million, which uses the economic "value of life" originally developed by Richard Thaler.[80] For nonfatal casualties, the simulation deflated the number to 10 percent of the fatality value; $700,000. The effects were totaled, applying a coefficient of 1 for any successful attack, and -1 for any attack that was thwarted (i.e., attack attempted but investigation occurred, thereby yielding a "negative cost," or said differently, a societal gain).

The simulation ran each formula 13030 times, which represented each day in the time period of the sample. The simulation ran over five iterations for each scenario; Table 2 shows these averages. As would be expected in a simulation that ran as many turns within each iteration (13030), the average number of attacks were at or very close to 189, ranging between 179 (just below 95 percent of the expected result) and 190.8 (only one percent above the expected result). The average of the detections should be expected to be the same across all models, 70 percent of 13030, which equals 9121 (here the range only varied by less than one percent in either direction). Finally, the fourth variable, which represents the instances where attacks were both detected and occurred, should be close to 70 percent of the total number of attacks (132.3), and again the spread in the results ranged vary close (five percent below to two percent above).

It is in the remaining outcomes where the different models vary. For investigations opened, the number of cases opened varied widely, from 391.6 to 9164.4. This is to be expected. With the *rapidly diminishing* scenario, which is heavily dependent on the outcomes of earlier turns of the attack variable, the result was only slightly twice that of the attacks. Even a result that high is more a result of an averaging component—the decision was based on prior outcomes *and* averaged with the probability of the earlier

[80] Richard Thaler, "The Value of Saving a Life: Evidence from the Labor Market," in *Household Production and Consumption*, ed. Nestor E. Tereckyj (Washington, DC: National Bureau of Economic Research 1976), quoted in Richard Thaler, *Misbehaving: The Making of Behavioral Economics* (New York: W.W. Norton, 2015), 15.

investigative decision. Absent that second component, the decision would be purely based on attack results themselves; therefore, after a certain number of turns running toward infinity, the probability to investigate should converge toward the probability of attack. In this model, the averaging effect makes it more responsive to recent attack/non-attack outcomes, and as such, yielded a number that was significantly greater than the number of attacks themselves, yet still small.

Table 2. Monte Carlo Simulation Results—Average over Five Iterations

	Rapidly Diminishing Vigilance	**Reactive Vigilance (returns to probability of 100% after an attack)**	**Gambler's Fallacy—looking back five decisions**	**Investigate Everything that is Detected**
Attacks	189	179	190.8	186.4
Detections	9113	9096.4	9099.4	9124.4
Investigations Opened	391.6	536.4	826	9124.4
Attack and Detected	135	125.8	135.2	129
Attack and Investigated	3	8.4	11.2	129
Attack Detected and Investigated	2.2	6.8	7.4	129
Fatalities	1002.4	1006.2	1109.6	300.4
Nonfatal injury	2340.2	2342.2	2585	700.8
Fatalities Prevented	17.2	43.8	76.4	689.8
Injuries Prevented	39	102.4	177	1609.8
Net Economic Impact	$8,512,420,000	$8,304,660,000	$8,918,000,000	$ (3,362,100,000)

A consequence of the *rapidly diminishing* model's very low number of investigations was the opportunity to detect *and* investigate, meaning the attack failed, was only 2.2. The difference between detected attacks and those subsequently investigated was 132.8. This represents the number of "false positives" wherein attackers would have encountered law enforcement—71 percent of all attacks in this model.

The intermediate models, *reactive vigilance* and *gambler's fallacy*, both resolved with a greater number of investigations; therefore, they also yielded a larger number of thwarted attacks. *Reactive vigilance* resulted in a 37 percent increase in opened investigations, yet resulted in over three times as many thwarted attacks, on average.

Gambler's fallacy, which took the decision model of the *rapidly diminishing* model and then weighted it based on series of similar investigative decisions, made the decision at any point dependent on both the outcomes of attacks/non-attacks and previous decisions. This made the model's greater number of investigations than *rapidly diminishing* unsurprising, and a result that was greater than *reactive vigilance* but only slightly so. What was surprising is that although the model was also efficient in this increase of thwarted attacks compared to greater investigations (211 percent more investigations compared to 336 percent more disrupted attacks), it was less efficient than *reactive vigilance.* This indicates that the relationship between thwarted attacks and increasing caseloads is nonlinear; progressively opening a greater number of investigations, though positively correlated, yields diminishing returns.

Increasing caseload yields a diminishing benefit; however, it can yield a similar rate of false negatives (attacks detected but not investigated), and an increasing number of false positives (investigations that did not result in an attack). *Rapidly diminishing*, *reactive vigilance*, and *gambler's fallacy* yielded false positive rates of 70 percent, 66.5 percent and 67 percent, respectively. Contrasting this are the very low rates whereby attacks are disrupted: 1.6 percent, 4.7 percent and 5.9 percent. The remaining attacks are "bolts out of the clear blue sky;" the undetected surprise attacks that, under these hypothetical circumstances, went undetected and rounded out to 24.1%, 28.8 percent and 27.1 percent.

These results illustrate three characteristics of lone actor attacks that frustrate investigators. First, the strong effect of diminishing returns means that greater investment of resources and a concomitant increase in opportunity cost and exposure to liability will not necessarily yield an equivalent increase in benefits. A cursory review of the casualty rates and net economic costs from these attacks underscores this point; each of the models resulted in similar aggregate casualties and economic losses. Second, there will

always be attacks that are true surprises, and that proportion may be large enough to draw the conclusion that many or all lone actor attacks are undetectable. Finally, the first three models demonstrate that regardless of the single investigative agency's decision-making process, the outcome relies on the randomness of the event. Essentially, this is a game that relies more on the configuration of the dartboard, than the way the darts are thrown. With lone actor events, the bullseye occupies less than 1.5 percent of the board, which is the probability of an attack on a given day.

The *investigate everything* discussion warrants examination but only as a representation of the most extreme case in which an investigative agency is adequately resourced to investigate every lead. In this model, every attack that is detected is investigated, and ultimately, thwarted. This yields significant benefits and resolves to a net economic impact that is a societal *gain* of $3.3 billion; however, two things should be considered. First, this number should be amortized over the 33-year span of the model. Second, this benefit also comes with the cost of almost 9000 investigations that are opened but do not resolve to an attack.

Such a proportion means an average of almost five investigations-per-week would be false alarms. Furthermore, those false alarms come with their own costs. There are the already mentioned resource and opportunity costs as well as exposure to liabilities. In addition to these costs would be a cost that is difficult to quantify—the potential erosion of civil liberties. This effect is not trivial; investigative "fishing expeditions" were one reason that Congress imposed the "least intrusive means" restriction on intelligence operations within the United States and against U. S. citizens while abroad.[81] Considering more recent instances in which broad investigative authorities were later restricted, such as the FBI's use of national security letters in the early 2000s, it is likely that a 9000 to 189 ratio of invalid investigations to valid ones would offend public sensibilities.

These models are limited in their consideration of ancillary effects of investigative decisions. They do not capture nor quantify public opinion on either side of

[81] Exec. Order No. 12333, C.F.R. 3 (1981), https://www.archives.gov/federal-register/codification/executive-order/12333.html, 200.

the margins, which is the salience of attacks when they occur and the effect of overly-intrusive investigations when attacks do not occur. The models also do not assess the potential costs, whether opportunity costs or civil liabilities, which may occur from false alarms. In spite of the absence of these costs from the models, the frequency of the events that produce them remains. Through additional research, a more complete net effect of these costs could be added to these models and a more complete net cost estimate could be produced.

The scale of the models is another over simplification, albeit a deliberate one. This model was scaled to present a problem where the probability of attack was set for an attack on a particular day with no regard to population size or geographical extent. Models could be built that approach either probability of attack, whether it was the number of attacks in a given period divided by the total population of the United States, or the number of attacks divided by a predetermined ratio of the surface area that is determined to be affected by an attack to the surface area of the United States. Either of these possibilities would require a larger number of cycles—far greater than the chosen 13030; however, the results of the models, and the differences between them, would begin to resemble those of the models used for this report, which relied on day-to-day events and a single investigative entity as the decision- maker.

Detection and decision making are also severely simplified in this model. It is highly unlikely that investigators play darts with investigation decisions, nor do they roll dice with 10 sides in terms of detection, or 30 to 100 sides to decide whether to investigate a threat. In reality, the presence of evidence that indicates the potential for an attack will certainly influence both detection and decision making and would produce a much more complex model. Future models could consider this effect by simulating the issue of an indicator by the attacker, and the chance of detection by the investigator, or by building a decision-making equation that is more responsive to that indicator by the investigator or both.

The advantage of simplified models, scaled to a moderate size, is that variables can be isolated with the assumption that the other, more complex variables are encompassed in the more general relationships that are tested. Also, the interplay between

the decision parameters the researcher selects selected and randomness is observable. With the models selected, the general conclusion is that given the very low probability on a given day of an attack, decision making that is dependent on the frequency of that event in earlier days will yield modestly improved benefits if they are calibrated properly; however, that improvement will come at a much faster frequency of false positives. The results also help explain the frequency of pre-attack encounters between law enforcement and perpetrators; with the exception of the extreme *investigate everything* model, this happened far more frequently than successful investigations.

These findings suggest that randomness itself may contribute to the decisions investigators make. If an investigator seeks literal "hard" evidence that an attack will occur and does not find it, then there is little wisdom in investigating further if the ultimate goal is arrest, wherein due process obligates a high evidentiary standard. If the decision is framed by earlier outcomes, then the lack of evidence can provide an immediate reason to end an investigation. The organizational imperatives to produce arrests and the consequences of false positives may amplify one another and reduce the impetus to commit resources to a less compelling case.

If a less intrusive approach of managing potential risk is the endpoint, such as various intervention strategies that do not involve arrest, then the due process threshold may be reduced or eliminated; however, the challenge of decision making is not. In returning to the models, if the instances in which a suspect is investigated but would not attack are reframed from false arrests and intrusive investigations to simply false positives, the consequences of these errors are reduced but still come at a cost. With more "soft" strategies, such as countering violent extremism programs, the cost might be reduced confidence in the program. With the intervention of mental health professionals, it may be the overuse of a scarce resource. These outcomes obligate a decision-making model that is more precise than *investigate everything* but is more inclusive and complex than the other three models.

The models also illustrate the hazards of a single source of decision making, as they use a single decision-making node. This is not revelatory—the 9/11 Commission identified the "siloing" of decision making within the FBI as a contributing factor in the

failure to interdict the 9/11 attackers, and the Senate's examination of the Fort Hood attack showed the colocation of a more diverse group of analysts within decision-making task forces to have their own decision-making choke point. A single point of decision may present a single point of failure.

Soft strategies are inherently interdisciplinary; indeed, they rely on professions with different areas of expertise and their resources come from organizations with different imperatives. It is possible that the decision to commit to a long-term intervention strategy would benefit from insights that these various backgrounds can provide. For example, a potential attacker may show certain indicators considered concerning to some within an analytical forum and less so to others, but in aggregate, produce a more appropriate reflection of the risk the potential attacker presents than a single opinion. There are other experiments that have tested the accuracy of aggregated estimates, ranging from something as simple as many individual guesses of the number of pennies in a jar to the meta-analysis of multiple presidential election polls into a model that is more predictive than any of them were individually.[82] It is this principle tested in the following experiment, which uses the superforecasting technique to assess potential lone actor threats.

[82] James Surowiecki, *The Wisdom of the Crowds* (New York: Anchor Books, 2005), quoted in Daniel Kahneman, *Thinking Fast and Slow* (New York: Farrar, Straus and Giroux, 2013), 84.

IV. THE SUPERFORECASTING EXPERIMENT

A. SURVEY AND RESULTS

This research includes an online survey, from November 13 to December 1, 2017, with nine participating subjects. The intention of this survey was twofold. The first is to compare the risk assessments by a group of analysts of past incidents of lone actor or violence. The second intent is to present the participating subjects with broad hypothetical "prospects" in a threat assessment context to assess their overall sensitivity to risk. (See Appendix C for a description of the questionnaire describing this self-assessment).

Table 3. Professional Experience of Nine Participants in the Survey

Profession	**Number ***	**Years of Experience (range of years)**	**Average experience (years within profession)**
Law enforcement	6	2–31	17.5
Fire department or EMS	2	3–16	9.5
Military	0	n/a	n/a
Medicine or Public Health	2	6–18	12
Social Worker	1	1	1
Other (see Appendix B for a complete list)	5	1–10	6.2
	Total:	180	20

* There were only nine subjects in the survey; however, some of them had experience in two or more of the professions listed in Table 3. For this table, all of the experience is accounted for. For the calculation of data results, the experience was allocated for each individual for questions 1 and 3 through 6. For question 2, the risk probability question, a single profession was used to avoid skewing the results of that data.

The researcher recruited from the Naval Postgraduate School, from professional contacts, and by word-of-mouth. Subjects received and invitations by email and completed the survey with an online platform called LimeSurvey.

B. SURVEY PART ONE—SCENARIOS

The subjects viewed five cases of targeted violence. The selected cases were based on the availability of public information about the attackers—no information appearing in the scenarios derived from classified sources or those unavailable to the public. Also, the researcher selected the cases to represent at least one example of a "lone wolf terrorist," an assassin, and a school shooter. This information was synopsized and redacted to simulate two conditions: 1) the information in a networked analysis system, which would need to be filtered in order to be disseminated, and 2) information that was ultimately disseminated would usually be incomplete.

To meet the first condition, it was assumed that any broad network of analysts would have varying levels of access to data; therefore, any information distributed over such a wide system would require filtering of personally identifiable information of the person investigated as well as any information gained through classified means, grand jury subpoenas, access to health records, or other private data. Second, it was assumed that a realistic simulation would involve a set of information that could be reasonably obtained by the initial investigator; therefore, the scenario only included information the investigators discovered at the time they first investigated the suspects in these cases.

To simulate actual conditions for "new" analysis, the scenario did not identify the cases upon which the scenarios were based to the subjects. The cases from which the scenarios were derived are listed below, followed by the year which they first encountered an investigator. The information found in these scenarios derived solely from information available in the public domain, the sources of which are annotated with their respective case.

