

**BAYESIAN NETWORK ANALYSIS OF RADIOLOGICAL DISPERSAL  
DEVICE ACQUISITIONS**

A Thesis

by

GRANT RICHARD HUNDLEY

Submitted to the Office of Graduate Studies of  
Texas A&M University  
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

December 2010

Major Subject: Nuclear Engineering

Bayesian Network Analysis of Radiological Dispersal Device Acquisitions

Copyright 2010 Grant Richard Hundley

**BAYESIAN NETWORK ANALYSIS OF RADIOLOGICAL DISPERSAL  
DEVICE ACQUISITIONS**

A Thesis

by

GRANT RICHARD HUNDLEY

Submitted to the Office of Graduate Studies of  
Texas A&M University  
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Approved by:

Chair of Committee,	William S. Charlton
Committee Members,	Craig Marianno
	Sara Daly
Head of Department,	Raymond Juzaitis

December 2010

Major Subject: Nuclear Engineering

**ABSTRACT**

Bayesian Network Analysis of Radiological Dispersal Device Acquisitions.

(December 2010)

Grant Richard Hundley, B.S., United States Naval Academy

Chair of Advisory Committee: Dr. William S. Charlton

It remains unlikely that a terrorist organization could produce or procure an actual nuclear weapon. However, the construction of a radiological dispersal device (RDD) from commercially produced radioactive sources and conventional explosives could inflict moderate human casualties and significant economic damage. The vast availability of radioactive sources and the nearly limitless methods of dispersing them demand an inclusive study of the acquisition pathways for an RDD. A complete network depicting the possible acquisition pathways for an RDD could be subjected to predictive modeling in order to determine the most likely pathway an adversary might take. In this work, a comprehensive network of RDD acquisition pathways was developed and analyzed utilizing the Bayesian network analysis software, *Netica*. The network includes variable inputs and motivations that can be adjusted to model different adversaries. Also, the inclusion of evidence nodes facilitates the integration of real-time intelligence with RDD plot predictions.

A sensitivity analysis was first performed to determine which nodes had the greatest impact on successful completion of RDD acquisition. These results detail which portions of the acquisition pathways are most vulnerable to law enforcement

intervention. Next, a series of case studies was analyzed that modeled specific adversarial organizations. The analysis demonstrates various features of the constructed Bayesian RDD acquisition network and provides examples of how this tool can be utilized by intelligence analysts and law enforcement agencies. Finally, extreme cases were studied in which the adversary was given the maximum and minimum amount of resources in order to determine the limitations of this model.

The aggregated results show that successful RDD acquisition is mostly dependent on the adversary's resources. Furthermore, the network suggests that securing radiological materials has the greatest effect on interdicting possible RDD plots. Limitations of this work include a heavy dependence on conditional probabilities that were derived from intuition, as opposed to actual historical data which does not exist. However, the model can be updated as attempted or successful RDD plots emerge in the future. This work presents the first probabilistic model of RDD acquisition pathways that integrates adversary motivations and resources with evidence of specific RDD threats.

**DEDICATION**

To the “Lion of Fallujah”

Major Douglas A. Zembiec

April 14, 1973 – May 11, 2007

## TABLE OF CONTENTS

	Page
ABSTRACT .....	iii
DEDICATION .....	v
TABLE OF CONTENTS .....	vi
LIST OF FIGURES .....	viii
LIST OF TABLES .....	xii
 CHAPTER	
I INTRODUCTION.....	1
Background .....	2
Motivation .....	6
Objectives.....	7
Previous Work.....	10
II NETWORK DEVELOPMENT .....	12
Network Overview .....	12
Adversarial Motivation .....	13
Radioactive Material Acquisition.....	18
Weaponization.....	22
Assembly and Detonation .....	24
Final Device Probabilities and Characteristics.....	25
Adversary Inputs .....	27
Tactical Capabilities .....	28
Technical Capabilities .....	29
Funding.....	31
Bayesian Analysis .....	34
Netica .....	38
“Asia” Example Network.....	38
Constant Nodes .....	43
Conditional Probability Tables.....	46
Network Construction .....	50

	Page
CHAPTER	
III NETWORK VERIFICATION .....	77
Plot 1: Homegrown, Al-Qaeda Influenced Plot .....	77
Effect of Evidence for Delivery Methods .....	81
Effect of Evidence for Source Processing.....	82
Effect of Evidence for Radioactive Material Acquisition ....	83
Plot 2: Apocalyptic Group Plot .....	85
Effect of Evidence for Radioactive Material Acquisition ....	88
Effect of Evidence against Source Processing .....	89
Effect of Evidence for Radioactive Material Acquisition and Subsequent Plot Flags.....	91
Plot 3: Drug Cartel Plot.....	94
Effect of Increased Funding .....	99
Effect of Change in Adversarial Motivation and Evidence of Specific Target .....	101
Extreme Plot 1: Adversary with Maximum Resources .....	103
Extreme Plot 2: Adversary with Minimum Resources.....	107
Plot Comparison .....	112
IV SENSITIVITY ANALYSIS.....	116
V CONCLUSIONS .....	126
REFERENCES.....	130
VITA .....	133



## LIST OF FIGURES

	Page
Fig. 1. Abdulmutallab’s underwear used to conceal plastic explosives .....	4
Fig. 2. Positioning of charges inside the vehicle used in the May 2010 Times Square attempted bombing .....	6
Fig. 3. Visual depiction of the inputs and outputs of a Bayesian network analysis ....	9
Fig. 4 . Depiction of how to incorporate motivations into pathway decisions .....	17
Fig. 5. General overview of the network’s construction .....	33
Fig. 6. “Asia” Bayesian network provided as an example within <i>Netica</i> .....	39
Fig. 7. “Asia” network with the addition of evidence for a smoker and an abnormal X-ray .....	40
Fig. 8. Cumulative belief curve for risk of lung cancer according to “Asia” .....	43
Fig. 9. Constant node used to describe available adversary funding .....	44
Fig. 10. State values of the “Funding” constant node .....	46
Fig. 11. Nodes depicting evidence of thermite as an incendiary device type .....	48
Fig. 12. Truth table depicting evidence of thermite as an incendiary device type .....	49
Fig. 13. “Process Outcome” node whose probabilities are calculated by a Boolean logic equation and constant nodes .....	50
Fig. 14. Overview of RDD acquisition network .....	51
Fig. 15. Overview of adversary inputs and motivations section .....	52
Fig. 16. Adversary input portion of adversary inputs and motivations section .....	53
Fig. 17. Adversary motivation portion of adversary inputs and motivations section .....	53
Fig. 18. Suspected target location portion of adversary inputs and motivations section .....	54

	Page
Fig. 19. Overview of radioactive material acquisition section.....	55
Fig. 20. Medical facility portion of radioactive material acquisition section .....	56
Fig. 21. RTG portion of radioactive material acquisition section.....	57
Fig. 22. Irradiation facility portion of radioactive material acquisition section.....	57
Fig. 23. Commercial acquisition portion of radioactive material section .....	58
Fig. 24. Industrial use portion of radioactive material acquisition section .....	59
Fig. 25. Transport interdiction portion of radioactive material acquisition section ....	60
Fig. 26. Radioactive material summary portion of radioactive material acquisition section.....	61
Fig. 27. Overview of source weaponization section .....	62
Fig. 28. Source shielding portion of source weaponization section.....	63
Fig. 29. Source processing portion of source weaponization section .....	64
Fig. 30. Source weaponization input portion of source weaponization section.....	65
Fig. 31. Overview of assembly and detonation section.....	66
Fig. 32. Overview of explosives portion of assembly and detonation section.....	67
Fig. 33. Incendiary device portion of assembly and detonation section .....	68
Fig. 34. Low explosive portion of assembly and detonation section .....	69
Fig. 35. High explosive portion of assembly and detonation section .....	70
Fig. 36. Explosive summary portion of assembly and detonation section.....	71
Fig. 37. Delivery method portion of assembly and detonation section.....	72
Fig. 38. Detonation portion of assembly and detonation section .....	73

	Page
Fig. 39. Overview of final RDD design characteristics and overall chance of success section .....	74
Fig. 40. Final RDD design characteristics portion of RDD design characteristics and overall chance of success section .....	75
Fig. 41. Overall chance of success portion of RDD design characteristics and overall chance of success section .....	76
Fig. 42. Inputs for homegrown, Al-Qaeda influenced RDD plot.....	79
Fig. 43. Overall chance of success for a homegrown, Al-Qaeda influenced RDD plot .....	80
Fig. 44. Overall chance of success for a homegrown, Al-Qaeda influenced RDD plot with evidence of a vehicle purchase .....	81
Fig. 45. Overall chance of success for a homegrown, Al-Qaeda influenced RDD plot with evidence of source processing .....	83
Fig. 46. Overall chance of success for a homegrown, Al-Qaeda influenced RDD plot with evidence of radioactive material acquisition .....	84
Fig. 47. Inputs for apocalyptic group RDD plot .....	87
Fig. 48. Overall chance of success for an apocalyptic group RDD plot .....	88
Fig. 49. Overall chance of success for an apocalyptic group RDD plot with evidence of radioactive material acquisition.....	89
Fig. 50. Overall chance of success for an apocalyptic group RDD plot with evidence against source processing.....	91
Fig. 51. Transport interdiction evidence added to an apocalyptic group RDD plot.....	92
Fig. 52. Likely apocalyptic group actions based on evidence of radioactive material acquisition through transport interdiction .....	93
Fig. 53. Inputs for drug cartel RDD plot .....	96
Fig. 54. Overall chance of success for a drug cartel RDD plot.....	99

	Page
Fig. 55. Overall chance of success for a drug cartel RDD plot with increased funding .....	101
Fig. 56. Overall chance of success for a drug cartel RDD plot with a change in motivation and a water front city as a target .....	103
Fig. 57. Inputs for extreme case with maximum resources .....	105
Fig. 58. Overall chance of success for adversary with maximum resources .....	107
Fig. 59. Inputs for extreme case with minimal funding .....	108
Fig. 60. Overall chance of success for an adversary with minimal funding .....	111
Fig. 61. Sensitivity findings for “Overall Danger from Radioactive Exposure” node .....	118
Fig. 62. Sensitivity findings for “Panic Inducing Capability” node.....	119
Fig. 63. Sensitivity findings for “Capability to Weaponize Source” node .....	121
Fig. 64. Sensitivity findings for “Capability to Assemble and Detonate Device” node .....	122
Fig. 65. Sensitivity findings for “Overall Probability of RDD Plot Success” node....	124

## LIST OF TABLES

		Page
Table I.	Conditional probability table for the diagnosis of tuberculosis with an x-ray .....	35
Table II.	Homegrown, Al-Qaeda influenced RDD plot characteristics .....	80
Table III.	Homegrown, Al-Qaeda influenced RDD plot characteristics with evidence of source processing .....	83
Table IV.	Apocalyptic group RDD plot characteristics .....	86
Table V.	Apocalyptic group RDD plot characteristics with evidence against source processing .....	90
Table VI.	Drug cartel RDD plot characteristics .....	98
Table VII.	Drug cartel RDD plot characteristics with increased funding.....	100
Table VIII.	Drug cartel RDD plot characteristics with a change in motivation and a waterfront city as a target.....	102
Table IX.	RDD plot characteristics for an adversary with maximum resources ....	106
Table X.	RDD plot characteristics for an adversary with minimum resources.....	110
Table XI.	Comparison of RDD plot probabilities .....	114
Table XII.	Comparison of RDD plot characteristics .....	115

## CHAPTER I

### INTRODUCTION

The threat of terrorism has evolved rapidly in the past decade. A post 9/11 world has seen enhanced domestic security efforts that have forced terrorists to apply an ever-increasing will and creativity towards future attacks. This innovation, coupled with the vast availability of radioactive sources in nearly every country across the globe, makes a radiological dispersal device (RDD) an attractive option for an adversary seeking civilian deaths, chaos, and economic consequences. An RDD, in the most basic sense, is a device that exposes people to radioactive materials. However, this work will address RDDs that include explosive mixtures as the dispersal method. The substantial variety of radioactive sources and the numerous methods of dispersing them imply a nearly limitless number of possible designs. A study of RDDs is further convoluted by the number of adversaries willing to do harm to the United States. Groups ranging from a homegrown Al-Qaeda influenced cell to a well-equipped drug cartel could all benefit from the acquisition of an RDD. However, each adversary's ultimate motivations strongly influence the type of device they would want and the ultimate consequences of a successful plot. This variety of potential RDD threats, coupled with the vast disparity in damage and effects of different designs, demands an inclusive study of the acquisition pathways for an RDD.

---

This thesis follows the style of *Nuclear Technology*.

This thesis presents the first probabilistic analysis of RDD acquisition pathways. Utilizing Bayesian analysis of a thoroughly developed network of RDD acquisition pathways, predictions about the most likely RDD plots are developed. Specific characteristics about potential adversaries are integrated into the network to provide a flexible intelligence tool capable of modeling various RDD threats. The inclusion of pathway evidence allows the user to adjust the network to include plot actions the adversary may have already completed. This feature facilitates the focusing of law enforcement resources on likely adversary actions.

## **Background**

The terrorist of the twenty-first century is unconventional, creative, and desperate. For an adversary with these characteristics, an RDD is the ideal weapon. The potential consequences of a successful RDD detonation far outweigh the effort to gather radiological materials and construct a device.<sup>1</sup> Capitalizing on the public's nearly universal fear of radiation inspired by Three Mile Island, Chernobyl, and the Cold War, the effects of an RDD would reach much further than injury and fatality due to radiation sickness. Upon learning of an RDD detonation, people in the target area would panic and mass hysteria would ensue. After the area was secured, the environmental cleanup would take months to years and billions of dollars would be spent. Businesses located in the area would be devastated. Global markets would plummet in a similar response to the effects of 9/11. The political effects would be polarizing. And, most importantly,

terrorist adversaries across the globe would be further empowered in a seemingly unmanageable War on Terror.

The unconventional nature of terrorism is epitomized by the defining moment of the twenty-first century: the attacks of September 11, 2001. As two fuel-laden passenger airplanes struck the towers of the World Trade Center, the Pentagon, and a field in Pennsylvania, the terrorist playbook quickly expanded upon traditional car bombings and shootings. Al-Qaeda pioneered an approach to terrorism that did more than kill and injure innocent Americans. Today's terrorist, more than ever, strives to strike absolute fear into the hearts of their adversaries. This fear-based approach turned to suicide bombers, beheadings, and the holy grail of unconventional, fear-inducing terrorism: weapons of mass destruction (WMD).

Anti-terrorism security measures implemented after 9/11 have also forced the modern terrorist to approach attacks with a renewed creativity. Thorough airport screening methods have all but secured domestic passenger flights from conventional hijackings and bombing methods. Law enforcement surveillance is now capable of signaling terrorist plots by examining the purchase of devices and materials utilized to fabricate explosives. Monitoring of outgoing e-mail communications to international terrorist networks has netted large groups of individuals proclaiming a desire to harm America. The impetus for the implementation of most of these security measures has been a response to an attempted or successful attack. For example, requiring passengers to remove their shoes for screening prior to boarding a flight is a specific response to Richard Reid's attempted shoe bombing.<sup>2</sup> While these measures are likely to prevent a



repeat attempt of a specific plot, they are less successful at preventing innovative and creative attacks. Terrorists have capitalized on this weakness. Umar Farouk Abdulmutallab's attempted underwear bombing of Northwest Airlines Flight 253 typifies this creative approach to modern terrorism. Figure 1 presents an image of the underwear utilized to conceal plastic explosives in the attempted attack.<sup>3</sup> Airport security measures at the time were unable to detect the explosive device. Terrorists seeking to perform a creative attack, such as an underwear bomb, would find an RDD to be an attractive option. RDDs have a wide range of sizes, and can be delivered through numerous methods. Furthermore, materials to construct an RDD could be obtained inside the borders of the United States. Even only a small amount of radioactive material, dispersed in a creative method, could have drastic consequences. There is only one certainty about a future RDD attack. The device, whether crude or extremely advanced, will be designed with a high level of creativity.



Fig. 1. Abdulmutallab's underwear used to conceal plastic explosives.

Finally, the terrorist of the twenty-first century is desperate. A significant military presence in Afghanistan and counter-terrorism operations across the globe have succeeded in hampering terrorist activities. While terrorist groups retain high levels of recruitment and growing support, their leadership and funding sources are gradually being eliminated. Consequently, today's terrorist needs to execute successful attacks on a frequent basis to convey prestige, corner funding, and maintain both direct and indirect state support. Faisal Shahzad's May 2010 attempted Times Square bombing demonstrates this nature of desperation. The plot, funded by the Pakistani Taliban, consisted of a crudely designed explosive device placed in the back of a Nissan Pathfinder. The assortment of improvised explosives used in the vehicle included five gallon gas cans, 20 gallon propane tanks, firecrackers, and 250 pounds of urea based fertilizer encased in a metal gun locker.<sup>4</sup> A diagram of the charges within the vehicle is seen in Fig. 2. It is interesting to note that urea based fertilizer requires processing prior to its use as an explosive. A more sophisticated and knowledgeable adversary would have likely chosen ammonium nitrate fertilizer. From a technical standpoint, this poorly designed device is a step back from the advanced improvised explosive devices seen in other terrorist attacks. However, it certainly portrays a desperate adversary eager to execute a successful plot. This desperation makes an RDD plot a very attractive option. Some experts argue that certain terrorist groups would hesitate to utilize WMD—even if they had access to such weapons.<sup>5</sup> On the other hand, adversaries previously unwilling to resort to WMD may change their mind in the face of such desperation. Limited funding and technical knowledge may prevent the development of a conventional

terrorist attack. Consequently, the use of a well-designed RDD may result in more destruction and devastation for the same contribution of effort and funding.

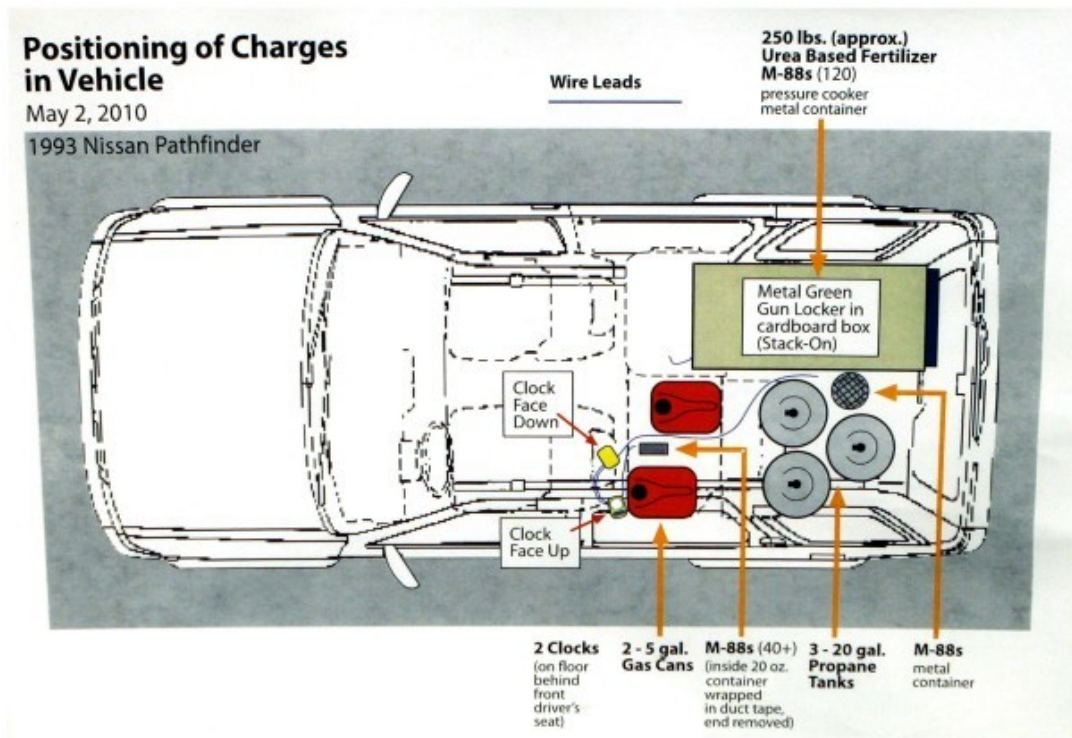


Fig. 2. Positioning of charges inside the vehicle used in the May 2010 Times Square attempted bombing.

### *Motivation*

Although an RDD has never successfully been employed as a terrorist weapon, it offers significant advantages to an adversary that may have poor funding and little technical capability. Many experts agree that a typical RDD attack would be incapable of causing mass civilian casualties. In fact, the only people likely to receive a lethal

dose of radiation would probably have to be close enough to the blast to have been killed or wounded by the blast itself.<sup>6</sup> However, the use of a radiological weapon would incite chaos and panic among local populations, and could have potentially devastating economic effects. On September 13, 1987, 1375 Curies of  $^{137}\text{Cs}$  chloride was released into the town of Goiânia, Brazil after two scrap metal scavengers looted a teletherapy machine. The source was removed from its sealed container and passed around the community. After medical personnel identified the radiological release, 112,000 people flocked to the city's soccer stadium for medical evaluation; 49 of those people were admitted to the hospital, and five individuals died. During cleanup operations, 85 buildings were determined contaminated, and seven were eventually demolished.<sup>6</sup> The incident in Goiânia, while not exactly parallel to an RDD attack, demonstrates the potential consequences from a radiological release in an urban population. If a similar incident occurred in downtown Manhattan, one could imagine the resulting panic and economic consequences of an evacuated Wall Street. The simplicity of an RDD and the availability of radiological materials imply that an RDD is capable of yielding an impact highly disproportionate to the risks and costs of carrying out such an attack.<sup>1</sup> It is important to note that, although unlikely, a technically advanced and well-funded adversary could create a sophisticated device capable of inflicting mass casualties.

### *Objectives*

This work has two main objectives in order to counter the threat that radiological terrorism poses to the United States of America. The first objective is to provide a

comprehensive picture of all available pathways to RDD acquisition. This is the first work to explicitly describe the variety of steps necessary to assemble an RDD. The vast availability of radioactive sources and the nearly limitless methods of dispersing them demand an inclusive study of the acquisition pathways for an RDD. A complete network depicting the possible acquisition pathways for an RDD could be subjected to predictive modeling in order to determine the most likely pathway an adversary might take.

The second objective of this work is to develop an analysis tool to analyze RDD acquisitions that is capable of integrating with real-time intelligence. A Bayesian analysis will permit the calculation of pathway completion probability. Additionally, the inclusion of node customization will allow this tool to become adaptable to developing security situations and terrorist threats. By integrating real-time intelligence signatures about possible terrorist actions, node probabilities can be adjusted to judge pathway completion and predict future terrorist actions. Fig. 3 depicts a visual representation of how the objectives of this work can be achieved through the use of a Bayesian network analysis. The three boxes in the top row represent inputs describing the adversary's characteristics. The four boxes in the second row represent the four pieces of information that feed into the Bayesian analysis: adversary motivations, adversary characteristics, priors, and evidence. Finally, the three boxes in the bottom row represent what information the Bayesian analysis provides in order to meet the stated objectives.

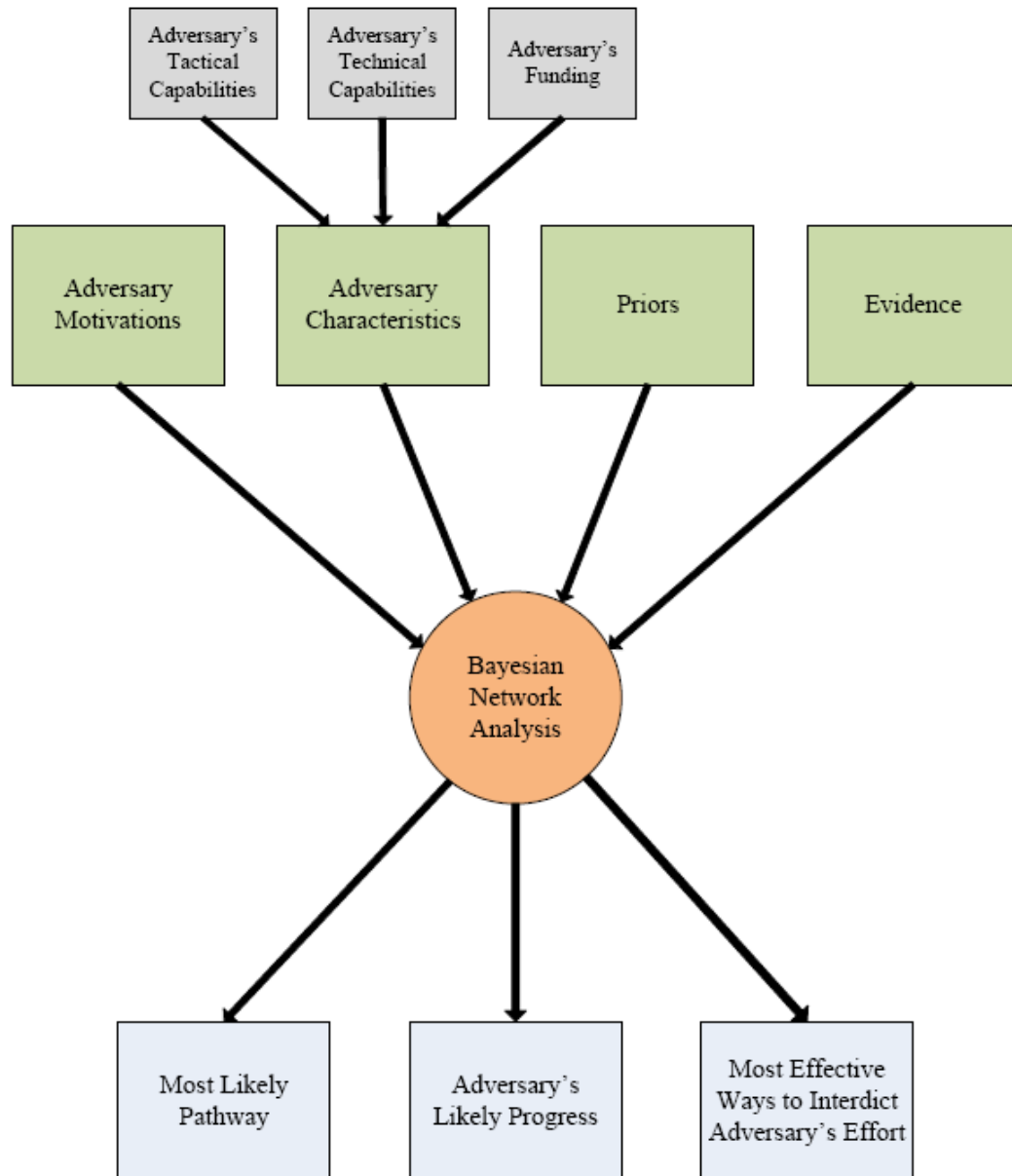


Fig. 3. Visual depiction of the inputs and outputs of a Bayesian network analysis.

## **Previous Work**

An open-source, probabilistic analysis of RDD acquisitions has not been previously performed. However, past research has investigated Bayesian analysis of nuclear weapon and improvised nuclear device acquisitions. Although these efforts address the development of nuclear fission devices, a fundamentally different process than the construction of an RDD, the objectives, Bayesian approach, and developed procedures parallel this proposed work. A thesis by Freeman presented the first Bayesian network analysis of nuclear acquisitions. The motivations and resources of state and terrorist organizations were evaluated to produce probability distributions for nodes within a network depicting the various pathways to nuclear weapon acquisitions. Evidence nodes allow for users of the network to integrate intelligence that may suggest which path an adversary has chosen to take. As the Bayesian beliefs are updated across the network, a relative probability of success can be calculated for various adversaries.<sup>7</sup> A thesis by Ford also presents an assessment tool for nuclear material acquisition pathways. This approach, however, used a resource based decision model implemented in Visual Basic.<sup>8</sup> Another paper by Eaton and Miller examines the terrorist acquisition of improvised nuclear devices. This Bayesian analysis, similar to the work done by Freeman, utilizes expert elicitation to determine which pathways are most likely for various terrorist organizations.<sup>9</sup> Both Bayesian analyses utilize a software package called *Netica*; which is the proposed method for this work. This previous work suggests that a Bayesian analysis of RDD acquisitions should be capable of providing the results detailed in the objectives of this research.