Scenario 1—Jared Lee Loughner (2009)	First contact with police: 2007[83]
Scenario 2—Omar Gonzalez (2014)	First contact with police: 2014[84]
Scenario 3—Nidal Hassan (2009)	First contact with police: 2008[85]

[83] National Threat Assessment Center, *Using a Systems Approach for Threat Assessment Investigations: A Case Study on Jared Lee Loughner* (Washington, DC: U.S. Secret Service, 2015).

[84] U.S. Department of Homeland Security, *2014 White House Fence Jumping Incident*.

[85] Senate Committee on Homeland Security and Governmental Affairs, *A Ticking Time Bomb.*

Scenario 4—Eric Harris (1999)	First contact with police: 1998[86]
Scenario 5—Dylan Klebold (1999)	First contact with police: 1998[87]

1. Survey Part One—Questions

Subjects answered six questions about each scenario:[88]

1. Are you familiar with this case? Although filtered, the scenarios were still widely reported when they occurred. If a subject recognized one of these cases, they would likely assign a high probability to question 2, thereby skewing the results. Asking this question allowed for a second analysis of the scores that corrected this bias.

2. On a scale of 0 to 100, rate how likely it is that this subject will commit violence in the future? This is the superforecasting question.

3. Do you think this subject should be investigated further? This question was included to see if there was a divergence of probabilities assigned by the subjects from their curiosity in or suspicion of the person described in the case.

4. If you chose to investigate further, what would be your next investigative step? This question is an expansion of question 3.

5. Based on the facts you read, do you think there is cause to arrest this subject? This question was intended to detect other potential biases, such as sensitivity to risk and the subject's general sense of the "probable cause" standard for arrest.

6. What were the key aspects of this case that influenced your decision? This question permits secondary analysis of which details in each scenario were the most salient to the subject.

2. Survey Part One Data—Scoring the Results

The experiment borrows from *Superforecasting* by using the "Brier score" to evaluate subjects' evaluations of the scenarios. The Brier score is a statistic borrowed

---

[86] State of Colorado Department of Law, Office of the Attorney General, *Report of the Investigation into the 1997 Directed Report and Related Matters Concerning the Columbine High School Shootings in April 1999* (Denver, CO: State of Colorado Department of Law, 2004), https://schoolshooters.info/sites/default/files/1997_1998_columbine_report.pdf; Columbine Review Commission, *The Report of Governor Bill Owens Governor's Columbine Review Commission* (Denver, CO, Columbine Review Commission, 2001), https://schoolshooters.info/sites/default/files/Columbine%20-%20Governor's%20Commission%20Report.pdf.

[87] Ibid.

[88] The complete survey can be found in Appendix C.

from meteorology to evaluate weather forecasters and is designed to reward precision.[89] It does this through an elegant formula, which adds the squared differences between a forecast and the actual outcome, and the forecast predicting against the same condition and that outcome. For example:

- If a forecaster predicts a 70 percent chance of rain the next day, and it actually rains, then the Brier score is calculated accordingly:
- The prediction is 70 percent *for* rain, therefore is it also a prediction of 30 percent *against* rain.
- The outcome was rain (100 percent for / 0 percent against), therefore;
- $(1\text{-}0.7)^2 + (0\text{-}0.3)^2 = 0.18$

A lower score represents a more accurate forecast with a minimum of 0 for a perfect forecast and a maximum of 2 for a completely inaccurate forecast. The effect of squaring the differences is that every change in forecasting precision is rewarded, or penalized, exponentially. See Tables 4–9 for scenario Brier score results.

A general rule of thumb for the results of a Brier score can then be:

- (perfectly accurate) to <0.5 (slightly more accurate than chance)
- 0.5 (complete chance—a result from choosing 50 percent, as with a coin toss)
- >0.5 (slightly less accurate than chance) to 2.0 (completely inaccurate).

[89] Glen W. Brier, "Verification of Forecasts Expressed in Terms of Probability," *Monthly Weather Review* 78, no 1 (1950): 1–3.

Table 4. Brier Scores for All Scenarios

	Scenario 1	**Scenario 2**	**Scenario 3**	**Scenario 4**	**Scenario 5**	**Average for all scenarios**
Overall	**0.221**	**0.241**	**0.723**	**0.100**	**0.409**	**0.306**
Law Enforcement	0.131	0.139	0.855	0.028	0.416	0.244
Fire Department or EMS	0.180	0.320	n/a	0.020	n/a	0.142
Medicine or Public Health	0.5	0.500	0.605	0.125	0.125	0.336
Other	0.151	0.101	0.720	0.361	0.845	0.378

Table 5. Scenario 1 Results

	Are you familiar with this case?	**Probability to commit violence***	**Investigate further?**	**Would you arrest?**
Overall	Yes: 0 No: 9	66.7% var =1.3%	Yes: 9 No: 0	Yes: 0 No: 9
Law Enforcement	Yes: 0 No: 4.69	74.4%	Yes: 4.69No: 0	Yes: 0 No: 4.69
Fire Department or EMS	Yes: 0 No: 0.78	70.0%	Yes: 0.78 No: 0	Yes: 0 No: 0.78
Medicine or Public Health	Yes: 0 No: 1.39	50.0%	Yes: 1.39 No: 0	Yes: 0 No: 1.39
Social Worker	Yes: 0 No: 0.07	*	Yes: 0.07 No: 0	Yes: 0 No: 0.07
Other	Yes: 0 No: 2.07	77.5%	Yes: 2.07 No: 0	Yes: 0 No: 2.07

*No score

Table 6. Scenario 2 Results

	Are you familiar with this case?	**Probability to commit violence**	**Investigate further?**	**Would you arrest?**
Overall	Yes: 0 No: 9	65.3% var =1.6%	Yes: 9 No: 0	Yes: 1 No: 78
Law Enforcement	Yes: 0 No: 4.69	73.6%	Yes: 4.69 No: 0	Yes: 0 No: 4.69
Fire Department or EMS	Yes: 0 No: 0.78	60%	Yes: 0.78 No: 0	Yes: 0.43 No: 0.35
Medicine or Public Health	Yes: 0 No: 1.39	50%	Yes: 1.39 No: 0	Yes: 0 No: 1.39
Social Worker	Yes: 0 No: 0.07	*	Yes: 0.07 No: 0	Yes: 0 No: 0.07
Other	Yes: 0 No: 2.07	77.5%	Yes: 2.07 No: 0	Yes: 0.57 No: 1.5

*No score

Table 7. Scenario 3 Results

	Are you familiar with this case?	**Probability to commit violence**	**Investigate further?**	**Would you arrest?**
Overall	Yes: 7 No: 2	39.9% var =0.3%	Yes: 7 No: 0*	Yes: 0* No: 7
Law Enforcement	Yes: 3.83 No: 0.86	34.6%	Yes: 3.64 No: 0	Yes: 0 No: 3.64
Fire Department or EMS	Yes: 0.78 No: 0	*No score recorded*	Yes: 0.43 No: 0	Yes: 0 No: 0.43
Medicine or Public Health	Yes: 0.39 No: 1	45%	Yes: 1 No: 0	Yes: 0 No: 1
Social Worker	Yes: 0 No: 0.07	**	Yes: 0.07 No: 0	Yes: 0 No: 0.07
Other	Yes: 2 No: 0.07	40%	Yes: 1.86 No: 0	Yes: 0 No: 1.86

*two respondents did not answer
**No score

Table 8. Scenario 4 Results

	Are you familiar with this case?	**Probability to commit violence**	**Investigate further?**	**Would you arrest?**
Overall	Yes: 3 No: 6	77.7% var =2.3%	Yes: 8 No: 1	Yes: 4 No: 5
Law Enforcement	Yes: 2 No: 2.69	88.2%	Yes: 4.64 No: 0.04	Yes: 1.79 No: 2.9
Fire Department or EMS	Yes: 0 No: 0.78	90%	Yes: 0.43 No: 0.35	Yes: 0 No: 0.78
Medicine or Public Health	Yes: 0 No: 1.39	75%	Yes: 1 No: 0.39	Yes: 1 No: 0.39
Social Worker	Yes: 0 No: 0.07	*	Yes: 0.07 No: 0	Yes: 0 No: 0.07
Other	Yes: 1 No: 1.07	57.5%	Yes: 1.86 No: 0.22	Yes: 1.21 No: 0.86

*No score

Table 9. Scenario 5 Results

	Are you familiar with this case?	**Probability to commit violence**	**Investigate further?**	**Would you arrest?**
Overall	Yes: 3 No: 6	54.8% var =4.0%	Yes: 6 No: 2*	Yes: 1 No: 7*
Law Enforcement	Yes: 1.04 No: 3.64	54.4%	Yes: 3.64 No: 1	Yes: 0 No: 4.64
Fire Department or EMS	Yes: 0.35 No: 0.43	No score recorded	Yes: 0.43 No: 0	Yes: 0 No: 0.43
Medicine or Public Health	Yes: 0.39 No: 1	75%	Yes: 1 No: 0.3	Yes: 1 No: 0
Social Worker	Yes: 0 No: 0.07	**	Yes: 0.07 No: 0	Yes: 0 No: 0.07
Other	Yes: 1.22 No: 0.86	35%	Yes: 0.86 No: 1	Yes: 0 No: 1.86

*one respondent did not answer
**No score

This experiment only covered a brief time and had a very small sample size. I limited the sample size to nine subjects due to restrictions that the Paperwork Reduction Act of 1995 places on researchers who are federal employees (such as I am).[90] Such a small sample size may not be representative of an experiment that is more broadly represented and longer term. For these reasons, the results of this survey should be regarded as an early prototype of an experiment that a law enforcement organization or academic institution could perform more extensively. Ideas for how this experiment could be expanded and improved are covered in a later section.

3. Analysis of the Scenario Results

The Brier scores of the analysts overall was .221 for Scenario 1 (Loughner); .241 for Scenario 2 (Gonzalez); .100 for Scenario 4 (Harris) and .409 for Scenario 5 (Klebold). These results should be regarded as highly predictive for Scenarios 1, 2 and 4, and better than chance for Scenario 5. Scenario 3 (Hassan) has a less than predictive score and is examined in depth later in this chapter. Although these results derive from too small of a sample size to claim that a superforecasting method is an improvement over single decision makers or investigative squads, it is promising enough to consider running a similar experiment on a larger scale.

Across all five scenarios, the Brier score was 0.288, derived from an average probability score of 62 percent with a small variance of 0.6 percent. The range of scores varied widely between 20 percent (a score assigned to Scenario 5 by a respondent who indicated recognition of the case) and 99 percent (a score assigned to Scenario 4 by a respondent who was also familiar with the case), but when averaged, the scores were more moderate but still predictive. This tendency of aggregated scores to generally offset the effects of exceptionally high or low individual assessments demonstrates the potential for this method. If a larger forum considered similar cases with a similar result, this may provide evidence that a broad array of disciplines would offset the extremes, thereby providing a more balanced treatment of a case.

[90] "Information Collection and Paperwork Reduction Act (PRA) Overview," Usability, accessed November 5, 2017, https://www.usability.gov/how-to-and-tools/guidance/pra-overview.html.

A larger sample size could also be presented with several iterations, wherein participants who present more accurate scores can be weighted more than those who are inaccurate in later turns. Tetlow used this technique in *Superforecasting* and produced forecasts that were superior to both individual superforecasters (individuals who were successful) and professional analysts.

Responses to other questions in the scenarios may also illuminate the difficulty that law enforcement agencies face when making the critical decision to carry a lone actor case further. When asked whether a scenario presented enough information to arrest the subject, respondents almost unanimously answered "no" across all scenarios; however, in four out of five scenarios, a majority of respondents indicated that there was enough information to investigate the subject further. This disparity speaks to the challenge for law enforcement agencies, which generally measure their success through arrest statistics. If a larger experiment registered this divergence in responses, it may provide further evidence for the need to develop "softer" solutions, such as countering violent extremism initiatives and more collaboration between law enforcement and other disciplines, such as public and mental health institutions.

4. Differences between the Disciplines

Given the limited number of participants in this experiment, one should not draw no definitive conclusions from the results. This level of analysis would be interesting in a larger experiment, but with only one or two representatives for all but law enforcement, it is impossible to distinguish the effects between the individuals and those of their calling in this prototype experiment.

5. The Fort Hood Exception

An interesting result emerged in the combined Brier score for Scenario 3, which represented the Fort Hood attack. Here, the participants only registered a .608, which reflect a result that is slightly worse than an even chance, coin-toss driven decision. There are several reasons why this may be the least predictive assessment by the group, but the simplest explanation may be the most likely. The information presented in the question represented what would have been available to analysts at a moment where a critical

decision about the case would have been made, which was not indicative unto itself that the subject demonstrated a risk for violence. If this result is consistent in a larger sample size, it would indicate that a broader treatment of the case, beyond that of the JTTFs that investigated Hassan, may have also found that his behavior, although concerning, was not cause to engage in a more intrusive investigation.

Answers to two other questions associated with the Fort Hood scenario were more equivocal. Only half of the respondents indicated that they would investigate further, although all indicated that an Army officer's communication with a "known terrorist leader" was concerning. None of the respondents indicated that the facts of the case indicated probable cause for arrest; however, this was typical for all scenarios—three scenarios (Gonzalez, Harris, and Klebold) had only a single respondent answer "yes" to that question., and the other had no respondents answer "yes."

The Fort Hood was also the scenario recognizable to the greatest number of respondents, which means that those who were familiar and continued to answer subsequent questions factored in their preconceptions about the case and underestimated the potential for violence; however, the data cannot determine this. The possibility of this effect only warrants mentioning here as a possible protocol for future experiments. If there were a larger number of participants, scores of those who were familiar could be compared to those who were not, and a correlation may emerge between familiarity and subsequent scores. Another possibility is that the scores from respondents who are familiar with a case can be discarded.

The data acquired from the case study part of this experiment provides insight into how certain narratives were salient for participants, while others were not. The reasons for that salience exceed the boundaries of this paper. Some possible lines of investigation are offered in Appendix A. One possible answer lies in the risk tolerance of the participants when they presented relatively similar choices. This is examined in the next phase of the survey.

C. SURVEY PART TWO—PROSPECTS AND RISK ASSESSMENT SURVEY

1. Survey Part Two—Prospect Theory Questions

The design of the second part of the survey was to gain a broader sense of subjects' risk tolerances and decision making based on a prospect theory model. In the findings from the original paper on prospect theory by psychologists Daniel Kahneman and Amos Tverskey, subjects demonstrated a preference for certain prospects, which, depending on how their choices were presented and risk under uncertainty, contradicted prevailing thought on expected utility theory.[91] This theory is premised on the assumption of the decision maker as a "rational actor," whereby the preferred choice between two prospects was the one that yielded the greatest product between the probability of it occurring and its payout. [92] For example, a 50 percent chance to win $100 would be preferred to a 100 percent chance to win $45, because the expected value of the first choice ($50, or 50% x 100) is greater than $45. Using a series of paired prospects, Kahneman and Tverskey found that certain choices were often preferred to uncertain ones with a higher expected value.[93]

Later research of intelligence professionals presented life-or-death prospects that reinforced the findings of prospect theory. This research indicated that intelligence professionals who were presented decision-making prospects were more prone to "irrational consistencies" than those who were not intelligence professionals. The irrational consistencies meant that they made opposite choices on equivalent prospects, which were framed as either a gain or a loss.[94]

---

[91] Daniel Kahneman and Amos Tversky, "Prospect Theory," *Econometrica* 47, no. 2 (1979): 263. doi: 10.2307/1914185.

[92] John van Neumann and Oskar Morgenstern, *Theory of Games and Economic Behavior* (Princeton: Princeton University Press, 1947), quoted in Kahneman, *Thinking Fast and Slow*, 270.

[93] Kahneman and Tversky, "Prospect Theory,"

[94] Valerie F. Reyna et al., "Developmental Reversals in Risky Decision Making: Intelligence Agents Show Larger Decision Biases Than College Students," *Psychological Science* 25, no. 1 (2013): 76, http://doi.org/10.1177/0956797613497022.

This tendency is what Kahneman and Tversky originally called the "framing effect."[95] This effect predicts that people will "overweight. . . sure things and . . improbable events, relative to events of moderate probability" and that "[d]ecision problems can be described or framed in multiple ways that give rise to different preferences."[96]

2. Survey Part Two—Results

The following six questions are intended to detect risk aversion or risk seeking behavior, and the "framing effect," by presenting the subjects with similar prospects. The questions derive form the work of Kahneman and Tverskey, but use a variation of the "life or death" context used in Reyna et al.[97] See Tables 10–15 for survey questions and results.

> Imagine you are managing an investigative squad in a homeland security agency, and you need to decide whether to open or close an investigation.

Table 10. Prospect 1 Question and Results

Prospect 1. If you could only choose one, which do you consider the higher priority case?

A.	B.
50% chance to save seven lives 50% chance that the case is a false alarm (nothing happens)	100% chance to save three lives

	A.	B.
Overall	**4.00**	**5.00**
Law Enforcement	1.64	3.04
Fire Department or EMS	0.43	0.35
Medicine or Public Health	1.00	0.39
Social Worker	0.07	0.00
Other	0.86	1.22

[95] Daniel Kahneman and Amos Tversky, "Choices, Values, and Frames," *American Psychologist* 39, no. 4 (1984): 341–350, doi:10.1037/0003-066X.39.4.341.

[96] Ibid.

[97] Reyna et al., "Developmental Reversals."

Table 11. Prospect 2 Question and Results

Prospect 2. If you could only choose one, which do you consider the higher priority case?

A.	B.
50% chance to prevent $55 million of damage 50% chance that the case is a false alarm (nothing happens)	100% chance to prevent $25 million of damages

	A.	B.
Overall	**4.00**	**5.00**
Law Enforcement	1.57	3.11
Fire Department or EMS	0.43	0.35
Medicine or Public Health	1.00	0.39
Social Worker	0.00	0.07
Other	1.00	1.07

Table 12. Prospect 3 Question and Results

Prospect 3. If you could only choose one, which do you consider the higher priority case?

A.	B.
1% chance that 100 people will die 33% that 9 people will die 67% that it is a false alarm	100% chance that three people will die

	A.	B.
Overall	**2.00**	**6.00***
Law Enforcement	0.79	2.90
Fire Department or EMS	0.00	0.78
Military	0.00	0.00
Medicine or Public Health	1.00	0.39
Social Worker	0.00	0.07
Other	0.21	1.86

*one respondent did not answer this question

Table 13. Prospect 4 Question and Results

Prospect 4. If you could only choose one, which do you consider the higher-priority case?

A.	B.
1% chance that $700 million of damage will occur 33% that $30 million of damage will occur 67% that it is a false alarm	100% chance that $15 million of damage will occur

	A.	B.
Overall	**2.00**	**7.00**
Law Enforcement	0.86	3.83
Fire Department or EMS	0.00	0.78
Military	0.00	0.00
Medicine or Public Health	1.00	0.39
Social Worker	0.07	0.00
Other	0.07	2.00

Table 14. Prospect 5 Question and Results

Prospect 5. Imagine you are up for promotion. Only 1% of cases you receive have intelligence as solid as the case your boss gives you. He assigns it to you and promises that if you succeed, you will receive a $10,000 performance bonus. Once you begin investigating, you realize that the intelligence is not as clear as you originally thought. Success may hinge on how long you investigate. Which choice below would you make?

Commit to a long investigation.	Close the case quickly.
45% chance that the case is fully successful (full $10,000 bonus) 55% chance that the case is a false alarm	100% chance that if you cut the case short, you will receive the bonus you received last year ($5,000)

	A.	B.
Overall	**9.00**	**0.00**
Law enforcement	4.69	0.00
Fire department or EMS	0.78	0.00
Military	0.00	0.00
Medicine or Public Health	1.39	0.00
Social Worker	0.07	0.00
Other	2.07	0.00

Table 15. Prospect 6 Question and Results

Prospect 6. You receive a promotion from your last case that increases your salary by $10,000 per year. Now, as a manager, you have to make the tough choices. Another case arrives on your desk, a "1 %" case, with the same issues as the last scenario. Here, you have to make a tough resource allocation decision.

Commit to a long investigation.	Close the case quickly.
45% chance that the case is fully successful 55% chance that the case is a false alarm and that your agency will be sued for ($10,000 loss)	100% chance that if you cut the case short, you will only waste the time and resources expended thus far ($5,000 loss)

	A.	B.
Overall	**4.00**	**5.00**
Law enforcement	2.64	2.04
Fire department or EMS	0.00	0.78
Military	0.00	0.00
Medicine or Public Health	1.00	0.39
Social Worker	0.07	0.00
Other	0.29	1.79

3. Analysis of the Prospect Theory Responses

In part two of the survey, respondents evaluated six "prospects" framed in a homeland security context. Prospects 1 and 3 and were similar prospects in terms of their utility as were Prospects 2 and 4; what distinguished each set was that the utilities were described as gains or losses. For example, in Prospects 1 and 2, respondents had to choose between two prospects that would "save lives," signifying a gain; however, in Prospects 3 and 4, respondents had similar choices wherein the consequence was "people will die," signifying a loss. Prospects 5 and 6 also contrasted in a similar manner, wherein the choices in five signified a gain in the form of a bonus for success, and the choices in six were described as a loss in the form of a potential law suit or lost time and resources.

The responses were strongly consistent with prospect theory in some ways, and less so in others. In Prospect 1, five respondents favored the choice of saving three lives with 100 percent certainty to a 50 percent prospect of saving seven lives with 50 percent certainty (an expected value of 3.5 lives saved). In Prospect 3, a strong majority of seven

favored the certain prospect of pursuing the case where "three people will die" with certainty over a case where 100 people will die with one percent probability, nine will die with 33 percent probability, and 67 percent probability that the case is a false alarm (and expected value of four deaths). These responses are consistent, although only mildly so in Prospect 1, with the "certainty effect" described by Kahneman and Tversky, whereby decision makers favor choices that are certain even when they resolve to a lower expected value to alternatives that are uncertain.[98]

Prospect theory would also predict that the framing of a perceived gain in one prospect, and the loss in another, would produce a favoring of the uncertain choice, or risk-seeking behavior, in loss-oriented prospect.[99] A cursory review of the data shows that this "reflection effect" was absent; however, a review of the manner in which the prospects were presented may indicate otherwise. In Kahneman and Tversky's original treatment of the reflection effect, the choices were a pure monetary gain or loss. For example, the loss could reflect the cost of a traffic ticket or the decision to buy or not buy insurance to recover the replacement cost of property loss.[100] In the experiment, the "loss" prospect was presented as a choice to prevent a loss, which may have unintentionally created a double-negative effect, thereby leading the respondents to perceive the choices as gains rather than losses.

Responses to Prospects 2 and 4 were similar to 1 and 3, wherein respondents favored certain choices over uncertain ones yeilding a larger expected value. The choices were also intended to be reflective, with one framed as a "prevented" economic damage and the other as "damage will occur;" however, this distinction may have also been ambiguous to the respondents. Like Prospects 1 and 2, the respondents selected the certain choices of preventing a smaller amount of expected economic damage over the uncertain, but larger, potential damage.

---

[98] Kahneman and Tversky, "Prospect Theory," 265–267.

[99] Ibid., 268.

[100] Ibid., 268–271.

In the final two prospects, the results were more clearly counter to prospect theory. In Prospect 5, all respondents favored the choice that was not only uncertain but also one with a smaller expected value: 45 percent probability of a $10,000 bonus versus a guaranteed bonus of $5,000. In Prospect 6, more respondents (five to three) favored the choice with a more favorable expected value of $5,000 over a "gamble" with a 55 percent chance of losing $10,000 but a 45 percent chance of losing nothing; however, this is also a potential contradiction to what prospect theory predicts. In facing losses, prospect theory predicts that respondents may become risk seeking, rather than favoring the certain gains demonstrated in the responses to Prospects 1 through 4.[101] The eccentricities of these responses may be a consequence of the way the choices were described in the survey questions, or they could reflect idiosyncratic risk tolerances of the respondents. Another explanation may be found in Kahneman's later description of loss aversion and prospect theory, which notes that the scale of different choices may affect a decision maker's choices.[102]

In spite of some possible inconsistencies, in very particular ways, with prospect theory, a pattern from the responses emerges generally favoring certain prospects to uncertain ones, despite the greater expected values of alternative choices. This may help to explain the relative strength of some probability scores in the case oriented scenarios than others. The highest predictions for scores were found in Scenarios 4, 1, and 2, which were the Harris, Loughner, and Gonzalez cases, respectively. There may be characteristics of that narrative, such as previous encounters with law enforcement, possession of weapons, or other characteristics, which make these choices more tangible, or by extension, certain, than the other two scenarios. Given the limited number of questions in this experiment, and the limited sample size, this can only be left to speculation here; however, it presents a possibility for further research where case studies can be presented alongside prospect theory questions to determine the effects of risk tolerance on case study related decisions.

---

[101] Kahneman and Tversky, "Prospect Theory," 271.

[102] Kahneman, *Thinking Fast and Slow,* 283–285.

The limited size of the survey precludes any larger assumptions about investigative decision making, and the results indicate an accuracy that is compelling in some cases, but it also generates further questions about why some cases were more compelling than others to the survey participants. These are questions that can only be examined through a larger survey, one which explores these decisions in depth. The combination of the scenario based and prospect theory questions would enable a simultaneous examination of risk detection in the cases, which would be correlated to the decision making that participants make under uncertainty in more hypothetical choices.

The possibility of a deployment of a superforecasting system into actual enforcement decisions also warrants examination. The advantages and pitfalls of such a deployment are examined in the next chapter, while several ideas for further research and some unresolved questions that this research yielded are cataloged in Appendix A.

V. IMPLEMENTATION OF A SUPERFORECASTING NETWORK FOR DETECTING LONE ACTOR VIOLENCE: THE SUPERNETWORK

It is worth revisiting the current framework of multidisciplinary collaboration in investigations, the task force model, in order to contrast it to a new model that uses a networked *Superforecasting* technique, which would be called a supernetwork. Task forces are generally a collocation of various practitioners who are organized under a unifying purpose, the "task," and a harmonizing organizational structure, the "force." This organizational model was a solution to a particular problem, where the disparate efforts of several government agencies were at best less than the sum of their parts, and at worst, worked at cross-purposes. But over time, task forces assume an organizational identity of their own, and it appears that as this identity grows, the benefits from interdisciplinary participation decreases.

A supernetwork could avoid this problem by using a flat, networked organizational model, wherein participants remain in their professions day-to-day, but dedicate a small percentage of their time to the analysis of potential threats. Such a view from afar would insulate them from decision-making biases that may result from being in a single organization while working toward a common purpose.

A. WISDOM OF THE CROWD VERSUS EXPERTISE

While the use of a supernetwork may improve threat analysis, it is likely a mistake to envision such a construct as a replacement for the in-depth examination that a traditional law enforcement investigation would provide. The advent of networked information and the rising availability of information has spawned the misconception that expertise does not matter. In a moment when populism and homegrown narrative and reporting have taken on significant strength, expertise suffered further damage. Tetlow dreads the prefix of "so-called" so often used by populists when describing experts.[103] This is confirmation bias turned on its head and taken to an extreme when pundits

[103] Tetlock and Gardner, *Superforecasting*, 71.

disparage expertise when the evidence is aligned against their narrative. They tear down the messenger and present "alternative facts."

On the other hand, the lesson of superforecasting seems to auger against pure reliance on expertise. It is a story of amateurs beating the professionals in prediction, even when the professionals had exclusive access to classified information. Groupthink speaks to the hazards of overreliance on expertise, particularly when it is a team of experts who amplify each other's biases. The result of this prototype experiment may support this assertion. The decision between expertise and the wisdom of the crowd may be a false choice. A mixed methodology can tether the depth of knowledge and commitment to craft that an expert has with the distributed strength found in a network.