Other previous work has discussed radiological weapons as a form of terrorism and addressed the motivations of terrorist organizations who may utilize WMD. While not directly applicable to a probabilistic analysis of RDD acquisitions, they provide important context as to why a terrorist organization may choose to utilize an RDD. Poston, in a keynote address, explains that an RDD is an ideal terrorist weapon and reasons that the United States is ill-prepared to respond to such an event.<sup>10</sup> A thesis by Elder discusses the terrorist act of releasing  $^{210}\text{Po}$  inside an aircraft cabin. This work presents a detailed analysis of the likely radiologic effects, and provides interesting information about the weaponization of radioactive sources.<sup>11</sup> MacKerrow addresses the broad reasons why radical Islamist terrorism frequently targets America. Using a modeling approach called agent-based simulation, his work explores terrorist motivations from a social-economic perspective.<sup>12</sup> A paper by Darby evaluates the risk for acts of terrorism with belief and fuzzy sets. While this approach utilizes a different type of modeling than the one proposed, his conclusions demonstrate the effectiveness of a quantitative approach to the mitigation of terrorist acts.<sup>13</sup>

While this thesis presents the first probabilistic modeling of RDD acquisitions, a great deal of previous work indicates the overall utility of such research. Bayesian modeling of both terrorist and state actor acquisition of nuclear weapons suggests a similar analysis of RDD acquisitions will have a successful outcome. Finally, previous work concerning radiological weapons as a means of terrorism should provide a sound background for the integration of RDD acquisition pathways with underlying terrorist motivations.



## CHAPTER II

### NETWORK DEVELOPMENT

#### **Network Overview**

The first task of this work was to develop a complete network of the various pathways to RDD acquisition. These pathways are numerous and interconnected. Each decision or action an adversary makes can affect both subsequent and prior nodes in the network. Unlike a relatively linear pathway analysis of nuclear weapon acquisitions, an adversary pursuing an RDD can alternate pathways or even omit large portions of the network and still produce a formidable device. To account for this complexity, the developed RDD acquisition network was split into four separate tasks. These tasks include adversarial motivation, radioactive material acquisition, weaponization, and assembly and detonation. A final portion of the network provides an overview of the RDD's design and probability of success. In most cases, the adversary's pathway will at least traverse through the motivation, radioactive material acquisition, and assembly and detonation portions of the network. The weaponization portion of the network is not a requisite to a successful RDD detonation. Successfully traversing this portion of the network, however, has important implications in the eventual device effectiveness and subsequent pathway chosen. The development of each of the five portions paints an important picture about the varied tasks necessary for a successful RDD detonation. Conversely, this also suggests numerous ways an adversary can be detected and defeated.

### *Adversarial Motivation*

The first portion of the network considers the motivations of the adversary. While inherently less tangible than other tasks such as radioactive material acquisition and source weaponization, adversarial motivation plays an important role in determining the path that a terrorist may take towards RDD acquisition. The flexible and variable nature of the RDD threat implies that significantly different RDD designs may meet specific terrorist motivations. For example, a crude and poorly weaponized device might be sufficient to fulfill motivations such as mass devastation or to manipulate policy. On the other hand, the intention to redress conventional military asymmetry or wage war on another nation would require a much more sophisticated device. If a certain organization's ultimate motivations are known, then later nodes in possible acquisition pathways may become more likely. Kristin Childress, a student of Texas A&M's Bush School of Government and Public Service, studied terrorism with the goal of linking a terrorist's motivation for nuclear terrorism to specific nuclear threats. The following is a list of the eleven terrorist motivations developed by Childress and utilized in this work:

1. Peaceful Prestige of Capabilities: Possessing the capability for terrorism demonstrates an organization's viability and legitimacy. The group believes that simply possessing the ability to successfully complete a nuclear terrorist threat will achieve its goals, and finds the

actual event to be unnecessary. It is also possible that the group may detonate a weapon as a show of strength in a non-populated area.

2. Non-Peaceful Prestige of Capabilities: Possessing the capability for terrorism demonstrates an organization's viability and legitimacy. The group clearly has no problem using nuclear terrorism to achieve their goals.
3. Manipulate Adversaries: A group pursues nuclear terrorism to use as leverage against or to demonstrate a weakness in other organizations or nations.
4. Apocalyptic Beliefs: The organization believes that the end of the world is near and is motivated to take an active role in promoting the event.
5. War on Own Nation: Separatist or nationalist group that wants to use nuclear terrorism to combat, overthrow, or undermine the current government of a country.

6. War on Another Nation: The organization has a deep hatred for a particular people or nation and they feel compelled to use nuclear terrorism to combat or enact revenge upon their adversary.
7. Redress Conventional Military Asymmetry: An organization has a finite amount of people and resources to combat a nation, and seeks to use nuclear terrorism to redress this imbalance.
8. Organizational Security: A group pursues nuclear terrorism in order to protect citizens/members of a certain group (religious, political, ethnic, etc.) from attack or persecution.
9. Mass Devastation or Chaos: The group is motivated to wreck economic, political and psychological havoc on a population, and thus devastate the nation's infrastructure or population by nuclear terrorism. In this case, the violence is the end in itself.
10. Religious Imperative: Religious extremists that believe they have been given a religious mandate or imperative to pursue the nuclear threat.

11. Manipulate Policy: A group seeks to use the nuclear threat to bring attention to or change a specific policy (political, economic, religious, etc) that it does not agree with.

Inclusion of these eleven varied motivations describes the reasons why an organization may choose to pursue an RDD. However, knowledge of a specific adversarial motivation does not intuitively convey how that motivation will affect the eventual pathway. To account for this fact, four specific device intentions are included in this portion of the network. These device intentions are derived from a single motivation or a combination of multiple motivations from probability distributions. The implementation of these intentions follows a model suggested by Freeman.<sup>7</sup> Figure 4 demonstrates how adversary motivations lead to device intentions and eventually affect the pathway chosen. The following is a list of the four device characteristics included in this work:

1. Need for Even Dispersal: The adversary seeks to deny a large area by the dispersal of radioactive material. Or, the adversary seeks to harm a significant portion of the human population in the target area. Both goals require a finely weaponized source capable of increasing radioactive contamination to a constant level over a significant area of land.

2. Need for a Easily Deliverable Device: The adversary seeks an RDD design that can be delivered reliably from a remote location. An RDD fitting this criteria is typically small in size, light in weight, and can be detonated remotely, by a timing device, or through a proximity sensor. Likely delivery methods include rockets or mortars.
3. Need for IAEA Category 1 Source: The adversary requires a radioactive source with an activity greater than 1,000 Curies that would be fatal to humans after minutes of exposure.<sup>14</sup>
4. Desire to Settle for a Crude Device: The adversary's motivation for RDD usage could be met by a large, unwieldy, and poorly designed RDD. This type of device would likely produce few radioactive injuries, but would still incite panic among the local population.

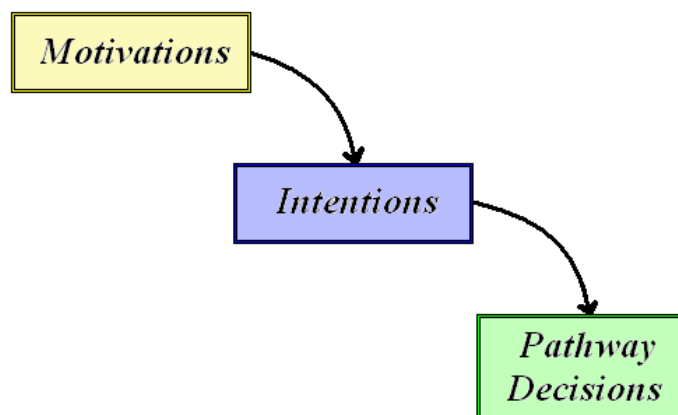


Fig 4. Depiction of how to incorporate motivations into pathway decisions.

Device intentions significantly affect the adversary's eventual pathway. A need for even dispersal primarily influences the amount of source processing an adversary will attempt. The need for an easily deliverable device influences delivery method, explosive type, and eventual device weight. This device intention is heavily weighted towards those adversaries attempting to redress conventional military asymmetry or waging war on nations. A need for an IAEA category 1 source solely affects the radioactive material portion of the network. A desire to settle for a crude device affects all portions of the network, including the overall probability of success.

#### *Radioactive Material Acquisition*

Radioactive material acquisition represents the largest and most complex portion of the developed RDD acquisition network. It is the lynchpin of successful plot completion, and thus the likely place where the adversary can be most easily stopped. An adversary cannot detonate an RDD without successful navigation of the radioactive material acquisition pathways. The purpose of this portion of the network is to represent possible methods of obtaining a radioactive source for utilization in an RDD. Millions of radioactive source are utilized daily in devices across the globe. It is impossible to characterize each radioactive source. The majority of these sources have low activities that negate their effectiveness as a radiological weapon. However, radiological sources of RDD concern can generally be obtained through six separate pathways: medical facility sources, irradiation facility sources, radioisotope thermoelectric generator (RTG)

sources, industrial use sources, commercial acquisition of sources (legal purchase), and the interdiction of sources during transport.

Medical facilities represent one of the more likely locations for radioactive source theft for use in an RDD. Most medical sources have an intermediate source strength of 1,000 to 20,000 Curies and are often constructed on mobile platforms for easy transportation<sup>1</sup>. Teletherapy devices utilize  $^{60}\text{Co}$  and  $^{137}\text{Cs}$  to kill cancerous tumors inside the body. The radioactivity level for these sources generally varies between 3,000 and 15,000 Curies.<sup>15</sup> The source is comprised of multiple 2.0 cm diameter pellets plated with nickel.<sup>1</sup> Blood irradiators utilize a  $^{137}\text{Cs}$  source to sterilize blood prior to transfusion. The source strength is approximately 5,000 Curies. Blood irradiators are about the size of a filing cabinet, and are often made highly mobile. Over 1,000 of these machines may exist in the world.<sup>15</sup> The  $^{137}\text{Cs}$  within blood irradiation sources is of particular concern since the cesium is already present in a readily dispersible powder. Brachytherapy involves the precise placement of sealed radioactive sources inside or adjacent to tumors within the body. These sources are typically of a lesser strength than other medicinal sources; however, their small size would make them attractive for theft. Radioisotope cows utilize  $^{99}\text{Mo}$  to produce a continuous supply of  $^{99\text{m}}\text{Tc}$ .  $^{99\text{m}}\text{Tc}$ , along with other isotopes of iodine, is frequently utilized as tracers within the body to diagnose potential ailments.

The relatively secure and immobile radioactive sources used in sterilization procedures represent less of an RDD threat than medicinal sources, but their high radiation levels make them an extremely valuable target. Hundreds of food and medical



supply sterilization facilities are located across the globe. The  $^{60}\text{Co}$  sources within these facilities range from 100,000 to 5 million Curies. The actual source is composed of hundreds of individual  $^{60}\text{Co}$  pencils.<sup>15</sup> The high source strength of these irradiators requires a large amount of shielding, and they are normally kept underwater for storage when the facility is not in operation. Consequently, an adversary would be required to raise the irradiator from the cooling pond prior to theft. Additionally, without a significant amount of shielding, any thief would likely receive a lethal dose of radiation prior to exiting the facility with the source.

Radioisotope thermoelectric generators (RTGs) were manufactured by the former Soviet Union and the United States to provide electricity in remote areas. The highest concentration of Soviet RTGs were utilized in the Arctic Circle, Far East, and Baltic Region to power remote electronic devices and lighthouses and over 1,000 were produced.<sup>15</sup> RTGs represent a particular RDD concern because many were lost after the fall of the Soviet Union and few records detail their locations. In addition, most have exceeded their engineered lifetime. RTGs typically use  $^{90}\text{Sr}$  with a source strength between 4,000 to 400,000 Curies. They may weigh anywhere from 80 pounds to two tons.<sup>1</sup> Although the entire RTG unit is not exceptionally mobile, scrap metal scavengers have succeeded in removing the actual source.

Wide ranges of radioactive sources are used in various industrial processes. Radiography sources are utilized to scan materials and determine the integrity of welds. These devices are always mobile, sometimes shielded, and may utilize  $^{137}\text{Cs}$ ,  $^{60}\text{Co}$ , or  $^{192}\text{Ir}$ .<sup>15</sup> Personnel unfamiliar with radiation and at remote construction sites often use

radiography, and it is not uncommon for a source to be lost at a work site or found in the bed of a stolen pickup truck.<sup>15</sup> Well-logging sources represent another RDD threat in the industrial use field. Containing a  $^{137}\text{Cs}$  source in the 15-20 Ci range and an americium-beryllium neutron source for activation analysis, over 10,000 of these devices are in use across the globe.<sup>15</sup> These devices are exceptionally mobile and are commonly transported between petroleum drilling sites by untrained hands. Gauge and luminescence sources represent the final threats. Gauges utilize radioactive sources to measure ambient conditions such as humidity, but the source strength is minimal.

The possibility exists that an adversary could attempt to purchase a radioactive source legitimately through commercial means. In fact, an investigative team from the Government Accountability Office (GAO) successfully obtained a specific source license for a bogus company existing only on paper in 2007. They were then able to enter into agreements with radioactive material suppliers to purchase enough  $^{241}\text{Am}$  to reach an IAEA category 3 level source.<sup>16</sup> Strict measures have been enacted by the Nuclear Regulatory Commission (NRC) and self-regulating agreement states to close this loophole. The issuance of licenses for large amounts of radioactive material must be accompanied by inspections to the site where the radioactive material is to be stored. However, a well-funded adversary, posing with a legitimate front company, may still be able to purchase a large radioactive source and divert it for RDD usage.

The final pathway for radioactive material acquisition includes the interdiction of a radioactive source during shipment. Radioactive sources are frequently shipped via land and ocean freight from source suppliers to sources consumers. Large food and

medical supply irradiators must be refueled twice a year. This constant stream of radioactive source shipments across the country, coupled with the fact that only a handful of companies actually supply radioactive materials, means that an adversary could have a reasonable chance of interdicting a shipment. The shipment of radioactive sources in large, protective flasks by companies such as MDS Nordion and REVISS helps to counter this threat; however, collusion with employees of source manufacturers and source carriers remains a significant concern.