A mixed approach may have advantages that extend beyond the aggregation of experts who are arrayed against a problem. The "citizen scientist" model, which has been effectively used in scientific endeavors such as astronomy and meteorology, provides examples of how a distributed network of detection can be aligned with deep expertise. In applying such a model to threat analysis, an organizational topology that is flat and wide may offset groupthink and increase the collective's sensitivity to emerging trends. Having it populated with experts will ensure that legal and ethical standards are held and that the public's rights are safeguarded.

B. ENGAGEMENT OF COMMUNITY LEADERS

In the specific case of religion-inspired lone wolf terrorism, a solution posited by some countering violent extremism strategies is to recruit faith leaders, such as imams for Islamic extremism, to identify radicalizing individuals or to have teachers and other educators report disturbing behavior. Yet, if there is a bond between social leaders and other group members operating at several levels, such as faith, culture, family and ethnicity, such an expectation that may be morally repugnant to those faith leaders. Compelling community leaders to engage directly in the detection of potentially violent behavior may be akin to expecting a mother to betray her child. A broad based analytical network may counterbalance that sense of betrayal. In this sense, proximity may be inversely related to objectivity.

C. POTENTIAL HAZARDS OF THE SUPERNETWORK

The analytical system, tested in the experiment and contemplated as an organizational model in this chapter, imagines an integrated and efficient network employing the talents of many disciplines to address a particular problem. Here, the question switches from "will it work" to "does it work too well?"

A secondary phase of the supernetwork could be to conduct background analysis of feedback from the analysts, including sentiment analysis of text, correlation with large data sets, and the use of social media tools to encourage dialog between government and the public. It is possible that an overreliance of any or all of these methods, including the network itself, could present unintended consequences.

D. CIVIL RIGHTS CONSIDERATIONS

An accepted supernetwork that works well could be misapplied or misinterpreted by an organization placing excessive faith in its predictive capabilities. Tools that rely on quantitative analysis have an inherent opacity. When this data is extruded through the analytical "black box," only a rarified few understand exactly what the box is doing. It is difficult for the analyst, the investigator, the prosecutor, the judge, or ultimately, the public to understand how that black box has developed its output. Analysts and investigators cannot entertain their skepticism with direct scrutiny of the methodology behind the analysis. Instead, they must fall back on conventional wisdom and first-hand experience. In doing so, another layer of uncertainty arises, since it may be their observations, through confirmation bias or other behavioral influences, that are flawed—not the predictive system itself.

Data mining tools are growing in capacity while the public leaves a rising volume of digital data "exhaust." Citizens knowingly and unknowingly leave a stream of heretofore private information that can be exploited by third parties. To date, case law is lagging behind. The Fourth Amendment protects against unreasonable searches by law enforcement, and case law and legislation have followed to refine those restrictions; however, they are based on the sensibilities of a decidedly analog society that existed over 35 years ago.

These laws and cases considered how modern government collection techniques and other authorities related to the Constitution. The principles of those standards endure, but the specific restrictions that they impose on the government struggle for relevance against contemporary collection and analytical capabilities.

- Katz v. U.S. (1967), Smith v. Maryland (1979), and Title III of the Omnibus Crime Control and Safe Streets Act (1968) form the bedrock of these standards for law enforcement, which obligate the probable cause standard for electronic intercepts, define reasonable expectation of privacy, mandate "minimization" procedures that restrict government collection and retention of intercepted communications.
- Terry v. Ohio (1968) determined, "The Fourth Amendment right against unreasonable searches and seizures, made applicable to the States by the Fourteenth Amendment, 'protects people, not places,' and therefore applies as much to the citizen on the streets as well as at home or elsewhere."[104]
- The Foreign Intelligence Surveillance Act of 1978 and Executive Order 12333 (1981) distinguished law enforcement from the intelligence community, set unique restrictions upon intelligence operations, obligated intelligence use the "least intrusive means" for collecting intelligence, and defined when the broader collection authorities over "agents of a foreign power" applied.[105]

Smith determined that telephone number recording "pen registers" (i.e., metadata collection devices circa 1979) were reasonable because similar collection was part of the course of doing business at a telephone company. In the words of Justice Blackmun,

> When petitioner voluntarily conveyed numerical information to the phone company and "exposed" that information to its equipment in the normal course of business, he assumed the risk that the company would reveal the information to the police.[106]

The contemporary meaning of "assumed risk" has been obscured as customers forfeit a much greater volume of data to a company than they did in 1979. The courts and Congress have not determined how accessible data should be for the government when it is originally acquired by a corporation or unknowingly forfeited by its citizens.

---

[104] Terry v. Ohio 392 S. Ct. 1 (1968).

[105] Exec. Order No. 12333.

[106] Smith v. Maryland, 442 S. Ct. 735 (1979).

Regarding *Terry*, which defined boundaries for physical searches and seizures, these principles have not been defined for the digital era. The protections against reasonable searches and seizures apply to an individual "at home or elsewhere," but there is no clear stipulation about whether "elsewhere" includes data in a digital device, or on "the cloud."

The Foreign Intelligence Surveillance Act and Executive Order 12333 define an "agent of a foreign power," which enables more invasive collection against such powers. Conventional wisdom conflates terrorists with agents of a foreign power, as does the 2004 lone wolf amendment to FISA. Yet terrorism is an elusive definition, which is often defined outside of the courts.

The operative standard is a "reasonable expectation of privacy," wherein privacy is the primary concern. What this standard does not consider is what is "reasonable" in an era where data collection and analysis capabilities are far greater than they were at the time these rules were written? Is the reasonable standard changed with the force multiplier effects of cameras, data processing, and analytics that put a "virtual" cop at every corner? At what point is the greatly enhanced technological capability of government an encroachment on the Fourth Amendment? It is not difficult to imagine a moment when technical capacity for predictive and data mining tools will outpace case law and public sensibilities of what data is in bounds for analysis and what is not.

E. HYPER-VIGILANCE, CONFIRMATION BIAS, AND THE CONTAGION OF PREJUDICE

With the onset of a broadly networked system to analyze threats, there is a risk that the constant pulse of threat-related information to laypersons outside of the security-related professions will cause them to become inordinately security conscious. An extreme but ominous extension of this trend would be the emergence of a security state that is reinforced by a steady dose of threat related information.

In their research on risk, Kahnneman and Tversky note that humans have a tendency to detect false patterns in randomness and randomness in patterns.[107] It is

[107] Kahneman, *Thinking Fast and Slow*, 76.

possible that analysts who view a steady stream of threat synopses could also perceive false patterns. Those biases could emerge spontaneously, or could reinforce existing biases, what the researchers call *confirmation bias*.

Examination of "fake news" and investigation of the potential exploitation of latent biases in American society by a foreign power provide a tangible example of how this trend can occur. It also exemplifies how information, good and bad alike, can propagate through an effective network. Just as ignition requires heat, fuel, and oxygen, the emergence of a broad social shift requires a compelling narrative, the means to transmit it, and a willing society—removal of one component will stop the reaction.

F. CONSIDERING THE NET EFFECTS OF DEPLOYMENT

It is difficult to forecast whether deployment of a supernetwork would be a net benefit or loss to the greater public. Contemplating this question is reminiscent of other nascent technologies, which solve a particular problem but yield unintended consequences. The potential risks of a supernetwork do not necessarily preclude it deployment; however, they should be recognized and considered honestly. A supernetwork, no matter its predictive accuracy, is still a forecast, with a same potential for false positives and false negatives that any forecast carries. It is a timeworn expression in forecasting that correlation should not be confused with causation. This is analogous to the relationship young investigators learn between circumstantial evidence and guilt: one may be indicative of the other but not necessarily.

VI. CONCLUSION

Considering the limited number of participants in the superforecasting survey, it can only be speculated here why the threat analysis of this group was superior to actual investigators. The most apparent explanation is that the wide range of backgrounds lends itself to more thorough analysis. This may be true, but there are already multiagency or multidisciplinary teams, such as task forces, that should yield a similar result if that was the strongest factor. It may be that the subjects, unlike members of a task force, are unburdened from the conventions and constraints of being in an organization. Unburdened by groupthink, the analysts are free to provide better analysis.

Superforecasting analogizes biased decision making by referring to the "green tinted glasses" in *The Wizard of Oz*, wherein all citizens wore tinted glasses within the Emerald City to accentuate its "greenness" but at the expense of seeing anything else.[108] It is possible that investigators wear green eyeshades. With a more particular expertise and mission, an investigator might only see the "green" of a threat, while missing other warning signals. Conversely, an investigator's glasses might be "red"—the opposite of green—wherein a steady dose of false alarms leads the investigator to assume that all threats are negative. In this case, the subtle shading of the threat grows invisible, and the investigator recognizes only the extremely prominent details. The results of the Monte Carlo experiment demonstrate that neither scenario—the green being the *investigate everything* model and the red being the *rapidly diminishing*—produces efficient results.

Considering the result of the Monte Carlo models and prototype superforecasting experiment together encourages further examination into the art and science of investigative decision making and analysis. The scope of both was limited and neither can be judged as conclusive; however, the results of both are counterintuitive. The Monte Carlo models demonstrate how different decision-making models may yield marginal improvements in detection, but when applied to a "low-probability / high consequence" phenomenon like lone actor attacks, will do so with rapidly increasing exposure to false

[108] Tetlock and Gardner, *Superforecasting*, 70–71.

positive decisions. The superforecasting experiment indicates that a diverse forum of analysts may be better capable of detecting the signals of emerging violence than a single decision maker or investigative agency.

It is possible that implementing a superforecasting network may enable an investigative organization to calibrate its decision making while reducing the exposure to false positive risk indicated in the Monte Carlo models. Aside from the improved accuracy of detection, an analytical forum that is representative of the community that is being policed may diffuse the consequences of false positives, as analysts could factor their constituent concerns, cultural sensitivities, and civil liberties into their analysis.

At the same time, a networked forum may be vulnerable to the contagion of certain biases, which would amplify poor decision-making. The following section will contemplate how an analytical network could be implemented, how and why it may improve lone actor investigations, and the potential risks from its implementation.

In the final weeks while this thesis was written, three additional lone actor attacks occurred in the United States. The earliest, the mass shooting in Las Vegas in October 2017, was included in the Monte Carlo modeling but not in the survey. The other two, a vehicle attack in New York City (late October 2017), and a mass shooting in San Antonio (early November 2017), occurred too late for inclusion in the research.

The Las Vegas attack is an apt example of the randomness of lone actor attacks and stands in contrast to the Fort Hood attack, which was the topic of this paper's introduction. The investigation of the Las Vegas attacker is ongoing, and our understanding of what motivated the attack remains uncertain. Unlike with the attacker at Fort Hood, the behavioral indicators that the Las Vegas attacker exhibited were available to few, did not appear to be available to law enforcement for consideration, and only seem indicative of violence in hindsight.

It is in witnessing tragedies like Las Vegas and the experience of this research, I am more circumspect about what I characterized as "missed opportunities" of law enforcement agencies when the research of this thesis began. In the face of randomness and the realization that even the most effective method of analysis could not detect the

Las Vegas attack, I return to a favored axiom of my father, an earlier practitioner in my field, who used to say “there is no such thing as perfect security.”

However, I do remain hopeful for a modicum of improvement. Lone actor attacks appear infrequent when compared to other crimes and tragic events, yet seem all too frequent as they are witnessed nearly two out of every three months over the past several years. As caretakers of the public security, practitioners should strive to find better ways to detect these events and reduce their frequency. At the same time, as sworn defenders of the Constitution, practitioners should achieve those gains without the expense of undermining the tenets the Constitution delineates. Involvement of a broad forum of analysts in assessing potential threats may or may not be effective, but it is democratic.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. IDEAS FOR FURTHER RESEARCH AND OPEN QUESTIONS

In conducting the research and writing for this thesis, I found that in spite of my status as a practitioner in threat analysis, I had a lot to learn about the science of decision making generally, and more specifically, how it is applied to threat investigations. This led to a very meandering path toward conclusion of this effort, which I hope is not too apparent in the body of this paper but will likely be obvious in the ensuing paragraphs. Over the course of this process I did a lot of free associative writing over the summer in anticipation of writing the thesis. Some of it was more germane and found its way into the main chapters, some was not, and some sort of fell in the middle. With apologies for the free form nature of the way these sections are presented, here is what may be called the "director's cut" of ideas and unresolved questions that were always in the background, but I regulated here for me to remember and return to later.

The *Superposition* of Threats—Schrödinger's Lone Wolf

In the early twentieth century, physicist Erwin Schrödinger used a thought experiment to demonstrate how the behavior of subatomic particles could be true in one hand, and untrue more generally—particularly toward larger physical phenomena. This paradox is that a quantum particle could occupy two states simultaneously; this was later affirmed through the theory's underlying math and several experiments, yet such a physical *superposition* would be considered bizarre to the naked eye.[109] For instance, I cannot be in Rome and Monterey at the same time.

Schrödinger's experiment described a hypothetical scenario in which a cat was inside a box, and within the box was a device that may or may not kill the cat. The device had a trigger that was purely automatic and random, meaning that an observer outside the box may know the probability of whether the trigger had actually engaged and eventually killed the cat but could not know with certainty whether the cat was dead unless the box

[109] Ismael Jenann, "Quantum Mechanics," in *Stanford Encyclopedia of Philosophy*, spring 2015 ed., https://plato.stanford.edu/archives/spr2015/entries/qm/.

was opened. Absent the observation, which imposes one essence or the other on the cat, the cat is both alive and dead simultaneously.[110]

Such a dual state as alive and dead may be an affront to common sense, but quantum physics accepts such a dual state as true. Investigators must apply the same logic to threat investigations. A subject for investigation may be a physical threat, or not. The essence of the threat cannot be defined until one of two things have happened—either the subject attacks, or enough time has elapsed whereby the subject does not attack, and a reasonable observer can consider the subject to be safe.