### *Weaponization*

Weaponization of the radioactive materials used in an RDD presents a complicated set of pathways that an adversary may or may not choose to pursue. Unlike the acquisition of radioactive materials, which is rather straightforward due to public knowledge on the uses, locations, and types of commercially available sources, processing of radioactive sources can be approached from numerous directions. Based on the knowledge, technical capability, and funding of the adversary, processing of the radioactive material would allow an RDD to inflict significant human casualties and almost certainly disastrous economic consequences.

Processing of a source for RDD use would first consider the type of radiation emitted from the particular isotope within the source. The gamma rays emitted by sources such as  $^{137}\text{Cs}$  and  $^{60}\text{Co}$  are highly penetrating and pose an external exposure hazard to humans. On the other hand, the alpha particles emitted by sources such as  $^{241}\text{Am}$  and  $^{238}\text{Pu}$  cannot penetrate the skin and must be inhaled, ingested, or absorbed

into the blood through an open wound. Because of these characteristics, sources used in medicinal and industrial fields are fabricated into physical forms that are not inherently expedient to easy dispersal. Gamma ray sources are typically cast into relatively large, solid pieces of metal. For example,  $^{60}\text{Co}$  is formed into pencil shapes.  $^{137}\text{Cs}$ , on the other hand, is manufactured into a white powder. Alpha emitters are commonly cast into solids or sealed into metallic containers that prevent the material from escaping and posing ingestion or inhalation hazards.

Explosives attached to a pencil of  $^{60}\text{Co}$  would do little more than propel the source away from the detonation. While an exposure hazard would be present near the source, human casualties due to radiation would be minimal. Fragmenting the source into many shards or pellets prior to detonation would increase radiation exposure and spread material over a much larger area; however, the radiation danger would cease as the population exits the blast site. A third method of processing, and certainly the most dangerous, would grind the source into a powder with the goal of creating a persistent radioactive cloud. This cloud would be carried by wind and air currents away from the blast site and towards other population areas. Any humans exposed to the cloud would inhale the radioactive particles, which would become lodged in the body. Human casualties due to radiation, based on cloud movement, may be catastrophic.

Another aspect of the weaponization portion of the network includes obtaining shielding. Shielding serves two purposes. First, shielding would protect the adversaries from the radioactive emissions of the source while they construct the device. Previous RDD studies suggest that a device carrying 10,000 Curies of gamma ray radiation would

need roughly 310 pounds of lead shielding to protect those handling the device.<sup>17</sup> Based on the ultimate motivations and resources available to an adversary, they may or may not be concerned about self-protection. Secondly, shielding may be needed to block radioactive emissions from reaching radiation detectors installed in the target area. Large cities, government installations, military bases, and sporting events all have radiation detectors to prevent RDD attacks or detect the smuggling of nuclear weapons. The need for shielding is also dependent upon the type of radioactive material obtained. For example, a large amount of lead shielding is not necessary to stop weakly-penetrating alpha particles from certain sources. The presence of shielding would be more likely for highly-penetrating sources emitting gamma rays.

#### *Assembly and Detonation*

The final portion of the network considers various means a terrorist organization would take to disperse a radioactive source. Various combinations of high explosive, low explosive, and incendiary methods are included. The use of high explosives represents the most likely pathway; however, low explosives and incendiary methods would increase source vaporization and likelihood of inhalation. Each explosive pathway is split into specific subsets that, when integrated with real-time intelligence, can suggest which pathway an organization is pursuing towards the completion of an RDD. For example, Najibullah Zazi's search for an explosive based on oxidizer and fuel combinations was flagged by his scouring for hydrogen peroxide and nail polish remover in beauty supply stores during September of 2009.<sup>18</sup> Additionally, the

explosive method chosen may depend on the specific radioactive source obtained. A pathway involving the dispersal of an unprocessed alpha emitter such as  $^{241}\text{Am}$  would be weighted towards incendiary explosives to fully vaporize the weakly penetrating but highly-damaging alpha particles.

This portion of the network also considers delivery and detonation methods. Delivery nodes include vehicles, projectiles, and hand-carried methods. The inclusion of delivery and detonation methods is important to a pathways analysis of an RDD acquisition network since the chosen methods are likely dependent on previous paths the terrorist organization has taken. Terrorists utilizing an alpha emitter ground into small diameter particles might choose to use a timed projectile that detonates over a highly populated area. For a strong gamma emitter, the usage of a truck would allow for a greater amount of explosives to spread radiation over a wider area. Terrorists and insurgents in today's conflicts have demonstrated their aptitude at constructing highly effective explosive devices from crude and unconventional materials, and successful completion of these final nodes will ensure a successful RDD detonation.

#### *Final Device Probabilities and Characteristics*

The final portion of the network includes nodes that detail the adversary's chance of success and provide an overview of likely RDD characteristics. This portion of the network does not represent specific actions or decisions as in the previous four portions. Instead, these nodes provide the overall outcome of the pathways chosen. Four of these nodes provide overall chances of success for each of the four network tasks. They are

motivation to attempt an RDD attack, capability to obtain radioactive material, capability to weaponize the radioactive source, and capability to assemble and detonate the device. Next, these four probabilities are integrated to provide a final overall chance of success for a given plot. Each of the component probabilities does not uniformly contribute to the overall chance of success. The final outcome is heavily weighted towards the success of obtaining radioactive material. Furthermore, a low probability of successfully weaponizing the obtained source has little effect on the overall chance of success.

Three characteristics of the RDD are inferred from the adversary's path through the network. The inclusion of these nodes aids in identifying how specific actions by the adversary may eventually affect the outcome of a successfully acquired RDD. The three characteristics are device weight, overall danger from radioactive exposure, and overall panic inducing capability. Device weight is determined from the type of radioactive material acquired, the presence of shielding, the type of explosives, and the delivery method. A predicted device weight provides law enforcement agencies with a physical quantification of the suspected RDD. This information can be used to determine the size of the RDD, how many people would be needed to move such an item, and how feasibly the RDD can be delivered to various targets. A prediction of the overall danger from radioactive exposure should allow law enforcement to tailor their response prior to an RDD detonation, or better augment a response to an already detonated device. The various pathways to successful RDD acquisition imply that the danger from radioactive exposure is certainly not constant across different RDD designs.

Finally, a prediction of the overall panic inducing capability provides a measure of the level of fear and chaos the RDD will incite among the target population. Unlike many aspects of the produced network, this node is not influenced by the type of radioactive material utilized in the device or the level of source processing. The situation immediately after an RDD detonation is likely to be extremely hectic. Depending on the location of the detonation, and the use of any previously installed radiation detectors, the presence of radioactive materials might be detected within minutes to hours after the initial explosion. Initial panic induced by the RDD would likely be due to the delivery method and the type and amount of explosives used. Eventually, the panic level would increase as authorities release information detailing the presence of radioactive materials. Due to the general public's perception of radiation, this fear and panic is likely to be independent of the type of radioactive material released. Consequently, the node predicting the panic inducing capability of a successful RDD plot is mainly influenced by type of delivery method and the type of explosives.

### **Adversary Inputs**

The inclusion of information about the capabilities and resources of a particular adversary allow for the network to be customized to a specific RDD threat. Pathways chosen by the adversary and eventual chance of plot success are inherently dependent on the capabilities of the organization. The three adversary inputs are tactical capabilities, technical capabilities, and funding.



### *Tactical Capabilities*

The first input judges an adversary's tactical capabilities. Tactical capabilities include access to weapons, intelligence and surveillance abilities, and military type training. The level of tactical capability solely affects the radioactive material acquisition portion of the network. A tactically capable adversary is better suited to acquire radioactive material by penetrating facilities and stealing sources. On the other hand, an adversary with little tactical capability is more likely to attempt commercial acquisition of a radioactive source. This input includes three levels of tactical capability:

1. Novice: Access to no firearms or a small number of handguns. No surveillance or intelligence capabilities. No military training.
2. Criminal: Access to a moderate number of handguns, shotguns, and semi-automatic rifles. Ability to conduct covert surveillance on facilities containing radioactive materials. Ability to utilize open source information to develop targeting plans and exploit weak points of radioactive source containing facilities. Moderately trained in firearms usage. Capable of performing violent acts on par with organized, gang-related crimes.
3. Paramilitary: Access to a large number of handguns and automatic rifles. Access to a small number of rocket-propelled grenade launchers and small-caliber indirect fire weapons. Ability to conduct detailed surveillance and

collect specific intelligence about radioactive source security. Highly trained in firearms usage. Capable of implementing coordinated small-unit tactics.

### *Technical Capabilities*

The second input judges an adversary's technical capabilities. Technical capabilities are both a function of education level and presence of laboratory facilities. This input mainly affects an adversary's ability to process a radioactive source. However, advanced technical capabilities also increase the success an adversary may have in commercially acquiring a source. Advanced laboratory facilities may allow an adversary to pass a regulating inspection and obtain a license to purchase radioactive sources. An adversary's technical capability is judged by determining which of the available laboratory facilities most closely match the adversary's education level and technical facilities. For example, the capabilities of a high school laboratory would be equivalent to an adversary with a high school education and a poorly equipped laboratory facility. Technical capabilities are added into the network by equating the adversary to one of seven possible laboratory types:

1. No Technical Capabilities: No formal education. No laboratory facilities or processing equipment.
2. Garage Laboratory: Average adversary education level is high school or less. Rudimentary laboratory only containing hand tools.

3. High School Laboratory: Average adversary education is at the high school level. Poorly equipped laboratory containing hand tools, poor electronic equipment, and a minimal chemistry capability.
  
4. University Laboratory: Average adversary education is at the bachelor degree level. Well equipped laboratory containing hand tools, moderate electronic equipment, moderate chemistry capability, moderate fume hood processing capability, and a moderate amount of precise measuring devices.
  
5. Undeveloped Government Laboratory: Average adversary education is at the master degree level. Well equipped laboratory containing hand tools, moderate electronic equipment, advanced chemistry capability, advanced fume hood processing capability, and a moderate amount of precise measuring devices.
  
6. Technical Corporation Laboratory: Average adversary education is at the PhD level. Well equipped laboratory containing hand tools, advanced electronic equipment, advanced chemistry capability, advanced fume hood processing capability, and an advanced level of precise measuring devices.

7. Developed Government Laboratory: Average adversary education is at the PhD level with decades of experience. Well equipped laboratory containing hand tools, the most advanced electronic equipment, the most advanced chemistry capability, the most advanced fume hood processing capability, and the most advanced level of precise measuring devices.

### *Funding*

The third input judges an adversary's level of funding. It is important to note that the level of funding represents the amount of money the adversary is willing to devote to the RDD plot. A well-funded adversary who devotes minimal funding to an RDD plot would have little chance of success. The level of funding significantly affects all portions of the network. Sufficient funding permits an adversary to purchase resources in order to steal radioactive materials from various facilities. Also, funding could be utilized to purchase facility intelligence or to bribe an insider to collude either passively or actively. The possibility of commercial acquisition of radioactive materials also becomes more likely with a large amount of funding. Commercial acquisition would likely require thousands of dollars to purchase a source license and hundreds of thousands of dollars to purchase a high activity source. Funding also affects the type of explosives available to the adversary. A small amount of funding may require the adversary to construct homemade explosive mixtures from ammonium nitrate or chlorates. On the other hand, a well-funded adversary could purchase military grade

explosives. Finally, funding permits the purchase of more advanced delivery systems and RDD detonation components. The input for funding presents eight choices:

1. \$1,000
2. \$10,000
3. \$50,000
4. \$100,000
5. \$250,000
6. \$500,000
7. \$1,000,000
8. \$2,000,000

A general overview of the network's construction can be seen in Fig. 5. The top row of the figure depicts adversary motivations and adversary characteristics. Both of these inputs are utilized to characterize various adversaries. Adversary characteristics includes tactical capabilities, technical capabilities, and funding. The group of green boxes represent various tasks the adversary must complete to successfully detonate an RDD. These include radioactive material acquisition, source weaponization, and assembly and detonation. It is important to note that one pathway in Fig. 5 bypasses source weaponization. This represents the fact that this step is not mandatory to successfully acquire an RDD. The orange box represents the final outputs

of the created network. These outputs include device characteristics and success probabilities.

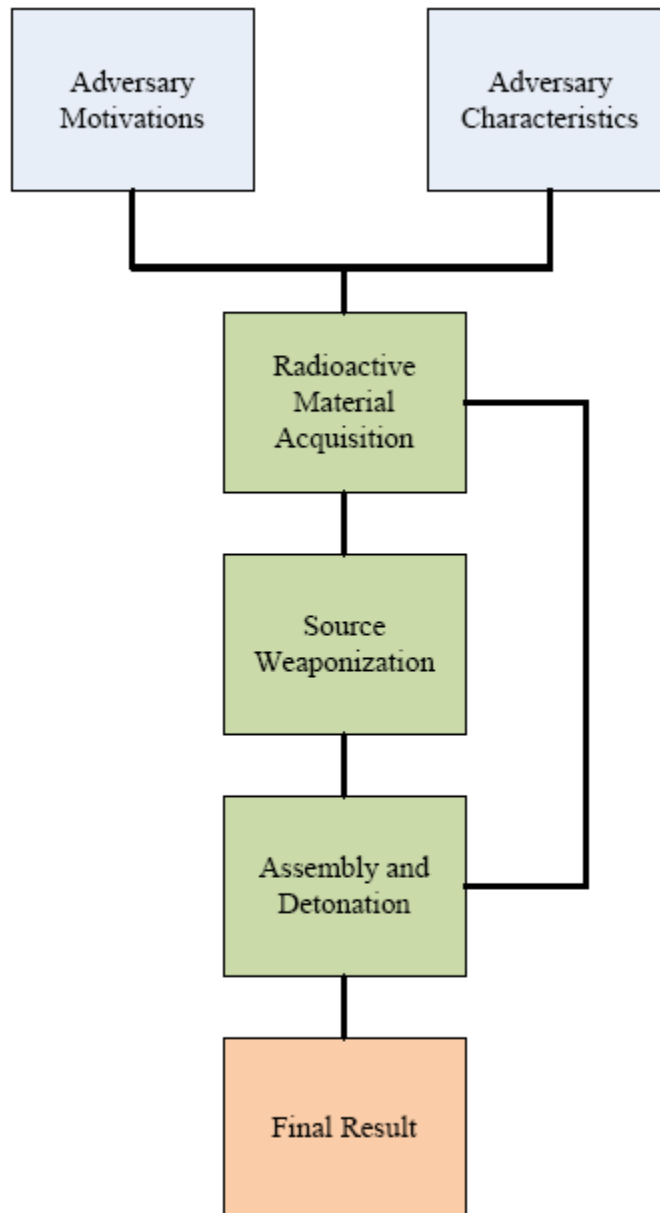


Fig. 5. General overview of the network's construction.