Extending this analogy one step further demonstrates the confounding nature of threat investigations. Once the attack has occurred, but no earlier, the subject is definitely a threat; however, the subject who does not attack always carries a potential to do so at some point in the future. The superposition in the latter case is perpetual. It is also difficult to determine whether the benign state of a subject is the result of his or her never carrying the intention to attack, or a result of the imposition of the investigator into his or her life. This is a measurement effect that should be contemplated in future research on threat assessment, and particularly if the superforecasting experiment is expanded. The Brier score relies on a binary "it happened/it did not happen" outcome; however, there is never a pure "did not happen" scenario with threats.

Gamifying Analysis to Maintain Supernetwork Participation

An explanation for why the subjects in the experiment of this research produced superior analysis may be found in the way I presented the questions to them as a game-like exercise. *Superforecasting* describes how a broad, networked assembly of analysts triumphs over professionals. Underlying this story is an examination of the ways cognitive biases can lead an individual or group from good decisions. However, underlying the whole Tetlock's experiment was a tournament, a game.

Gamifying is the use of game-like elements for endeavors that typically are not competitive.[111] Gamified systems are used by social media sites, marketers, and

[110] James Robert Brown, and Yiftach Fehige, "Thought Experiments," in *Stanford Encyclopedia of Philosophy*, summer 2017 ed., https://plato.stanford.edu/archives/sum2017/entries/thought-experiment/.

elsewhere, as an effective means to captivate and hold participants. It may be that a gamified approach to threat analysis may encourage more sustained attention, better collaboration, and more diverse participation.

Feeding the Network

What phenomena spur growth and divergence in an analytical network? What causes pruning of the ineffective parts of the network? Does this mimic neural expansion and pruning?

Other Questions about Networks

How would a distributed model affect espirit de corps? How would it affect collaboration? Would there be an ingroup-outgroup dynamic?

What about cultural differences? Would a distributed approach be better positioned to detect trends in a diverse environment?

Concerning the previous question, what about international systems? It seems that Interpol and Europol are less centralized. Both are a clearinghouse for information. This might be a step toward integration, but it might also be the best example of a networked approach that is available. What are the legal strictures for Europeans? Is their access greater than, or less than, that of the United States? Does this and their diversity dictate a networked approach? What about media richness? Does the remote perspective of networked analysts improve or diminish their comprehension of a threat?

Marketing, Epidemiology, and Countering Violent Extremism

Marketing guru Seth Godin describes *otaku*, which is the obsessive devotion to a particular thing. He describes how important it is to engage *otaku* as a marketing strategy. If *otaku* is properly stimulated, then that idea will go viral.[112]

---

[111] Steffen P. Walz and Sebastian Deterdin "An Introduction to the Gameful World," in *The Gameful World: Approaches, Issues, Applications,* ed. Steffen P. Walz and Sebastian Deterdin (Cambridge: MIT Press, 2014), 1–2.

[112] Seth Godin, "How to Get Your Ideas to Spread," TED, February 2003, https://www.ted.com/talks/seth_godin_on_sliced_bread#t-676376.

Taking the idea of "going viral" literally, epidemiologists identify certain members of a population as critical when trying to interdict the spread of a virus. When inoculating an entire population is impossible, it is almost as effective to identify these prominent members who, if they are infected with a disease, will spread it wider and more rapidly than others.

Some social scientists have observed that violence propagates through a social network the way a popular marketing trend or an infectious disease does.[113] Similarly, corrosive social ideas can spread as efficiently through a network as any other trend.

What can we learn from these ideas? What would marketers or epidemiologists say about the several approaches to countering violent extremism that target at the fringes of a social network? These strategies in marketing or epidemiology appear to be doomed to failure. Are the various countering violent extremism strategies that the U.S. government employs doomed to the same fate?

It may be that our counter narratives, our interventions, and our broader strategy for counterterrorism needs to focus on the *otaku* in the culture from which the threat emerges. If terrorists are essentially lethal "fan-boys" then maybe something that is more compelling will reintegrate them into their host society. This does not imply that an individual who appears resolved to attack should be ignored; this would be as foolish as leaving someone who has caught a disease to die if they are not one of the critical nodes in their social network. However, remaining in a constant hunt for individual threats is equally foolish and will certainly strain limited resources.

Observing from an organizational perspective, strategies to fight an epidemic that do not integrate several different disciplines tend to fail. Epidemics tend to emerge from a miasma of poverty, a diminished public health infrastructure, and cultural practices that enable the spread of the pathogen. A singular focus on the etiology of the disease, or the society from which the disease emerges, only addresses part of the problem. The same

[113] Andrew V. Papachristos et al., "The Company You Keep? The Spillover Effects of Gang Membership on Individual Gunshot Victimization in a Co-offending Network," *Criminology* 53, no. 4 (2015): 624–649, doi: 10.1111/1745-9125.12091.

goes for a strategy of quarantine, which in a networked world will only contain a problem for so long.

If it has not occurred yet, maybe the counterterrorism (or counterviolence) apparatus would benefit from studying what has worked with epidemiology. What has worked to arrest the emergence of an epidemic may also work with the growth of a violent ideology. In turn, what has failed in one field may portend a failure of a similar strategy in the other.

Maybe we are approaching the whole thing too literally. Maybe we are too focused on the pathology that drives the killer, the ideology that inspires him, or the global-scaled forces that propel those ideas. The fact that the idea is articulated or justified on global terms does not mean that the attacker operates with a global agenda. On the opposite end, the anxieties extant in the attacker may not be the sole precursor to violence.

Google Trends and Sentiment Analysis

Seth Stephens-Davidovitz published research that correlates Google search data to social events.[114] This strikes me as a crude form of sentiment analysis. Maybe there is a correlation that can be found within Google data that will targeted violence.

Why:

- Stephens-Davidovitz's research seems to argue that this is a reflection of our true selves—more than surveys or personal interviews.[115] If Google searches are the window into our souls, then maybe this dark corner of them can be revealed.
- This is true meta-analysis. It may be enough to scrape the top layer of social media data to get results that are predictive enough.
- OR—It may contextualize personal interviews that occur with suspects.
- It may portend seismic shifts that could trigger violence.

[114] Seth Stephens-Davidovitz, *Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us about Who We Really Are* (New York: HarperCollins, 2017), 9.

[115] Ibid., 106.

    - But—does this agree with NTAC research? It indicates that a personal event portends violence, more so than outside influence.
- If ISIS is finding and manipulating potential violent actors, then why are the police so unsuccessful?

Why not:

- This is sentiment analysis but done crudely.
- Sentiment analysis requires foreknowledge of the sentiment, and how it is reflected in words. Some attackers use language that is incoherent to an outside listener, but has deep meaning to the assailant. For example: Loughner repeatedly spoke of the meaning of math.
- First Amendment protections.

Google Trends Analysis of lone actor phenomena—correlate lone actor search activity with wider search activity to see if behavior is "triggered' by particular events.

Salience in investigations—What makes a case more prominent? Why is terrorism salient to the members of public? Why is their risk perception so distorted?

Terrorism captivates a population. Positioning it in the family of "asymmetric warfare" alludes to the out scale effect of terrorist violence. For example—in the summer of 2017 a car careened into Times Square and killed three people but was later determined to be an accident. Two weeks later, a van deliberately ran into six pedestrians on London Bridge, killing six. Both are tragic, but only one was characterized as terrorism—London. Once the New York attack was defined as a tragic accident, the world moved on, but the public's attention to London endured for several days.

There are many theories of why we react to terrorism in such a strong way, in spite of the low probability that we will be victims of it. For one, people are poor judges of risk; what they fear the most does not always accord with the probability. Beyond terrorism, people perceive shark attacks as a greater risk than drowning; violent crime more than vehicle accidents; or continuing with vehicles, dwell on the few incidents in which self-driven vehicles fail while on the day those incidents happen, an average of 100 people die across the nation from human error behind the wheel without mention.

Also, is there a "multiplier" for this effect? Can I quantify two similar incidents—one an act of terrorism and the other not—and determine how much terrorism amplifies

coverage by the media, or perceived fear in the public? Would a treatment of Google search activity for two such events and news coverage get us to this multiplier?

Can this technique also measure resilience? For example, the October 31, 2017 vehicle attack in New York City received intensive coverage; it was the largest terrorist attack in New York since the September 11, 2017 attacks. It was also committed in the shadow of the new World Trade Center. Yet the mayor of New York City emphasized the resilience of New Yorkers, who moved on to their Halloween activities that night. Just as the construction of the new World Trade Center is a metaphorical example of resilience, the return to normalcy on Halloween night may be a literal an immediate example of the same.

Google trends may illuminate this. In its "Google Insights" page for June 6, 2017, Google tallied the relative search interest for the London Bridge terrorism attacks that occurred on June 3. The search interest for this topic lasted 31 hours, peaking on the hour of the attack and diminishing to 10 percent over a day later. This incident accumulated over 28,464 news articles. For the Orlando shooting, the Google interest in the story diminished by 90 percent about 14 hours after the attack.

"A-B" Testing Potential and the Study of Salience in Violent Events

A-B testing is a common practice in online marketing, wherein advertising messages presented to different consumers is altered slightly and their reaction is quantified. Such a technique could be used to study what aspects of threat-related information are most salient to investigators, or supernetworked analysts.

Tribalism and the Analysis of Threats and Pre-conceptions

Robert Sapolsky wrote that the human brain makes constant microbiological adjustments at any minute, which can trigger different biases.[116] In his book *Behave*, Sapolsky takes a biological explanation for phenomena as wide ranging as sociology, social psychology, political science, and other aspects of human behavior. If there are

[116] Robert M Sapolsky, *Behave: The Biology of Humans at our Best and Worst* (New York: Penguin, 2017).

physiological predispositions to cooperation, are there ways we can stimulate them to get an intended result? Are the methods we are using offensive to these hardwired triggers?

As for multinational organizations, such as Europol, how can social and national divides be differentiated from organizational effects?

Specialization

The use of a broad multidisciplinary network for analysis requires participants to act as generalists while they analyze threats. In *Behave*, Sapolosky describes organic specialization: Specialized, different organisms have different relative strengths and weaknesses that are the product of evolution.[117] Do members of complex organizations naturally specialize in the same way? On the other hand—stem cells carry the potential to become any specialized cell. Are we more like stem cells, or specialized cells?

Digital Jurisprudence—Civil Rights in the Digital Age

This is not a new idea, but one that returned throughout the writing of this thesis, and the duration of this master's program. Just as we appear to be emerging into what is sometimes called a new Industrial Revolution, where the assumptions that guided efficient corporate organization, labor and management relations, trade, and other economic theories; an analogous transformation of our social interactions may be afoot.

We need to consider the implications of these changes on civil rights and freedom generally. Any innovations that are deployed by government that may infringe on those rights should be included in this discussion, including the implementation of an analytical network like the one considered in this thesis.

Industrial Organization

The economics of imperfect competition defines why, in some markets, organizations compete while others will behave in oligopolistic ways. In this form of cooperation, firms will agree to forgo competition out of self-interest and to retain market dominance.

[117] Ibid., 7–9.

Are investigative agencies monopolistic or oligopolistic? Why do agencies cooperate at times and not in others? Can this be explained through an industrial organization framework? If so, then what is the benefit for which they are competing? Is it a broader social good? If so, then why not cooperate? If it is something more banal (like prestige) then is the propensity to cooperate more situational? Are task forces like joint ventures? Do they follow the rules of cartels?

Auftragstaktik and Government Decision Making

James Q Wilson's *Bureaucracy*, describes *Auftragstaktik*, which is the German military philosophy that emphasizes tactical initiative at the lowest possible rank.[118] It contrasts the philosophy of many other armies, including the U.S. Army, on command-and-control, which requires a constant reach back to high commanders who were several ranks above and many miles away from the actual fighting. American tactical leaders are given detailed instructions on how an objective should be achieved. In contrast, *Auftragstaktik* gives tactical leaders the objective but leaves the details of how to achieve it to those leaders.

How does this translate to threat analysis? Are there examples of either in the investigation of threats? Traditionally, sole investigators and remote field investigative units like task forces have the initiative to follow leads in a way they see fit. On another, the failure to detect some threats has led to a call by critics to centralize and harmonize command and control of broadly-distributed investigative units.

Does this demonstrate the divide between tactics and strategy? Maybe institutional imperatives, such as arrests and other success stories, flow through to the tactical level, thereby leaving investigators compelled to seek visible signs of success. It is difficult to measure success without these dramatic conclusions, and the failures are extremely prominent.

---

[118] James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (New York: Perseus Books, 1989), 3–13.

Analysis of Threats and Pre-conceptions

Consider the emergence of a threat presented by an individual as the intersection between a person's solitary motivations, the norms of society. If context colors behavior, that context is shaped by culture, which is as broad as national and religious identity, and as discrete as mother to child. A remote analysis of that individual's behavior can be blind to the contours of cultural influences. How broad and varied does analysis have to be to gain awareness of context?

Prospect Theory and Terrorist Recruitment

Is recruitment of a single actor a prospect theory problem? The risk versus rewards of recruitment are very different for vetting a terrorist aspirant than it is for investigating one. Said differently, ISIS can reject an applicant who means it no harm, and it is only an opportunity cost. When the police identify a suspect as a threat when she or he is not, the costs are great (measured in wasted resources, in liability, and in deleterious effects in the community). A second cost is when a threat is erroneously identified as benign; however, the rarity of these events makes it a "safer bet."

The Pitfalls of Predictive Analytics and Reasonable Expectations

Using predictive tools can be a dangerous exercise when placed in the hands of those who are not aware of the limitations of the practice. While the expectation is a perfect forecast, being able to gauge broader trends that are more productive than the mean is sufficient.

Isn't this what we are trying to achieve with good policy? Are we simply trying to reach a decision that is within one or two standard deviation's accurate rather than pinpoint accuracy? Are we simply trying to beat the coin toss decision? How does this translate to threat assessment, where we are looking at individuals in a very precise scenario?

APPENDIX B. MODEL SELECTION AND HYPOTHESIS TESTING FOR THE TIME SERIES ANALYSIS AND MONTE CARLO MODELS

In Chapter III of this thesis, I described how I collected data on lone actor violence in the United States between 1982 and 2017. In that chapter, I also explain three methods I used to analyze that data. These methods were time series autocorrelation analysis, a "runs test," and a Monte Carlo model. This appendix elaborates on why I used these three techniques, and more specifically, why I made decisions in each of the models to analyze the data, represent the data, or both.