## Bayesian Analysis

Bayesian networks, or belief networks, are a method of understanding probabilistic models. What makes Bayesian networks unique as a probabilistic modeling tool, however, is the fact they can account for prior probabilities when determining the likelihood of an action, decision, or outcome occurring.<sup>19</sup> A Bayesian network, when modeling an interconnected system, can have its beliefs updated as more information is added. Consequently, the ultimate effect of a small system change can easily be determined. Bayesian analyses are valid in all probabilistic interpretations; however, they are frequently used in science and engineering.<sup>20</sup> The most prevalent use of Bayesian networks occurs in analytical medical diagnostics.<sup>21</sup>

The central concept of a Bayesian network is Bayes' Theorem.<sup>22</sup> Thomas Bayes was an eighteenth century clergyman who surmised that so-called conditional probabilities could account for the effects of prior evidence in a network. Let  $A_i$  denote one of  $n$  events, and  $E$  be some evidence about the network; then, Bayes' theory can be written as:

$$P(A_i|E) = \frac{P(A_i)P(E|A_i)}{\sum_{i=1}^n P(A_i)P(E|A_i)} \quad (1)$$

where  $P(A_i|E)$  is the probability of  $A_i$  given  $E$ ,  $P(A_i)$  is the prior probability of  $A_i$ , and  $P(E|A_i)$  is the conditional probability of  $E$  when  $A_i$  is true.<sup>23</sup>

An article entitled "The Use of Bayesian Networks in Decision-Making" appearing in *Key Topics in Surgical Research and Methodology* presents a common

example used to illustrate Bayesian analysis.<sup>23</sup> This example analyzes how the addition of evidence, in the form of an x-ray scan, changes the probability that a patient has tuberculosis. Initial diagnosis by the doctor suggests that the patient has a 30% chance of having tuberculosis. This 30% probability represents the prior probability, or  $P(A_i)$  in Eq. 1. Next, the doctor calls for an x-ray scan to help confirm or deny the condition. Previous experience shows that an abnormal x-ray is observed in 90% of patients with tuberculosis and 10% of patients without tuberculosis. As expected, an abnormal x-ray does not conclusively prove a patient has tuberculosis, and a normal x-ray does not conclusively prove a patient does not have tuberculosis. A conditional probability table can then be written to show this data. Table I shows the conditional probability table for the diagnosis of tuberculosis with an x-ray.

TABLE I  
Conditional probability table for the diagnosis of tuberculosis with an x-ray.

X-ray	Tuberculosis Present (%)	Tuberculosis Absent (%)
Normal	10	90
Abnormal	90	10

Bayesian analysis and the conditional probability table aid in quantifying the effect of adding evidence for the x-ray. Assume that the doctor finds the x-ray is normal. Intuitively, the doctor knows that the patient's chance of having tuberculosis has dropped below the prior 30% diagnosis with the evidence of a normal x-ray.



However, what is the actual chance? Bayes' Theorem says that the probability of tuberculosis, given a normal x-ray result and a 30% prior probability, is only 4.54%:

$$4.54\% = \frac{(0.30 \times 0.10)}{((0.30 \times 0.10) + (0.70 \times 0.90))} \times 100\% \quad (2)$$

Equation 2 demonstrates the calculation of the new probability through the use of Eq. 1. This quantification ability of Bayesian networks has far-reaching consequences. The benefit to medical fields is readily apparent. Often, it's much more comforting for a patient to hear the doctor quantify their diagnosis with a small probability. In a complicated medical situation, the integration of medical test evidence and symptoms in a Bayesian network can provide a simple diagnosis that may be beyond the qualitative capabilities of the diagnosing doctor. While medicine pioneered the use of Bayesian analysis, many mathematical, scientific, and defense fields are adopting this flexible tool.

A Bayesian analysis is an ideal method to develop an intelligence tool analyzing the acquisition of RDDs for three reasons. First, Bayesian analysis can be performed on complex networks with thousands of nodes. These networks can be constructed to provide an overall probability of success for a complex action or decision. Consequently, Bayesian analysis of RDD acquisition allows for analysts to derive an overall chance of plot success based on inputs describing the adversary. Without a Bayesian approach, an analysis of this type would be complicated and time consuming.

Secondly, Bayesian networks can integrate evidence and accomplish the difficult task of instantaneously updating all probabilities across the network. Types of evidence

about an RDD plot are numerous. Untrained analysts may not recognize how certain evidence affects various portions of the network. Thus, an accurate Bayesian analysis of RDD acquisitions would allow analysts to concentrate on assessing the actual threat, rather than attempting to determine how specific evidence affects the network.

Finally, a Bayesian analysis of RDD acquisitions can provide signals or flags that allow law enforcement agencies to focus their efforts on stopping the threat. The addition of evidence into a Bayesian network instantly updates all other probabilities within the network. For example, evidence about a certain radioactive material acquisition may change the probability that an adversary will attempt to obtain a certain type of homemade explosive. This information can be shared with law enforcement agencies, who can scour sources for the ingredients of the homemade explosive. These signals, or plot flags, facilitate the focusing of a small number of resources in a limited timeframe.

A Bayesian network analysis of RDD acquisitions does have a few downsides. All calculations performed in the updating of a Bayesian network are derived from conditional probability tables programmed into the network. Consequently, any results derived from the network are only as good as the coded conditional probabilities. Case studies are utilized to rectify these potential uncertainties. By analyzing case studies with expected answers, the conditional probabilities can be adjusted until the network provides the expected results. Once the Bayesian network results have been vetted and the conditional probabilities adjusted, it can then be used to analyze potential or current RDD acquisition plots with some degree of confidence.

## **Netica**

Many software packages are available to build and analyze Bayesian networks. On such package, called *Netica*, was utilized to perform the Bayesian network analysis of RDD acquisitions presented in this work. *Netica* boasts a user-friendly graphical interface and an ability to perform complex sensitivity analyses.<sup>24</sup> Additionally, *Netica* allows the inclusion of special constant nodes within a Bayesian network. These nodes have no associated conditional probabilities. Instead, their constant values can be called on to influence other nodes within the network. By adjusting the constant node's value to reflect characteristics of an adversary, a few simple clicks can quickly adjust a Bayesian network to permit analysis of RDD plots by various adversaries. Other Bayesian analysis software excludes this key feature so vital to an effective RDD acquisition analysis.

### *“Asia” Example Network*

The *Netica* software package includes a sampling of example Bayesian networks as tutorials. The most popular example Bayesian network is named “Asia” and is shown in Fig. 6. “Asia” is a simple tool used to diagnose a lung condition. The analysis of this simple Bayesian network is a useful exercise before attempting to understand the complex network depicting RDD acquisitions. Individual network nodes in *Netica* are depicted as yellow rectangles. Nodes are given a title and any number of states. In “Asia”, each node has only two states. Each state is a possible outcome of the observation described by the node's title. For example, the node “Smoking” includes the

two states “Smoker” and “NonSmoker.” Each node also shows the probability of each state being true. “Asia” assumes that, without the addition of any evidence, a patient has a 50% chance of being a smoker. The black lines connecting the nodes are called links. The arrow of the link points from the parent node to the child node. Consequently, the node “Visit To Asia” is a parent of “Tuberculosis” and the node “Smoking” is a parent of both “Lung Cancer” and “Bronchitis.” This parent-child relationship depicts how the nodes interact with each other. A visit to Asia affects the chance of a patient having tuberculosis. On the other hand, smoking affects the chance of a patient having either lung cancer or bronchitis. Parent nodes affect their children, their children’s children, and so on. Parent nodes do not directly affect other parents of their children. Evidence of high pollution will increase the chance of lung cancer. However, evidence of high pollution will not directly affect the chance that the patient smokes.

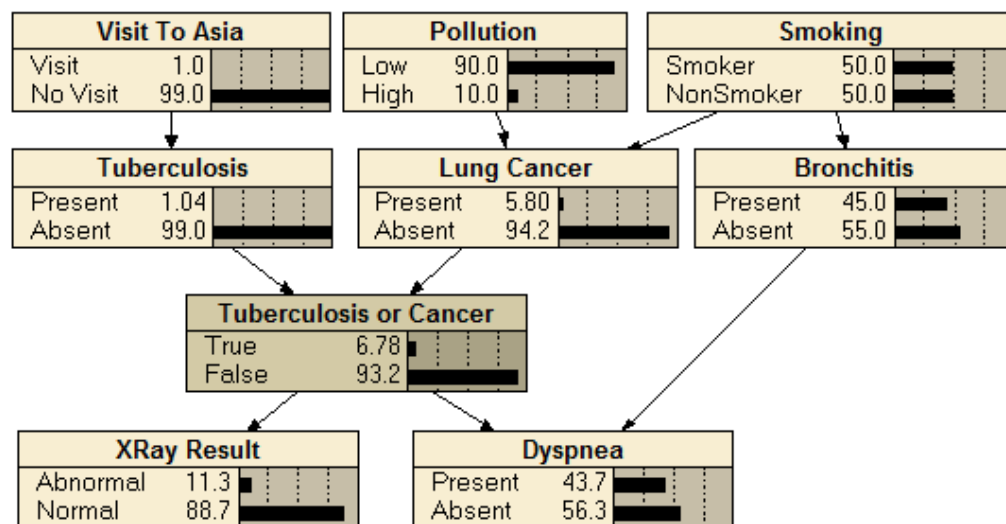


Fig. 6. “Asia” Bayesian network provided as an example within Netica.

The nodes within “Asia” are organized into risk factors, conditions, and symptoms. The top row of nodes represent risk factors (“Visit to Asia,” “Pollution,” and “Smoking”), the second row represents possible conditions (“Tuberculosis,” “Lung Cancer,” and “Bronchitis”), the third row represents a combination of conditions (“Tuberculosis or Cancer”), and the bottom row represents observable symptoms or evidence (“XRay Result” and “Dyspnea”). Analysis of the “Asia” network informs doctors of likely patient conditions based on available evidence. The default network risk factors are a 1.0% chance of a visit to Asia, a 90% chance of low pollution, and a 50% chance of smoking. These risk factors contribute to a 1.04% chance of tuberculosis, a 5.8% chance of lung cancer, and a 45% chance of bronchitis.

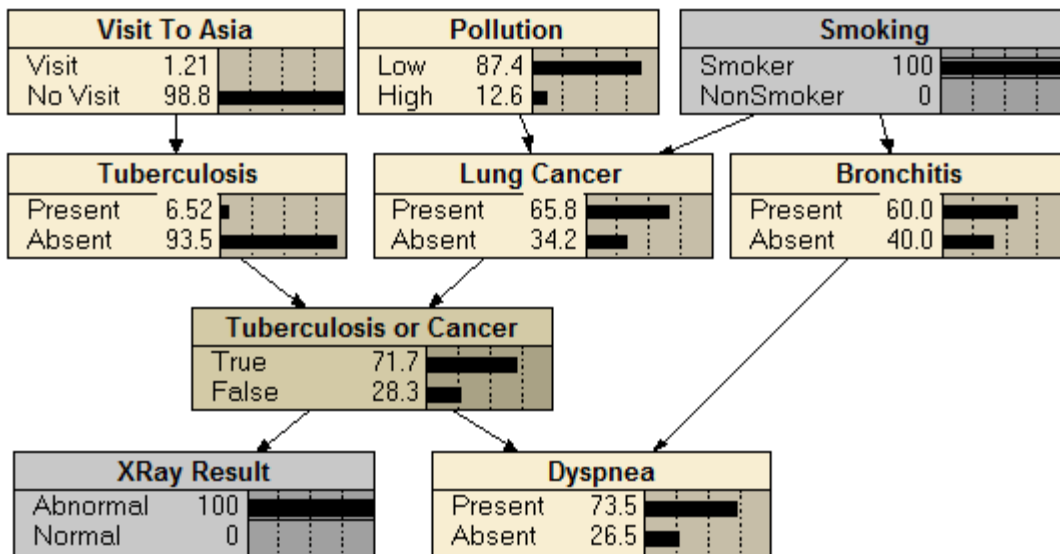


Fig. 7. “Asia” network with the addition of evidence for a smoker with an abnormal X-ray.

The use of “Asia” as a static probability model is helpful in predicting the chance of disease based on constant probabilities. However, the addition of evidence to “Asia” demonstrates how Bayesian networks can be used as dynamic tools to model various situations. Figure 7 depicts “Asia” with the addition of two pieces of evidence. Imagine a patient has entered the clinic with chest pain. The patient is a smoker. To gather more information, the doctor orders an x-ray and the results are abnormal. These two pieces of information are then entered into “Asia.” *Netica* displays the addition of evidence into nodes by changing their color to gray. Notice that the nodes “Smoking” and “XRay Result” have turned gray and the respective smoker and abnormal states now read a 100% probability. This evidence suggests that the patient has a 6.52% chance of tuberculosis, a 65.8% chance of lung cancer, and a 60% chance of bronchitis. As expected, evidence of smoking and an abnormal x-ray significantly increase the chance of lung cancer. The chance of tuberculosis remains relatively low, since its parent has not changed. However, the chance of tuberculosis did increase from 1.04% to 6.52% due to the evidence of an abnormal x-ray.

The authors of “The Use of Bayesian Networks in Decision-Making” suggest investigating the addition of evidence to the “Asia” network through the use of a cumulative belief curve.<sup>23</sup> A cumulative belief curve is constructed by adding evidence subsequently to the network and analyzing the effect on a specific node. An analysis of the risk of lung cancer as evidence of smoking, dyspnea, an abnormal x-ray, and a visit to Asia are added to the network is seen in Fig. 8. The figure depicts the expected result of a 5.8% chance of lung cancer with no evidence added to network. However, with the

cumulative addition of smoking, dyspnea, and an abnormal x-ray, the chance of lung cancer grows to 10.5%, 15.5%, and 73.4%, respectively. The final evidence of a visit to Asia has a startling effect. The risk of lung cancer actually decreases to 59.2%. How can this be since a visit to Asia has no link to lung cancer? This occurs since a visit to Asia increases the chance of tuberculosis. The resulting increase in the chance of tuberculosis provides an alternate explanation for the evidence of an abnormal x-ray and dyspnea. This subsequently decreases the chance of lung cancer. Fig. 8 demonstrates that while a parent cannot directly affect another parent of its child, it can have an indirect effect upon the addition of evidence into the network. This has important implications for more complicated Bayesian networks, such as the one created for this work to model RDD acquisitions. Introduction of evidence for a certain RDD pathway will decrease the likelihood of other pathways. This effect epitomizes the utility of a Bayesian analysis approach to RDD acquisitions.

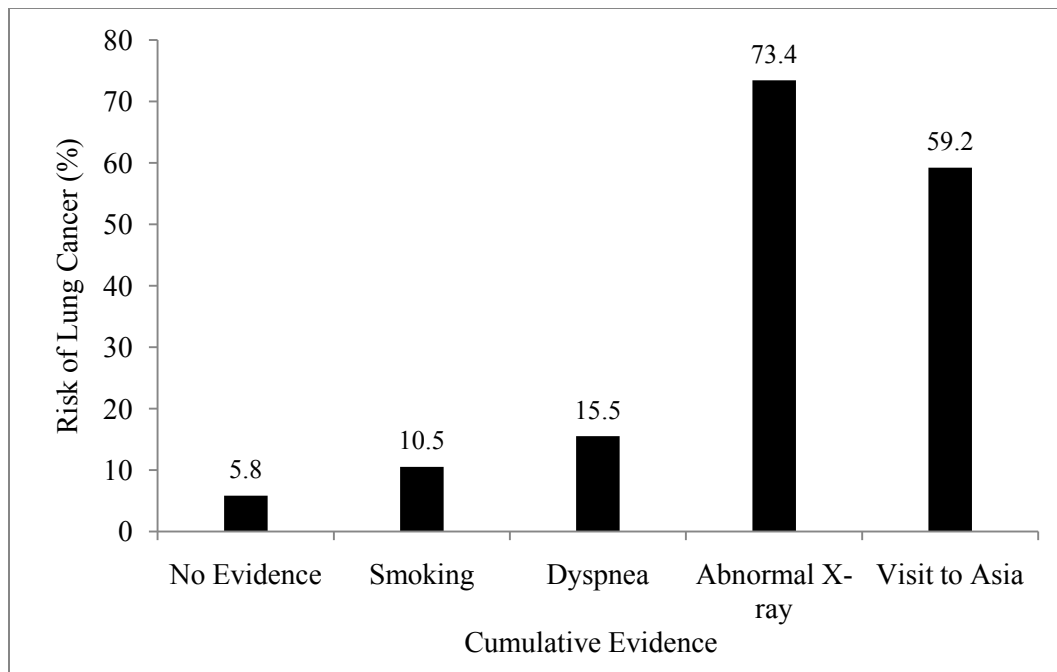


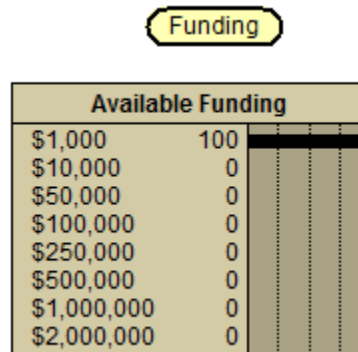
Fig. 8. Cumulative belief curve of risk of lung cancer based according to “Asia”.

### *Constant Nodes*

Constant nodes provide values that can be utilized by all nodes within a *Netica* Bayesian network. Unlike other nodes within the network, constant nodes are unlinked and do not change as evidence is added. Constant nodes are deterministic in the fact that they can have only one active state at a time. However, the user can easily switch between states when desired. As the state is switched, all nodes that utilize the value embedded in the constant node will adjust. This property facilitates the flexibility that allows a Bayesian analysis of RDD acquisitions to analyze different adversaries and plots with minimal user input. Three constant nodes are utilized in the constructed RDD



acquisition network to describe the three adversary inputs previously described: tactical capabilities, technical capabilities, and funding.



Available Funding	
\$1,000	100
\$10,000	0
\$50,000	0
\$100,000	0
\$250,000	0
\$500,000	0
\$1,000,000	0
\$2,000,000	0

Fig. 9. Constant node used to describe available adversary funding.

Figure 9 depicts a constant node used to describe the funding available to an adversary's RDD plot. The actual constant node is the smooth-cornered rectangle with the title "Funding." Below the constant node is a deterministic node linked to the constant node's value. This node is merely included to indicate to the user the current state of the constant node. As shown in Fig. 9, this constant node is currently set to a state that describes a funding level of \$1,000. Figure 10 displays the properties of the constant node. The text box shows that this constant node has eight separate states. Each of these states corresponds to a level of plot funding: \$1,000, \$10,000, \$50,000, \$100,000, \$250,000, \$500,000, \$1,000,000, and \$2,000,000. These states are assigned a respective value, varying from 0.05 for the \$1,000 state to 1 for the \$2,000,000 state.

When a constant node is called from within the network to calculate a node's probabilities, the value corresponding to the constant node's current state will be used. For example, this constant node is utilized within the RDD acquisition network to determine the likelihood of an adversary obtaining radioactive material through commercial acquisition. If the constant node is set to \$1,000, representing a poorly-funded adversary, a value of 0.05 will be used in an equation to calculate a low probability of commercial acquisition. On the other hand, if the constant node is set to \$2,000,000, representing a well-funded adversary, a value of 1 will be used in an equation to calculate a much higher probability of commercial acquisition. With the establishment of a constant node and a respective value for each state, probabilities within the network can be fine tuned by changing the equation that calls the constant node's value. The use of equations to calculate probabilities is discussed in the following section.

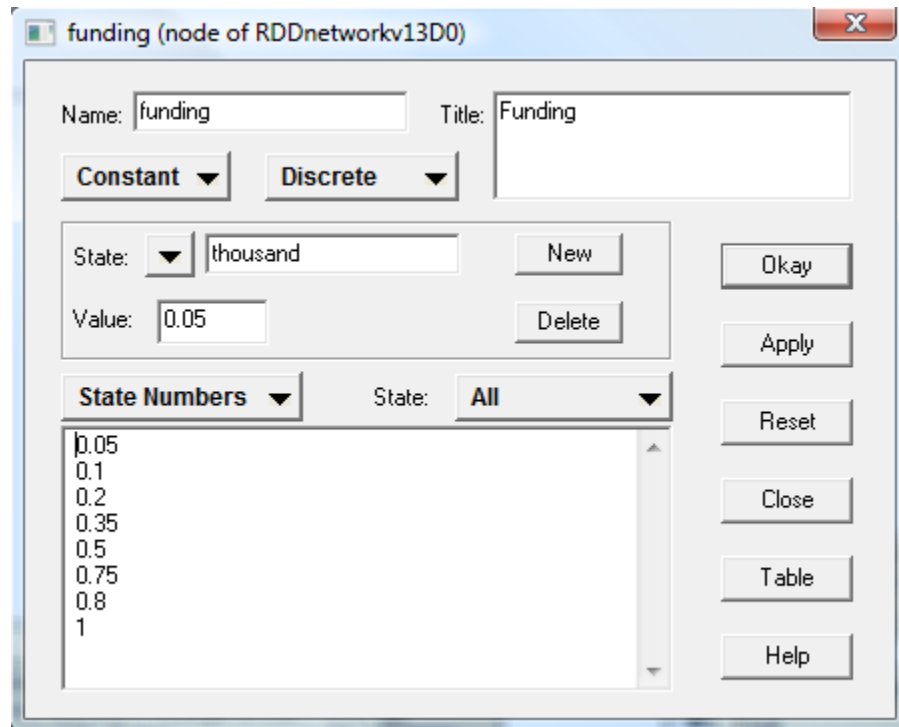


Fig. 10. State values of the “Funding” constant node.

### *Conditional Probability Tables*

*Netica* updates the node probabilities within a Bayesian network by utilizing conditional probability tables entered by the user. Conditional probability tables are also called truth tables. These tables are not unlike the crude example shown in Table I depicting the presence of tuberculosis from the result of an x-ray. *Netica* allows two methods of constructing truth tables. The first method involves entering each conditional probability individually. This is an easy process for a simple truth table like the one presented in Table I. However, for nodes with multiple parents, the number of entries in the truth table increases into the thousands. This makes cell-by-cell entry infeasible. The second method permitted by *Netica* is the use of Boolean logic

equations. After a logic equation is written into a node's properties, *Netica* automatically calculates each entry in the truth table. This method makes short work of an otherwise unwieldy task that could take years to accomplish by hand.

Truth table construction by hand will be demonstrated by using examples from the RDD acquisition network constructed in *Netica*. Figure 11 depicts a small portion of the network including nodes that account for evidence of an adversary obtaining thermite to utilize in an RDD. The "Thermite Purchased" and "Thermite Stolen" nodes represent specific actions that the adversary can perform. Both of these nodes indicate evidence that the adversary is attempting to utilize thermite. The "Thermite Evidence" node is the parent of the two evidence nodes, and serves to represent the overall evidence of thermite. Finally, the "Incendiary Device Type" node is a parent of the "Thermite Evidence" node and the "Pryophoric Evidence" node (not shown). This node serves to represent which type of incendiary device (either thermite or pyrophoric) is most likely. The state labeled "none" represents the fact that another explosive type is currently more likely than an incendiary device.

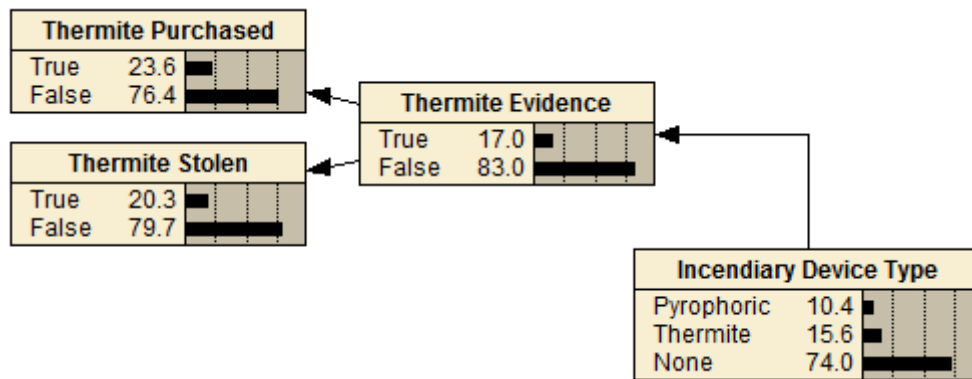


Fig. 11. Nodes depicting evidence of thermite as an incendiary device type.

The truth table governing the calculation of the “Thermite Evidence” node is seen in Fig. 12. By right-clicking on the node within *Netica* and selecting “Table...” the truth table can be adjusted in a similar fashion to a Microsoft Excel spreadsheet. The column on the left is titled “Incendiary Device Type” and lists the three states of that node. This node is the parent of the “Thermite Evidence” node, and parent nodes will always appear in this column while editing truth tables. Cells containing numbers in Fig. 12 show how the “Incendiary Device Type” node is affected by the “Incendiary Evidence” node. A “True” state of the “Incendiary Evidence” node will result in a “Thermite” state 98% of the time. A “False” state will result in a “Thermite” state only 2% of the time. On the other hand, a “False” state in the “Thermite Evidence” node will result in a “Pyrophoric” and “None” state 98% of the time. These probabilities ensure that evidence of a thermite device correctly affects the proper state of the “Incendiary Device Type” node. Like the example presented in Fig. 12, most evidence nodes within the RDD network are linked to their parents probabilistically instead of

deterministically. Generally, a deterministic relationship places too much emphasis on evidence nodes and can severely dampen other portions of the network when evidence is added.

Therm Table (in net RDDnetworkv13D0)

Node: Therm

Chance % Probability

Apply Okay

Reset Close

Incendiary Device Type	True	False
Pyrophoric	2	98
Thermite	98	2
None	2	98

Fig. 12. Truth table depicting evidence of thermite as an incendiary device type.

As previously mentioned above, truth tables can be calculated by *Netica* if the relationship between nodes is described by the user with Boolean logic equations. This method is utilized if the truth table is complex, or if the node's probabilities call on the value of a constant node. Fig. 13 depicts a node within the constructed Bayesian network named "Process Outcome." This node characterizes the type of source processing performed by the adversary in the source weaponization portion of the network and includes four states: "Solid," "Fragments," "Powder," "Solution," and

“None.” The eight small circles seen in Fig. 13 are minimized nodes that call on constant values within the network. The value in each of these nodes is calculated with a Boolean logic equation utilizing the currently selected value of the constant node. This implementation allows the network to quickly adjust the values of certain nodes to reflect the characteristics and capabilities of various adversaries.

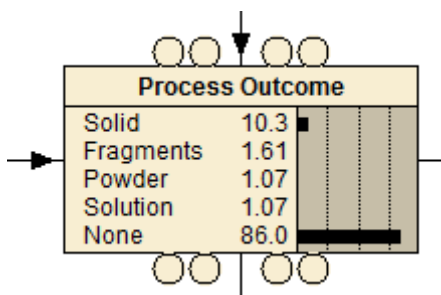


Fig. 13. “Process Outcome” node whose probabilities are calculated by a Boolean logic equation and constant nodes.

### Network Construction

A Bayesian network was constructed in *Netica* to analyze RDD acquisitions. The network includes 291 probability nodes describing the pathway to successful RDD construction and three constant nodes allowing for inputs describing the characteristics of the modeled adversary. Additionally, the network is broken into five general sections: adversary inputs and motivations, radioactive material acquisition, source weaponization, assembly and detonation, and final RDD design characteristics and overall chance of success. The entire network can be seen in Figs. 14 to Fig. 41.