Statistical model building masquerades as a purely objective undertaking; however, it is as much art as science. The art is in found in data selection, and in choosing how to analyze the data one it is selected. Like bakers and carpenters, quantitative analysts are reminded of the hazards of overworking their material. In statistics, this is usually summarized by quoting "Occam's razor," which emphasizes that "descriptions be kept as simple as possible until proved inadequate."[119] For this reason, I left the data, which appears at the end of this appendix, as untouched as possible. In analyzing that data, I used basic tests for pattern detection assuming that if a pattern emerged, then that may justify rejection of the hypothesis that lone actor violence, over time, was random.

Time Series Analysis

I first determined whether there was a pattern to be discovered in these attacks, based on earlier, or "lagged," data points.[120] This is based on the assumption that detection of a more complex pattern from other variables was unlikely, given the multiplicity of motives and affiliations (if any) of attackers. Also, lone actor attacks are sudden and unexpected; therefore, I assumed that any detection of these attacks was

[119] Maurice G. Kendall and William R. Buckland, *A Dictionary of Statistical Terms*, quoted in Damodar Gujarati, *Basic Econometrics* (New York: McGraw-Hill, 1988), 353–354.

[120] Gujarati, *Basic Econometrics*, 505–512.

lagged, rather than "real-time." Arguably, any explanatory data that is not lagged in this context is too late, since the attack has occurred.

Autocorrelation is defined as the "correlation between members of series of observations ordered in time or space."[121] This statistic was used to make an initial assessment of any pattern within the time series data used for this thesis. If a pattern between an attack and lagged attacks existed, there would be a statistically significant autocorrelation between the time that attack occurred, and a point in time before it occurred. For this series, days when attacks occurred were given a value of one, and days without an attack were given a value of zero; therefore, if an attack, or non-attack, at time *t* depended repeatedly on the occurrence of the same outcome at time *t-x* (where x equals the length of the lag), then the autocorrelation would be 1. If there was an opposite relationship (i.e., an attack at time *t* depended on a non-attack at time *t-x*) then the outcome would be -1. If there is no relationship, the statistic is close to zero.

To determine the autocorrelations, I analyzed the series of attacks using a time series for every day between January 1, 1982 and October 1, 2017 with the JMP Pro 12.2.0 statistical program. Using the one for dates with attack, zero for dates with attack method described in the previous paragraph, the program calculated correlations existed between a data and lags up to 365 days prior. For attacks, there were no statistically significant correlations, as indicated by the correlation coefficients themselves and corresponding hypothesis test statistics that are generated by the program.

If there was any autocorrelation detected, then the next step would be to determine an appropriate time-series model where an equation would yield estimates that best fit the existing data; however, given that there was no correlation within the time series data and lagged values, this was not necessary.

I repeated this technique for corresponding latitude and longitude values to see if a spatial relationship between the site of an attack and an attack at a lagged point in time as far as 25 attacks prior. There was a weak correlation between the latitude data and lags

[121] James Roy Newman ed., *The World of Mathematics* (New York: Simon and Schuster: 1956), 1247, quoted in Gujarati, *Basic Econometrics*, 34.

of *t-1* and *t-2*; however, these were still fairly weak. Also, considering the statistic would only merit further examination if there was a corresponding correlation between the same lags of longitudinal data, which would then offer the possibility of a predictive model on two dimensions. If there is a relationship between the latitude of an attack at time *t* and previous attacks one or two times prior, but only that relationship, it would have the effect of predicting an attack will happen in Baltimore, Cincinnati, Salt Lake City or Reno, because they share a latitude that is similar, but not knowing which one because the longitudinal data (east to west) is random. For those reasons, it was generally asserted in the thesis that the geospatial data of attacks over time is random.

Use of a Gamma Distribution to Estimate the Random Numbers for Casualties within the Monte Carlo Model

I describe in Chapter III the challenge of determining appropriate random numbers for the Monte Carlo model. I built this model using Microsoft Excel, which will yield any number between zero and one with equal probability. I evaluated the frequency of casualty rates in lone actor attacks, and recognized that this data is neither equally distributed, like the random numbers, nor normally distributed, where most of the attacks would result in casualties close to the mean value of all attacks, and taper gradually in numbers greater than or less than the mean at equivalent rates. Instead, the data appeared to be *skewed*, which means that the distribution of each casualty rate from one to progressively rising numbers is asymmetrical.[122] If I applied either the default random number generator in Excel, or adjusted the random numbers to follow a normal distribution, the simulated casualty rates would be to frequent for values, and to infrequent in others. The actual data resembled an exponential function, where most of the attacks were five or fewer, but occasionally yielded greater numbers, and very occasional "black swan" attacks where more than twenty died from the attack.[123]

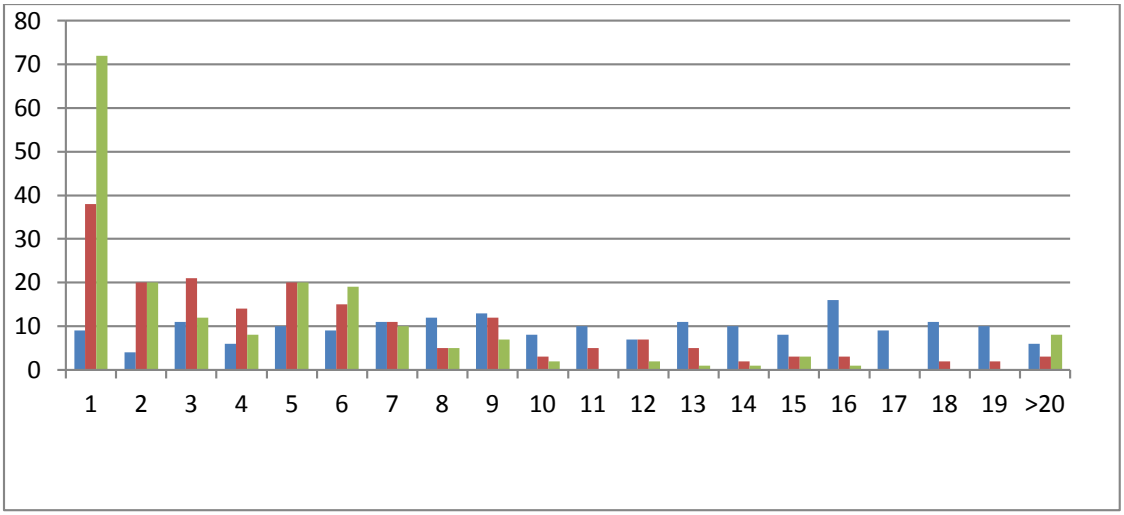
---

[122] National Institute of Standards and Technology, "Measures of Skewness and Kurtosis," in *Engineering Statistics Handbook* [online], last updated October 30, 2013, http://www.itl.nist.gov/div898/handbook/eda/section3/eda35b.htm.

[123] It should be noted that such large-scale attacks have been growing in frequency in recent years and are arguably less "black swan" events than they once were.

To yield simulation data that best fit the actual data, I tried a gamma distribution that resembled the shape of the data. The parameters were chosen based on a naked-eye estimate of different gamma distributions, and then iterated in the model until the simulation yielded data that best resembled the actual data.[124] Figure 1 illustrates the difference between frequencies of casualty rates that were yielded by the default random number generator (the left bars, colored in blue), the gamma distributed data (the center bars, in red), and the actual data (the right bars, in green).

Figure 1. Frequency Comparisons of Simulated Casualty Rates from Random Numbers, Random Numbers that are Gamma Distributed, and Actual Casualty Rates



Note: Frequency rates appear on the vertical (Y) axis, and casualty rates appear on the horizontal (X) axis

To further validate the fit of the gamma model, a Chi-squared goodness of fit test was used.[125] This test often, but not always, yielded values that indicated that the gamma distribution was, within 95 percent certainty, the best fit for the actual data.

[124] National Institute of Standards and Technology, "Gamma Distribution," in *Engineering Statistics Handbook* [online], last updated October 30, 2013, http://www.itl.nist.gov/div898/handbook/eda/section3/eda366b.htm.

[125] National Institute of Standards and Technology, "Chi-Squared Goodness of Fit Test," in *Engineering Statistics Handbook* [online], last updated October 30, 2013, http://www.itl.nist.gov/div898/handbook/eda/section3/eda35f.htm.

Table 16. Lone Actor Attacks in the United States

DATE	CITY	STATE	DEATHS	INJURIES	LAT.	LONG.
1/28/1982	Los Angeles	California	1	0	34.05349	-118.24532
4/5/1982	New York City	New York	1	8	40.71278	-74.005941
5/4/1982	Somerville	Massachusetts	1	0	42.38668	-71.098264
5/5/1982	Nashville	Tennessee	1	1	36.16778	-86.778365
5/16/1982	San Juan	Puerto Rico	1	3	18.46617	-66.106654
5/18/1982	San Juan	Puerto Rico	1	2	18.46617	-66.106654
5/22/1982	Stamford	Connecticut	1	0	41.05182	-73.542234
8/2/1982	Houston	Texas	1	0	29.76045	-95.369784
8/11/1982	Honolulu	Hawaii	1	15	21.30694	-157.85833
8/20/1982	Miami	Florida	8	3	25.79649	-80.226683
12/8/1982	Washington	District of Columbia	1	0	38.89037	-77.031959
2/13/1983	Medina	North Dakota	2	1	46.89426	-99.299994
8/8/1983	Canton	Michigan	1	0	42.30865	-83.482158
8/9/1983	Detroit	Michigan	2	0	42.33169	-83.047924
9/21/1983	New York City	New York	1	0	40.71278	-74.005941
1/27/1984	Dallas	Texas	1	0	32.77816	-96.795404
5/28/1984	San Francisco	California	1	1	37.77713	-122.41964
6/18/1984	Denver	Colorado	1	0	39.74015	-104.94841
6/29/1984	Dallas	Texas	6	1	32.78011	-96.800008

DATE	CITY	STATE	DEATHS	INJURIES	LAT.	LONG.
7/18/1984	San Ysidro	California	22	19	32.552	-117.04308
6/2/1985	Cleveland	Ohio	1	0	41.50437	-81.690459
10/11/1985	Santa Ana	California	1	0	33.74557	-117.86783
12/11/1985	Sacramento	California	1	0	38.57907	-121.49101
4/29/1986	San Juan	Puerto Rico	1	0	18.46617	-66.106654
8/20/1986	Edmond	Oklahoma	15	6	35.6672	-97.42937
4/23/1987	Palm Bay	Florida	6	14	28.03319	-80.64297
8/7/1987	Garden Grove	California	1	0	33.77607	-117.93616
2/16/1988	Sunnyvale	California	7	4	37.36883	-122.03635
6/20/1988	Mayaguez	Puerto Rico	1	1	18.20132	-67.145125
1/17/1989	Stockton	California	6	29	37.9577	-121.29078
9/14/1989	Louisville	Kentucky	9	12	38.25424	-85.759407
11/22/1989	Seven Corners	Virginia	1	0	38.86078	-77.143347
12/16/1989	Mountain Brook	Alabama	1	1	33.50212	-86.755509
12/18/1989	Savannah	Georgia	1	0	32.08078	-81.090719
1/30/1990	Tucson	Arizona	1	0	32.22223	-110.92575
2/8/1990	Knoxville	Tennessee	1	0	36.01258	-84.016279
6/18/1990	Jacksonville	Florida	10	4	30.33218	-81.655651
9/22/1990	Bailey’s Crossroads	Virginia	2	0	38.84803	-77.12916
11/5/1990	New York City	New York	1	0	40.71278	-74.005941
2/18/1991	Miami	Florida	1	0	25.76437	-80.201529
3/15/1991	Miami	Florida	1	0	25.76437	-80.201529

DATE	CITY	STATE	DEATHS	INJURIES	LAT.	LONG.
10/16/1991	Killeen	Texas	24	20	31.11712	-97.727796
11/1/1991	Iowa City	Iowa	6	1	41.66069	-91.530221
11/14/1991	Royal Oak	Michigan	5	5	42.48948	-83.144649
2/18/1992	Boston	Massachusetts	1	0	42.35864	-71.056699
3/11/1992	New York City	New York	1	0	40.71278	-74.005941
5/1/1992	Olivehurst	California	4	10	39.07869	-121.54758
10/15/1992	Watkins Glen	New York	5	0	42.38106	-76.870578
7/1/1993	San Francisco	California	9	6	37.77896	-122.4192
8/6/1993	Fayetteville	North Carolina	4	8	35.05299	-78.878706
12/7/1993	New York City	New York	6	19	40.72677	-73.634296
12/14/1993	Garden City	Aurora, Colorado	4	1	39.75471	-104.83587
3/1/1994	New York City	New York	1	3	40.71278	-74.005941
3/9/1994	Miami	Florida	1	0	25.76437	-80.201529
5/29/1994	New York City	New York	1	0	40.71278	-74.005941
6/20/1994	Fairchild Air Force Base	Washington	5	23	47.61864	-117.64836
7/29/1994	Pensacola	Florida	2	1	30.42085	-87.217239
9/12/1994	Washington	District of Columbia	1	0	38.89037	-77.031959
10/16/1994	Lubbock	Texas	1	0	33.57786	-101.85481
12/10/1994	Caldwell	New Jersey	1	0	40.84144	-74.276645
12/30/1994	Brookline	Massachusetts	1	3	42.33178	-71.121182
4/3/1995	Corpus Christi	Texas	6	0	27.82371	-97.417398

DATE	CITY	STATE	DEATHS	INJURIES	LAT.	LONG.
4/19/1995	Oklahoma City	Oklahoma	168	650	35.47202	-97.520354
4/24/1995	Sacramento	California	1	0	38.57907	-121.49101
10/9/1995	Hyder	Arizona	1	78	33.01499	-113.35217
1/23/1996	Miami	Florida	1	0	25.76437	-80.201529
2/9/1996	Fort Lauderdale	Florida	6	1	26.12231	-80.143379
7/27/1996	Atlanta	Georgia	1	110	33.74832	-84.391109
2/23/1997	New York City	New York	1	6	40.71278	-74.005941
9/15/1997	Aiken	South Carolina	4	3	33.55986	-81.721952
12/18/1997	Orange	California	5	2	33.78779	-117.85311
12/30/1997	Oakwood	Illinois	1	0	40.11411	-87.778197
1/29/1998	Birmingham	Alabama	1	1	33.5203	-86.811504
3/6/1998	Newington	Connecticut	5	1	41.68563	-72.729838
3/24/1998	Jonesboro	Arkansas	5	10	35.82099	-90.668261
5/21/1998	Springfield	Oregon	4	25	44.04624	-123.02203
7/24/1998	Washington	District of Columbia	2	1	38.89037	-77.031959
10/23/1998	Amherst	New York	1	0	42.97837	-78.799942
4/20/1999	Littleton	Colorado	15	24	39.61691	-105.01452
7/1/1999	Redding	California	2	0	40.58752	-122.39293
7/2/1999	Skokie	Illinois	1	0	42.02634	-87.755679
7/4/1999	Bloomington	Indiana	2	0	39.16402	-86.509869
7/29/1999	Atlanta	Georgia	9	13	33.7491	-84.390185
9/15/1999	Fort Worth	Texas	8	7	32.6934	-97.470671

DATE	CITY	STATE	DEATHS	INJURIES	LAT.	LONG.
11/2/1999	Honolulu	Hawaii	7	0	21.32551	-157.84731
12/30/1999	Tampa	Florida	5	3	27.94776	-82.458444
12/26/2000	Wakefield	Massachusetts	7	0	42.50648	-71.072831
2/5/2001	Melrose Park	Illinois	5	4	41.90059	-87.856728
10/2/2001	Boca Raton	Florida	1	5	26.36831	-80.128932
10/9/2001	Washington	District of Columbia	2	1	38.89037	-77.031959
10/15/2001	Washington	District of Columbia	2	6	38.89037	-77.031959
10/29/2001	New York City	New York	1	0	40.71278	-74.005941
11/14/2001	Oxford	Connecticut	1	0	41.43977	-73.126816
1/5/2002	Tampa	Florida	1	0	27.94735	-82.45875
7/4/2002	Los Angeles	California	3	4	34.05349	-118.24532
7/8/2003	Meridian	Mississippi	7	8	32.37608	-88.68978
12/8/2004	Columbus	Ohio	5	7	39.96226	-83.000707
3/12/2005	Brookfield	Wisconsin	7	4	43.06057	-88.106479
3/21/2005	Red Lake	Minnesota	10	5	47.87635	-95.01694
1/30/2006	Goleta	California	8	0	34.43628	-119.87144
3/25/2006	Seattle	Washington	7	2	47.6229	-122.3165
7/28/2006	Seattle	Washington	1	5	47.60356	-122.32944
10/2/2006	Lancaster County	Pennsylvania	6	5	39.9589	-76.0806
2/12/2007	Salt Lake City	Utah	6	4	40.76065	-111.89109
4/16/2007	Blacksburg	Virginia	32	23	37.22957	-80.413939
10/7/2007	Crandon	Wisconsin	6	1	45.57191	-88.902892

DATE	CITY	STATE	DEATHS	INJURIES	LAT.	LONG.
12/5/2007	Omaha	Nebraska	9	4	41.25873	-95.937873
2/7/2008	Kirkwood	Missouri	6	2	38.58339	-90.406785
2/14/2008	DeKalb	Illinois	5	21	41.92947	-88.750365
6/25/2008	Henderson	Kentucky	6	1	37.76721	-87.557374
7/27/2008	Knoxville	Tennessee	2	7	35.95176	-83.952337
3/29/2009	Carthage	North Carolina	8	3	35.3458	-79.417054
4/3/2009	Binghamton	New York	14	4	42.09869	-75.917974
5/30/2009	Arivaca	Arizona	2	1	31.57734	-111.33145
5/31/2009	Wichita	Kansas	1	0	37.68698	-97.335579
6/1/2009	Little Rock	Arkansas	1	1	34.75712	-92.380745
6/10/2009	Washington	District of Columbia	1		38.88671	-77.032607
11/5/2009	Killeen	Texas	13	32	31.13	-97.78
11/29/2009	Parkland	Washington	4	1	47.15585	-122.43703
2/18/2010	Austin	Texas	2	15	30.26761	-97.742984
3/4/2010	Arlington	Virginia	1	2	38.87186	-77.056267
8/3/2010	Manchester	Connecticut	9	2	41.77593	-72.521476
9/1/2010	Silver Spring	Maryland	1	0	38.99551	-77.028075
1/8/2011	Tucson	Arizona	6	13	32.22174	-110.92648
9/6/2011	Carson City	Nevada	5	7	39.1638	-119.7674
10/14/2011	Seal Beach	California	8	1	33.74118	-118.10464
2/22/2012	Norcross	Georgia	5	0	33.94121	-84.213531
4/2/2012	Oakland	California	7	3	37.80438	-122.27082

DATE	CITY	STATE	DEATHS	INJURIES	LAT.	LONG.
5/20/2012	Seattle	Washington	6	1	47.60383	-122.33006
7/20/2012	Aurora	Colorado	12	70	39.70928	-104.82349
8/5/2012	Oak Creek	Wisconsin	7	4	42.88585	-87.863136
9/27/2012	Minneapolis	Minnesota	7	1	44.9773	-93.265469
12/14/2012	Newtown	Connecticut	27	2	41.41232	-73.311424
2/7/2013	Corona	California	1	1	33.87529	-117.56644
3/13/2013	Herkimer County	New York	5	2	43.0456	-74.984891
4/15/2013	Boston	Massachusetts	2	132	42.35027	-71.080976
4/17/2013	West	Texas	15	151	31.81668	-97.087902
4/18/2013	Cambridge	Massachusetts	1	0	42.35961	-71.093134
4/19/2013	Watertown	Massachusetts	2	16	42.37089	-71.182911
4/21/2013	Federal Way	Washington	5	0	47.31296	-122.33937
6/7/2013	Santa Monica	California	6	3	34.00862	-118.49475
7/26/2013	Hialeah	Florida	7	0	25.86701	-80.291463
9/16/2013	Washington	District of Columbia	12	8	38.87498	-76.99453
11/1/2013	Los Angeles	California	1	4	33.94159	-118.40853
2/20/2014	Alturas	California	4	2	41.4871	-120.54224
4/3/2014	Fort Hood	Texas	3	12		
4/13/2014	Overland Park	Kansas	2	0	38.98223	-94.670792
4/27/2014	Seattle	Washington	1	0	47.49242	-122.23911
5/23/2014	Santa Barbara	California	6	13		
6/1/2014	Seattle	Washington	2	0	47.6153	-122.32344

DATE	CITY	STATE	DEATHS	INJURIES	LAT.	LONG.
6/6/2014	Cumming	Georgia	1	1	34.20641	-84.13969
6/8/2014	Las Vegas	Nevada	5	0	36.16481	-115.06286
6/25/2014	West Orange	New Jersey	1	0	40.79859	-74.238395
9/12/2014	Blooming Grove	Pennsylvania	1	1	41.37012	-75.154073
10/23/2014	New York City	New York	1	3	40.72822	-73.797888
10/24/2014	Marysville	Washington	5	1	48.05082	-122.17692
11/28/2014	Austin	Texas	1	0	30.26744	-97.734942
12/18/2014	Morganton	North Carolina	1	0	35.74541	-81.684819
12/20/2014	New York City	New York	2	0	40.67818	-73.941773
2/10/2015	Chapel Hill	North Carolina	3	0	35.89671	-79.009738
3/20/2015	New Orleans	Louisiana	1	2	29.98437	-90.257301
5/3/2015	Garland	Texas	2	1	32.95903	-96.641877
6/11/2015	Menasha	Wisconsin	3	1		
6/17/2015	Charleston	South Carolina	9	0	32.78747	-79.933101
7/16/2015	Chattanooga	Tennessee	6	2	35.09508	-85.253424
7/23/2015	Lafayette	Louisiana	3	9	30.20197	-92.045686
10/1/2015	Roseburg	Oregon	9	9		
10/31/2015	Colorado Springs	Colorado	3	0		
11/4/2015	Merced	California	1	4	37.3658	-120.42477
11/27/2015	Colorado Springs	Colorado	3	9	38.88089	-104.84905
12/2/2015	San Bernardino	California	16	17	34.07577	-117.27792
2/11/2016	Columbus	Ohio	1	4	40.06402	-82.863818

DATE	CITY	STATE	DEATHS	INJURIES	LAT.	LONG.
2/20/2016	Kalamazoo County	Michigan	6	2		
2/25/2016	Hesston	Kansas	3	14		
6/12/2016	Orlando	Florida	50	53	28.5196	-81.376794
7/7/2016	Dallas	Texas	6	9	32.77958	-96.804259
7/7/2016	Dallas	Texas	5	11		
7/17/2016	Baton Rouge	Louisiana	4	3	30.43348	-91.080857
8/13/2016	New York City	New York	2	0	40.6794	-73.858592
9/16/2016	Philadelphia	Pennsylvania	2	5	39.9575	-75.222965
9/17/2016	St. Cloud	Minnesota	1	10	45.55558	-94.210178
9/23/2016	Burlington	Washington	5	0		
11/28/2016	Columbus	Ohio	1	11	40.00329	-83.011421
1/6/2017	Fort Lauderdale	Florida	5	6		
4/18/2017	Fresno	California	3	0		
5/12/2017	Kirkersville	Ohio	3	0		
6/5/2017	Orlando	Florida	5	0		
6/7/2017	Tunkhannock	Pennsylvania	3	0		
6/14/2017	San Francisco	California	3	2		
10/1/2017	Las Vegas	Nevada	58	527		

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. EXPERIMENT SURVEY QUESTIONS

Preamble

In this survey, you are asked to review five case studies and decide whether the individual described in the case may commit violence. For the sake of the survey, please assume that the information that appears is what would be typically available after a brief field investigation over three days or less. Investigative techniques may include voluntary statements by the subject, statements by the subject's friends, family and associates, material posted in publicly available on-line forums, and arrest records.

The scenarios that appear are randomly selected for every volunteer in this survey. Some or all of these scenarios derive from actual cases. Although steps have been taken to obscure these cases, you may recognize one or more of them. If that occurs, please check the "I am familiar with this case" box below each scenario, and answer the remaining questions.

Thank you for participating in this survey.

Biographical Data

Please describe your professional background

Law enforcement y/n Years of experience in this field _____

Fire department or EMS y/n Years of experience in this field _____

Military ____ y/n Years of experience in this field _____

Medicine or Public Health ____ y/n Years of experience in this field _____

Social Worker ____ y/n Years of experience in this field _____

Other (describe) _____ Years of experience in this field _____

Has your professional experience included acting as an investigator or analyst? y/n

SCENARIOS

Scenario 1

A subject is being investigated for unusual behavior at his former school—a county-run community college. The subject withdrew from the college after a nine-month series of incidents wherein he engaged in series of verbal outbursts in classes and threatened two professors. These incidents led to five encounters with the campus police. Prior to these encounters with the police, the subject was arrested in previous years for low-level drug offenses and vandalism.

The subject's friends and family describe the subject's behavior as a recent change: while in high school he was intense, intelligent, and good at math. In his junior year, he became more distant, appeared in class intoxicated, was said to frequently speak about government conspiracies, and eventually dropped out of high school.

The subject is active online, and through chat rooms and posted videos of himself it appears he owns at least two firearms, a semiautomatic pistol and a shotgun. He has two tattoos, one on each shoulder blade, of nine-millimeter bullets. In other statements, he speaks or writes of voices in his head, and others involve the theme of the government listening to him and circulating a "new currency." Another post pictures a history book with an image of the White House on the cover, over which the subject has placed a pistol. Also online, he claims to have attempted to join the military but could not because of his history of drug use. He also admits to trouble holding regular employment in general. He was fired from a job, more than once, for outbursts on the job.

Are you familiar with this case?

Do you think this subject should be investigated further?

If you chose to investigate further, what would be your next investigative step?

On a scale of 0 to 100, rate how likely it is that this subject will commit violence in the future.

Based on the facts you read, do you think there is cause to arrest this subject?

What were the key aspects of this case that influenced your decision?

Scenario 2

> You are called to interview a subject who was stopped by police for having a hatchet visibly tucked in his waistband near a secure government building. A query of your agency's records shows that a colleague of yours, who works about 150 miles away, interviewed the subject one day ago. On that occasion, a state trooper stopped the subject for speeding and evading police. A sawed-off shotgun and a map of Washington DC were visible on the passenger seat. When trooper examined the map further, the he saw that government buildings were circled with a red marker. The subject was arrested for evading the police, and your colleague was contacted to interview the subject further about the map and gun.
>
> During the interview, the subject explained that he was a recently discharged combat veteran and that his evasive driving was a momentary "flashback" from his combat experience. Your colleague and the police accepted the explanation, seized his shotgun, and released him from custody.
>
> After learning these details, you interview the subject, who is cooperative. He consents to a search of his nearby vehicle, where you find he has two dogs locked inside, two other hatchets, and several empty ammunition cartridges but no firearms.

Are you familiar with this case?

Do you think this subject should be investigated further?

If you chose to investigate further, what would be your next investigative step?

On a scale of 0 to 100, rate how likely it is that this subject will commit violence in the future.

Based on the facts you read, do you think there is cause to arrest this subject?

What were the key aspects of this case that influenced your decision?

Scenario 3

> You receive a case to investigate a military doctor, who raised suspicions by communicating with a known terrorist leader.
>
> You query the subject's military personnel record and discover that he is a medical doctor who recently completed a public health fellowship at a nearby military medical school. You also see that the subject has served in the military for over 15 years and was recently promoted to the rank of major. The subject is about to be transferred for a short-term assignment to another state before being deployed to a medical assignment in a combat zone.

Are you familiar with this case?

Do you think this subject should be investigated further?

If you chose to investigate further, what would be your next investigative step?

On a scale of 0 to 100, rate how likely it is that this subject will commit violence in the future.