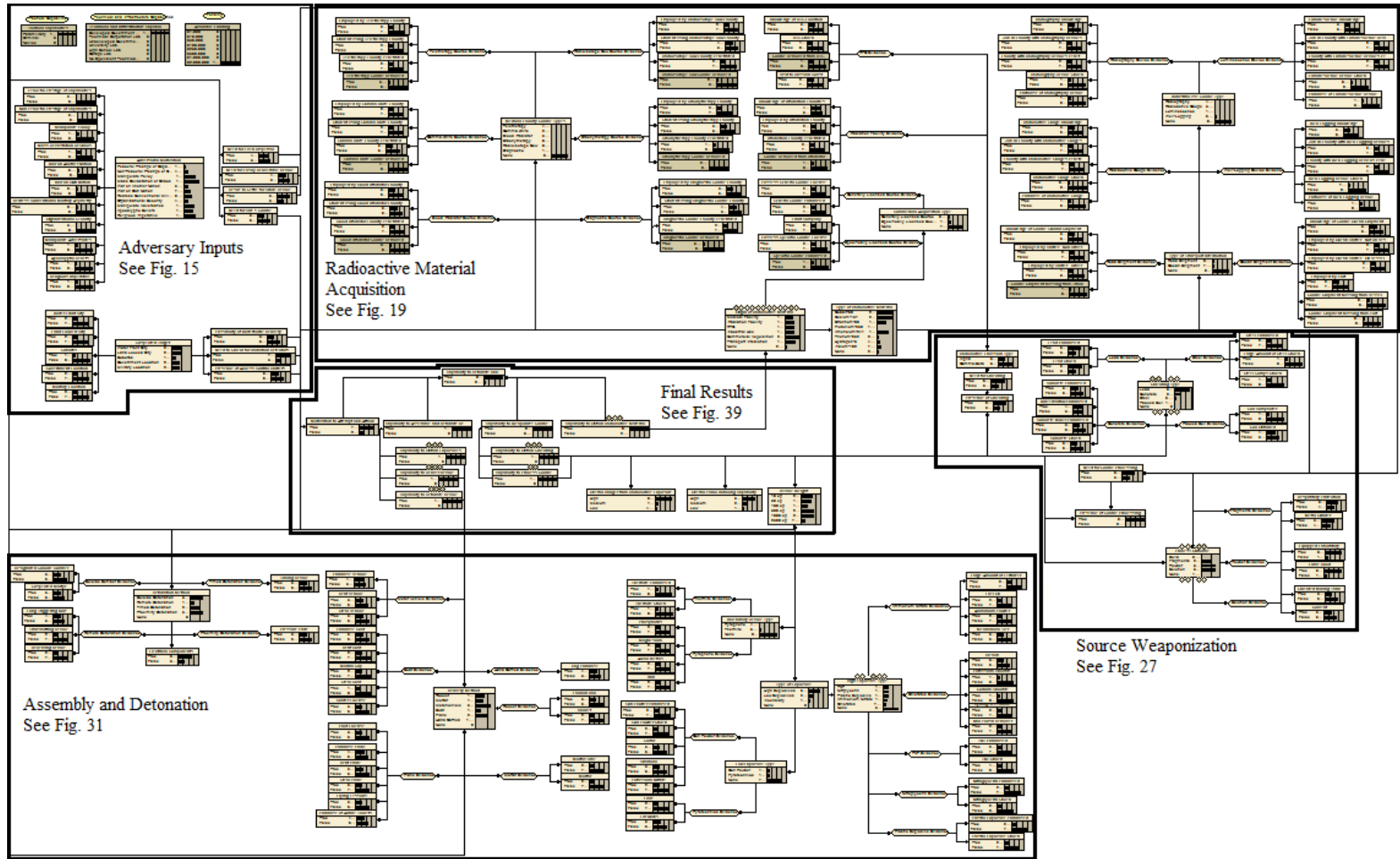
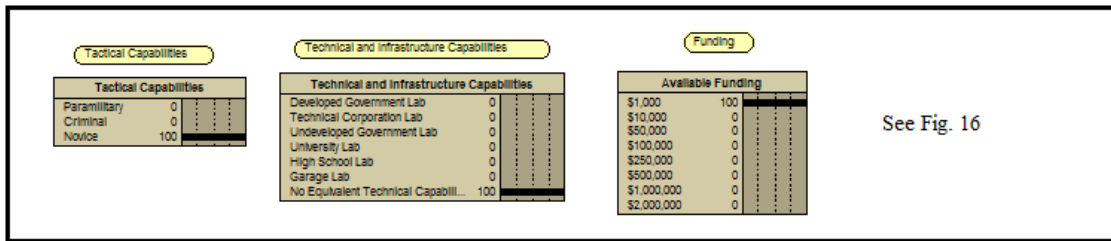
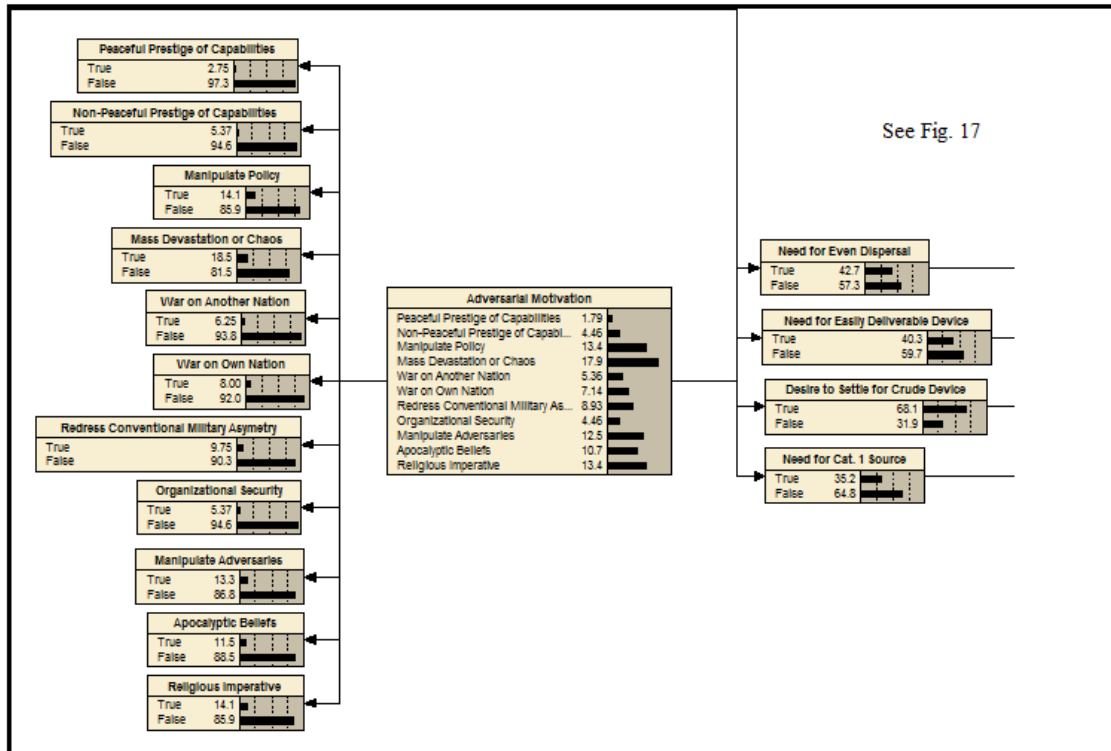


Fig. 14. Overview of RDD acquisition network.

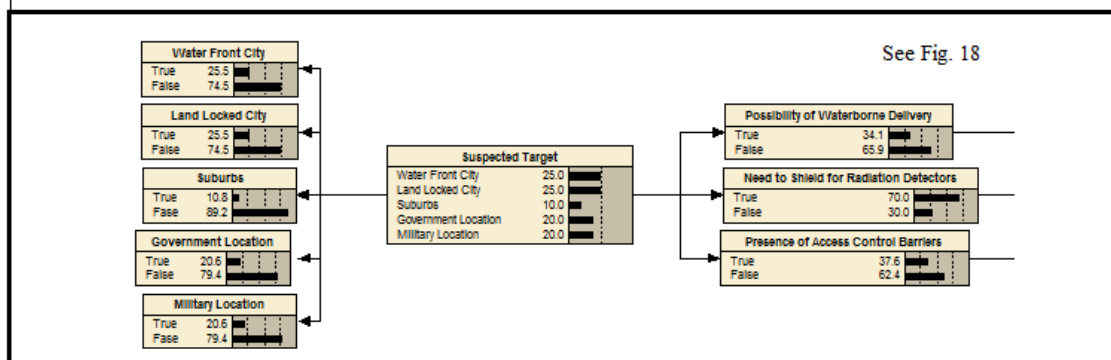




See Fig. 16



See Fig. 17



See Fig. 18

Fig. 15. Overview of adversary inputs and motivations section.

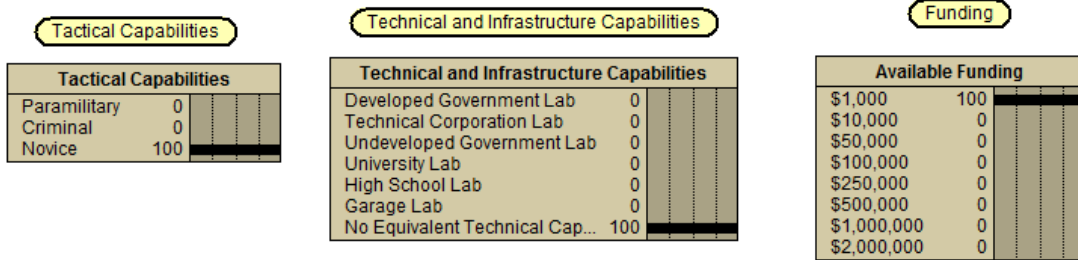


Fig. 16. Adversary input portion of adversary inputs and motivations section.

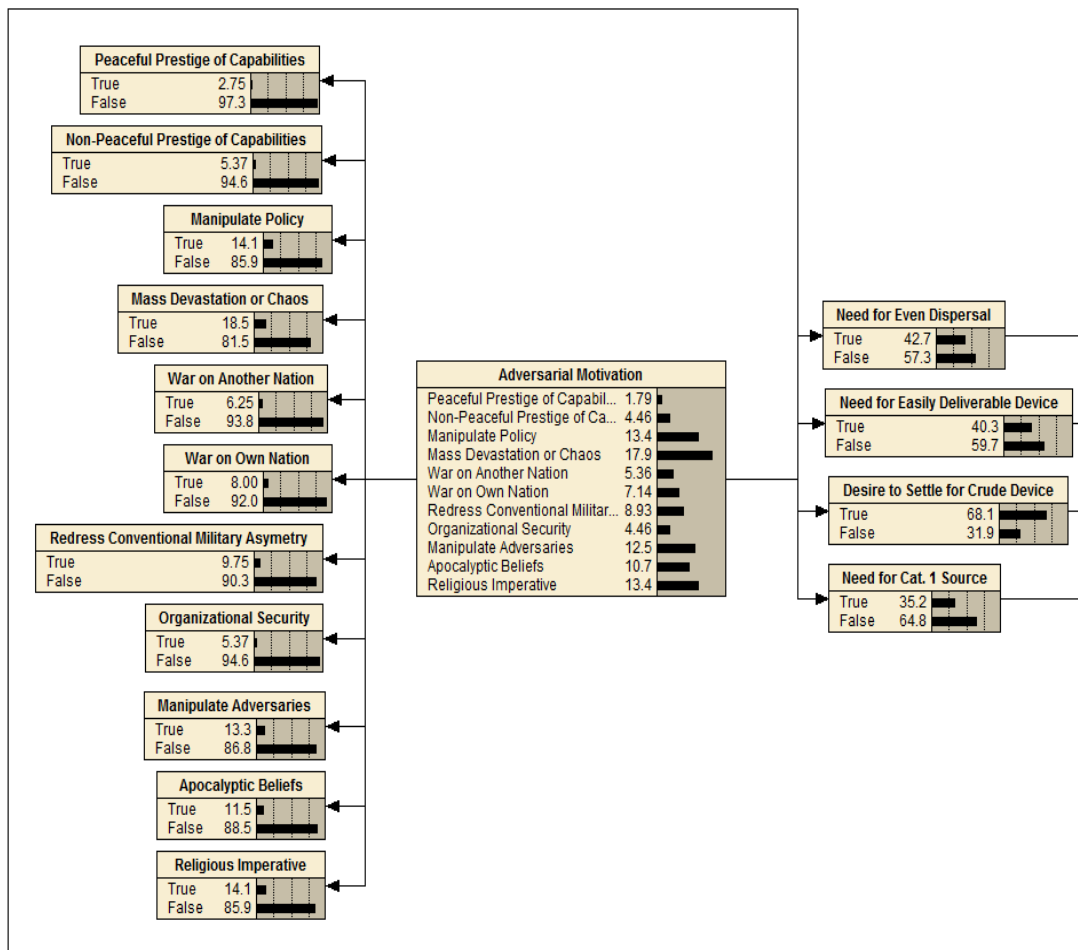


Fig. 17. Adversary motivation portion of adversary inputs and motivations section.

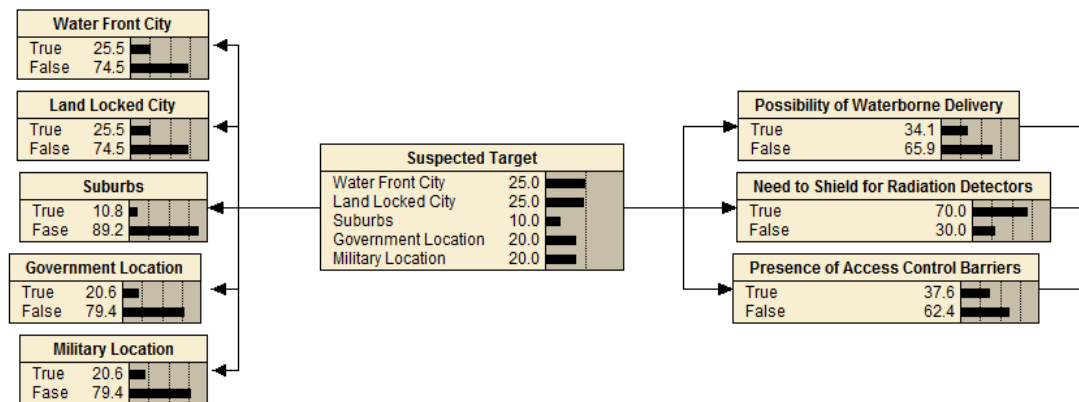


Fig. 18. Suspected target location portion of adversary inputs and motivations section.