Based on the facts you read, do you think there is cause to arrest this subject?

What were the key aspects of this case that influenced your decision?

Scenario 4

> You are called to investigate a teenage subject whom you and your agency encountered before for various complaints of disruptive activity. The most recent complaint was when the subject was accused, along with a friend who is the same age, of breaking into a vehicle and stealing items inside. On this occasion, your agency received complaints about the online activity of the subject, who posted online videos and comments including violent rants and a death threat.
>
> Reviewing the online posts and other internet activity, you note that the subject's friend is interested in Adolph Hitler, made several racist and homophobic rants, plans to destroy his high school, and listed personal grievances that he wishes to avenge. He also boasts of owning weapons, detonating small explosive devices, and vandalizing homes in the middle of the night; however, you have not found proof of these boasts.
>
> Witnesses tell a mixed story about the subject. His high school administrators say he appears intelligent and polite with no record of discipline; however, he also appears to be isolated from the student body and generally associates with two or three other students. Other associates from school and work report that he has openly boasted of assembling pipe bombs and other devices. He showed a pipe bomb to associates at work.

Are you familiar with this case?

Do you think this subject should be investigated further?

If you chose to investigate further, what would be your next investigative step?

On a scale of 0 to 100, rate how likely it is that this subject will commit violence in the future.

Based on the facts you read, do you think there is cause to arrest this subject?

What were the key aspects of this case that influenced your decision?

Scenario 5

> You are called to investigate a teenage subject whom you and your agency encountered before for various complaints of disruptive activity. The most recent complaint was when the subject was accused, along with a friend who is the same age, of breaking into a vehicle and stealing items inside. On this occasion, your agency received complaints about the online activity of his friend, who posted online videos and comments including violent rants and a death threat. The subject is mentioned in some of the posts.
>
> Reviewing the online posts and other internet activity, you note that the subject's friend is interested in Adolph Hitler, made several racist and homophobic rants, plans to destroy his high school, and listed personal grievances that he wishes to avenge. He also boasts of owning weapons, detonating small explosive devices, and vandalizing homes in the middle of the night; however, you have not found proof of these boasts.
>
> Witnesses describe the subject as socially isolated at school with only a few friends. He was a good student his first year in high school, but for the following three years he struggled. On some occasions, he submitted assignments that researched Charles Manson; others were fictional fantasies of a single gunman who commits mass killings.

Are you familiar with this case?

Do you think this subject should be investigated further?

If you chose to investigate further, what would be your next investigative step?

On a scale of 0 to 100, rate how likely it is that this subject will commit violence in the future.

Based on the facts you read, do you think there is cause to arrest this subject?

What were the key aspects of this case that influenced your decision?

Risk Assessment

The next few questions assess your general decision making.

Imagine you are managing an investigative squad in a homeland security agency, and you need to decide whether to open or close an investigation.

If you could only choose one, which do you consider the higher-priority case?

A.	B.
50% chance to save seven lives 50% chance that the case is a false alarm (nothing happens)	100% chance to save three lives

If you could only choose one, which do you consider the higher-priority case?

A.	B.
50% chance to prevent $55 million of damage 50% chance that the case is a false alarm (nothing happens)	100% chance to prevent $25 million of damages

If you could only choose one, which do you consider the higher-priority case?

A.	B.
1% chance that 100 people will die 33% that 9 people will die 67% that it is a false alarm	100% chance that three people will die

If you could only choose one, which do you consider the higher-priority case?

A.	B.
1% chance that $700 million of damage will occur 33% that $30 million of damage will occur 67% that it is a false alarm	100% chance that $15 million of damage will occur

Imagine you are up for promotion. Only 1% of cases you receive have intelligence as solid as the case your boss gives you. He assigns it to you, and promises that if you succeed, you will receive a $10,000 performance bonus. Once you begin investigating, you realize that the intelligence is not as clear as you originally thought. Success may hinge on how long you investigate. Which choice below would you make?

Commit to a long investigation.	Close the case quickly.
45% chance that the case is fully successful (full $10,000 bonus) 55% chance that the case is a false alarm	100% chance that if you cut the case short, you will receive the bonus you received last year ($5,000)

You receive a promotion from your last case that increases your salary by $10,000 per year. Now, as a manager, you have to make the tough choices. Another case arrives on your desk, a "1 %" case, with the same issues as the last scenario. Here, you have to make a tough resource-allocation decision:

Commit to a long investigation.	Close the case quickly.
45% chance that the case is fully successful 55% chance that the case is a false alarm and that your agency will be sued for ($10,000 loss)	100% chance that if you cut the case short, you will only waste the time and resources expended thus far ($5,000 loss)

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Baele, Stephane. “Lone-Actor Terrorist’s Emotions and Cognition: An Evaluation Beyond Stereotypes.” *Political Psychology*, 38, no. 3 (2017): 449–468. doi: 10.1111/pops.12365.

Blair, J. Pete, and Katherine W. Schweit. *A Study of Active Shooter Incidents, 2000—2013*. Washington DC: Texas State University and Federal Bureau of Investigation, 2014. https://www.fbi.gov/file-repository/active-shooter-study-2000-2013-1.pdf.

Brier, Glen W. “Verification of Forecasts Expressed in Terms of Probability.” *Monthly Weather Review* 78, no 1 (1950): 1–3.

Brown, Tim. *Change by Design: How Design Thinking Transforms Organizations and Inspires Innovation*. New York: Harper Collins, 2009.

Chen, Daniel, Tobias J. Moskowitz, and Kelly Shue. *Decision-Making under the Gambler’s Fallacy: Evidence from Asylum Judges, Loan Officers, and Baseball Umpires*. NBER Working Paper Series, National Bureau of Economic Research, 2016. http://www.nber.org/papers/w22026.pdf.

Christakis, Nicholas A., and James H Fowler. *Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives*. New York: Little Brown and Co., 2009.

Columbine Review Commission. *The Report of Governor Bill Owens Governor’s Columbine Review Commission*. Denver, CO, Columbine Review Commission, 2001. https://schoolshooters.info/sites/default/files/Columbine%20-%20Governor's%20Commission%20Report.pdf.

Ellis, Clare, Raffaello Pantucci, Jeanine de Roy van Zuijdewijn, Edwin Bakker, Melanie Smith, Benoît Gomis and Simon Palombi. “Analyzing the Process of Lone-Actor Terrorism: Research Finding and Recommendations.” *Perspectives on Terrorism* 10, no. 2 (2016): 33–41. http://www.terrorismanalysts.com/pt/index.php/pot/article/view/499/html.

Granovetter, Mark. “The Strength of Weak Ties.” *American Journal of Sociology* 78, no. 6 (1973): 1364–1366. https://doi.org/10.1086/225469.

Gujarati, Damodar. *Basic Econometrics*. New York: McGraw-Hill, 1988.

Fein, Robert, and Bryan Vossekuil. *Preventing Assassination: Secret Service Exceptional Case Study Project*. Washington, DC: National Institute for Justice, 1997. https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=167224.

Fein, Robert, and Bryan Vossekuil. *Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials*. Washington: National Institute for Justice, 2000. https://www.ncjrs.gov/pdffiles1/nij/179981.pdf.

Fein, Robert, Bryan Vossekuil, and Gwen A. Holden. "Threat Assessment: An Approach to Prevent Targeted Violence." *Research in Action*, NCJ 155000 (July 1995. https://www.ncjrs.gov/pdffiles/threat.pdf.

Follman, Mark, Gavin Aronsen, and Deanna Pan. *Mother Jones*, November 15, 2017. http://www.motherjones.com/politics/2012/12/mass-shootings-mother-jones-full-data/.

Ignatius, David. "More Chatter Than Needed." *Washington Post*, November 1, 2013.

Janis, Irving. *Victims of Groupthink: A Psychological Study of Foreign-Policy Decisions and Fiascoes*. Boston: Houghton Mifflin, 1972.

Jenkins, Brian Michael, Andrew Liepman, and Henry H. Willis. *Identifying Enemies Among Us: Evolving Threats and the Continuing Challenges of Domestic Intelligence*. Santa Monica, CA: RAND Corporation, 2014.

Kahneman, Daniel. *Thinking Fast and Slow*. New York: Farrar, Straus and Giroux, 2013.

Kahneman, Daniel, and Amos Tversky. "Choices, Values, and Frames." *American Psychologist* 39, no. 4 (1984): 341–350. doi:10.1037/0003-066X.39.4.341.

Kahneman, Daniel, and Amos Tversky. "Prospect Theory." *Econometrica* 47, no. 2 (1979): 263–292. doi: 10.2307/1914185.

Keynes, John Maynard. *A Treatise on Probability: Full Text of 1921 Edition*. www.Wealthof Nation.com, 2014. Kindle edition.

Lewis, Ted G. *Network Science: Theory and Practice*. Hoboken, NJ: John Wiley & Sons, 2009.

Loreto, Vittorio, Vito D. P. Servedio, Steven H. Strogatz and Francesca Tria. "Dynamics of Expanding Spaces: Modelling the Emergence of Novelties." In *Creativity and Universality in Language*. Lecture Notes in Morphogenesis Series, edited by Mirko Degli Esposti, Eduardo G. Altmann, François Pachet 59–83. Cham, Switzerland: Springer International, 2016. https://arxiv.org/pdf/1701.00994v1.pdf.

Mazzetti, Mark, Eric Lichtblau, and Alan Blinder. "Omar Mateen, Twice Scrutinized by F.B.I., Shows Threat of Lone Terrorists." *New York Times*, June 13, 2016.

Mitka, Mike. “Joint Commission Warns of Alarm Fatigue: Multitude of Alarms from Monitoring Devices Problematic.” *JAMA.* 309, no. 22 (2013): 2315–2316. doi:10.1001.

National Threat Assessment Center. *Attacks on Federal Government 2001–2013: Threat Assessment Considerations*. Washington, DC: United States Secret Service, 2015.

National Threat Assessment Center. *Using a Systems Approach for Threat Assessment Investigations: A Case Study on Jared Lee Loughner*. Washington, DC: U.S. Secret Service, 2015.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Washington, DC: National Commission on Terrorist Attacks upon the United States, 2004.

Papachristos, Andrew V., Anthony A. Baga, Eric Piza, and Leigh S. Grossman. “The Company You Keep? The Spillover Effects of Gang Membership on Individual Gunshot Victimization in a Co-offending Network.” *Criminology* 53, no. 4 (2015): 624–649. doi: 10.1111/1745-9125.12091.

Reyna, Valerie F., Christina F. Chick, Jonathan C. Corbin, and Anderw N. Hsia. “Developmental Reversals in Risky Decision Making: Intelligence Agents Show Larger Decision Biases Than College Students.” *Psychological Science* 25, no. 1 (2013): 76–84. http://doi.org/10.1177/0956797613497022.

Santora, Marc, and Adam Goldman. “Ahmad Khan Rahami Was Inspired by Bin Laden, Charges Say.” *New York Times*, September 20, 2016.

Sapolsky, Robert M. *Behave: The Biology of Humans at our Best and Worst*. New York: Penguin, 2017.

Senate Committee on Homeland Security and Governmental Affairs. *A Ticking Time Bomb: Counterterrorism Lessons from the US Government’s Failure to Prevent the Fort Hood Attack*. Washington, DC: Senate Committee on Homeland Security and Governmental Affairs, 2011. https://www.hsgac.senate.gov/imo/media/doc/Fort_Hood/FortHoodReport.pdf.

Senate Permanent Subcommittee on Investigations. *Federal Support for and Involvement in State and Local Fusion Centers—Majority and Minority Staff Report*. Washington, DC: Senate Permanent Subcommittee on Investigations, 2012. https://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers.

Shane, Scott, Michael S. Schmidt and Eric Schmitt. “Russia’s Warning on Bombings Suspect Sets off a Debate.” *New York Times*, April 25, 2013.

State of Colorado Department of Law, Office of the Attorney General. *Report of the Investigation into the 1997 Directed Report and Related Matters Concerning the Columbine High School Shootings in April 1999*. Denver, CO: State of Colorado Department of Law, 2004. https://schoolshooters.info/sites/default/files/1997_1998_columbine_report.pdf.

Stephens-Davidovitz, Seth. *Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us about Who We Really Are*. New York: HarperCollins, 2017.

Thaler, Richard. *Misbehaving: The Making of Behavioral Economics*. New York: W.W. Norton, 2015.

Walz, Steffen P., and Sebastian Deterdin "An Introduction to the Gameful World." In *The Gameful World*, edited by Steffen P. Walz and Sebastian Deterdin, 1–2. Cambridge: MIT Press, 2014.

Taleb, Nassim. *The Black Swan: The Impact of the Highly Improbable*. New York: Random House, 2007.

Tetlock, Philip, and Dan Gardner. *Superforecasting: The Art and Science of Prediction*. New York: Crown, 2015.

U.S. Department of Homeland Security, Office of the Inspector General. *2014 White House Fence Jumping Incident (Redacted)* (DHS-OIG Report OIG 16-64). Washington, DC: U.S. Department of Homeland Security, Office of the Inspector General, 2016. https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-64-Apr16.pdf.

van Zuijdewijn, Jeanine de Roy, and Edwin Bakker. "Analyzing Personal Characteristics of Lone-Actor Terrorists: Research Findings and Recommendations." *Perspectives on Terrorism* 10, no. 2 (2016): 42–49. https://openaccess.leidenuniv.nl/bitstream/handle/1887/44250/PersonalCharacteristics-PoT.pdf?sequence=1.

Wilson, James Q. *Bureaucracy: What Government Agencies Do and Why They Do It*. New York: Perseus Books, 1989.

Winkler, Robert. "Evaluating Probabilities: Asymmetric Scoring Rules." *Management Science* 40, no 11 (1994): 1395–1405.

Worth, Katie. "Lone Wolf Attacks Are Becoming More Common—And More Deadly." *Frontline*, July 14, 2016. http://www.pbs.org/wgbh/frontline/article/lone-wolf-attacks-are-becoming-more-common-and-more-deadly/.

Zegart, Amy. *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Princeton, NJ: Princeton University Press, 2007.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California