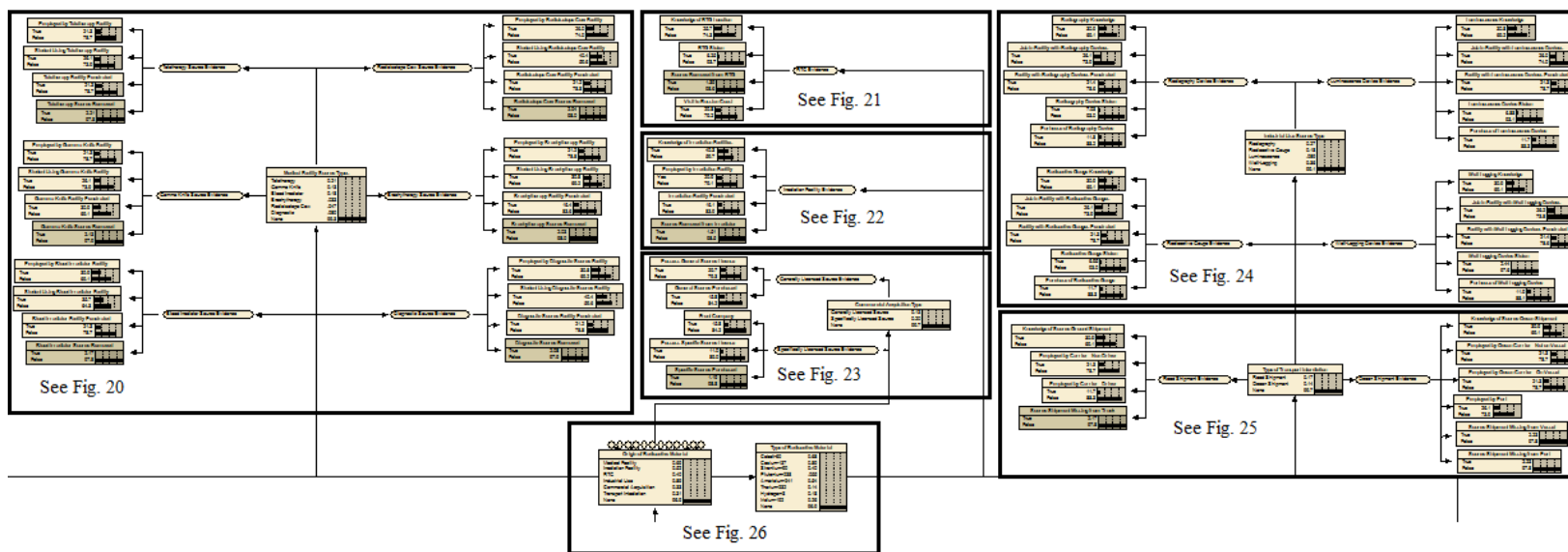


Fig. 19. Overview of radioactive material acquisition section.

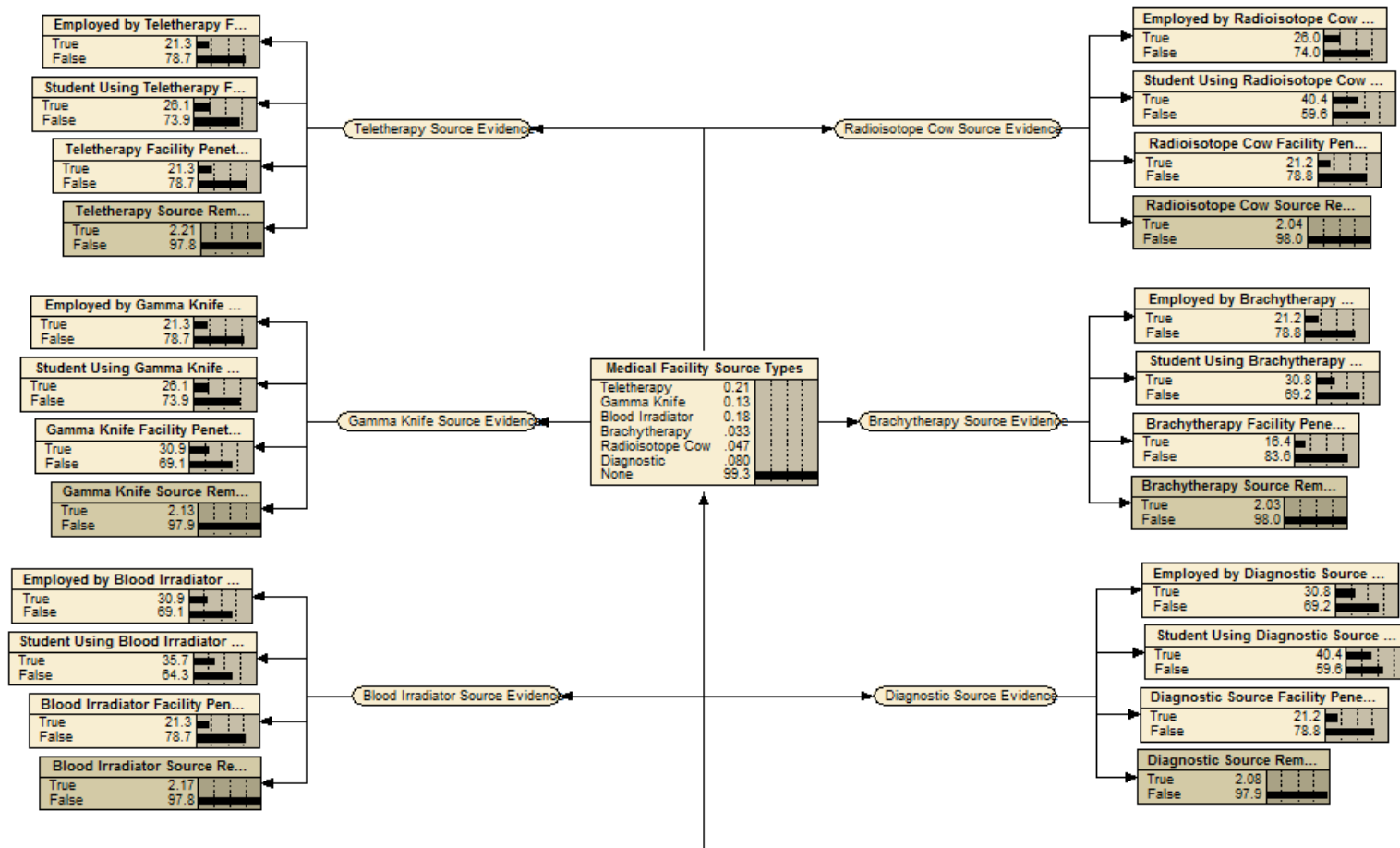


Fig. 20. Medical facility portion of radioactive material acquisition section.

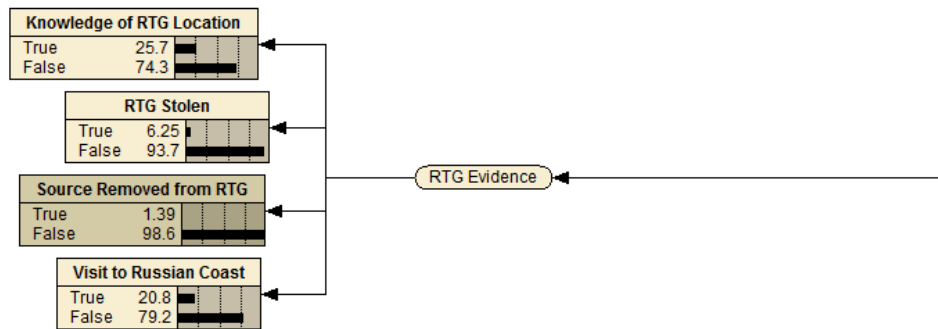


Fig. 21. RTG portion of radioactive material acquisition section.

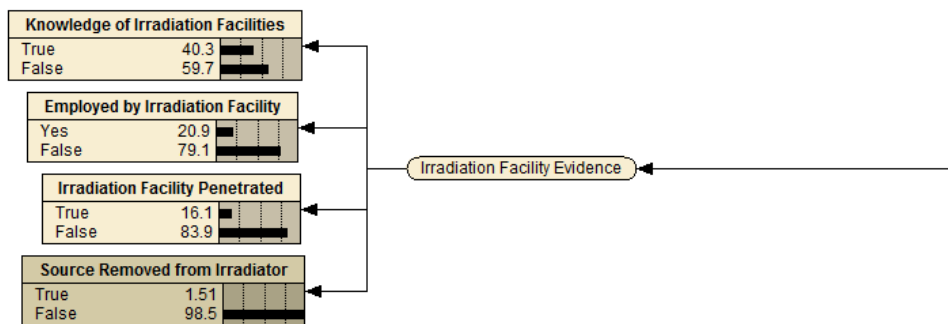


Fig. 22. Irradiation facility portion of radioactive material acquisition section.

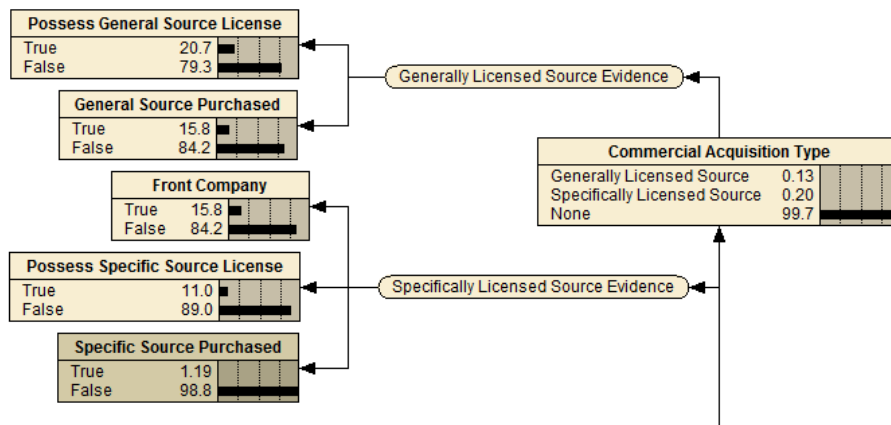


Fig. 23. Commercial acquisition portion of radioactive material section.

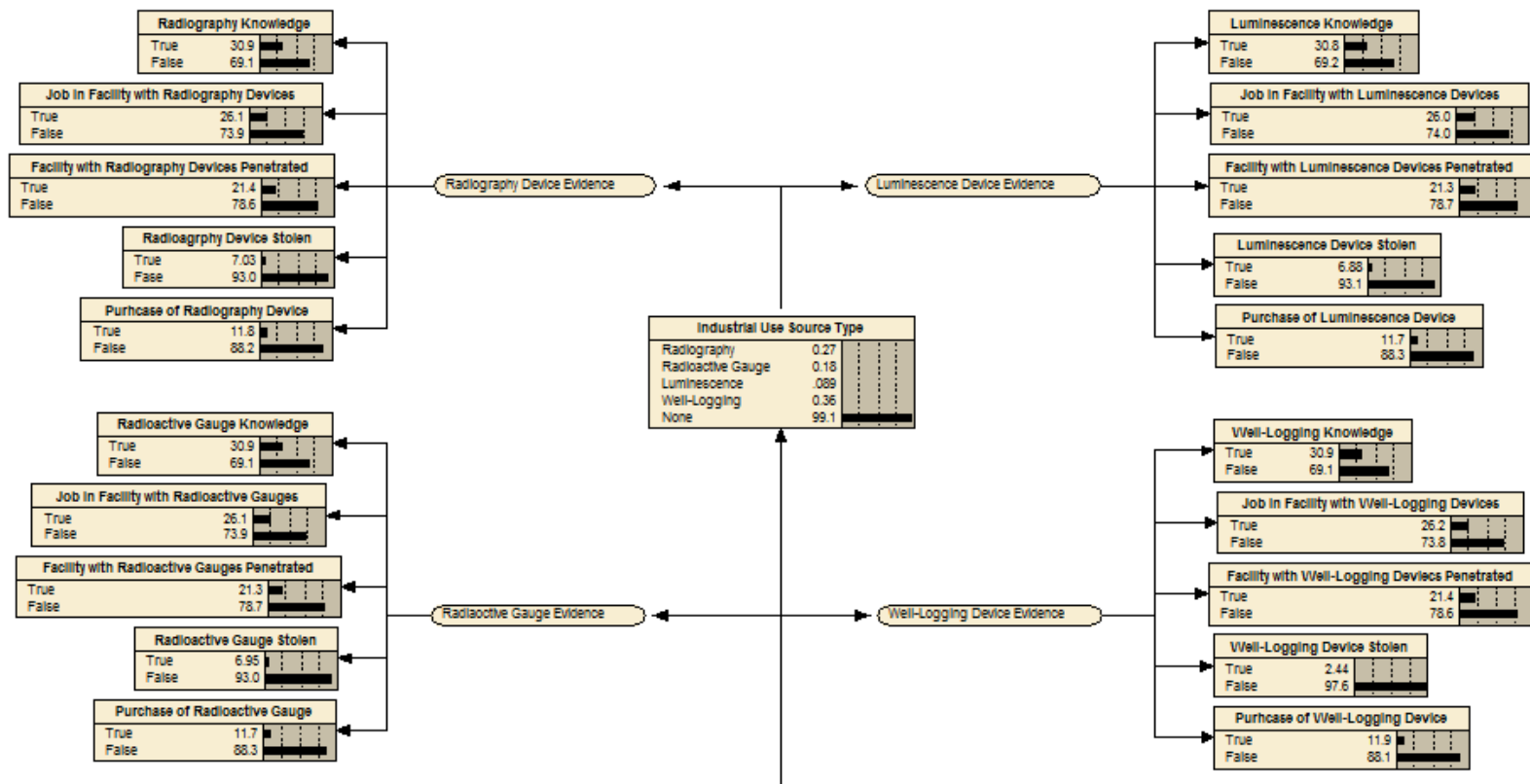


Fig. 24. Industrial use portion of radioactive material acquisition section.



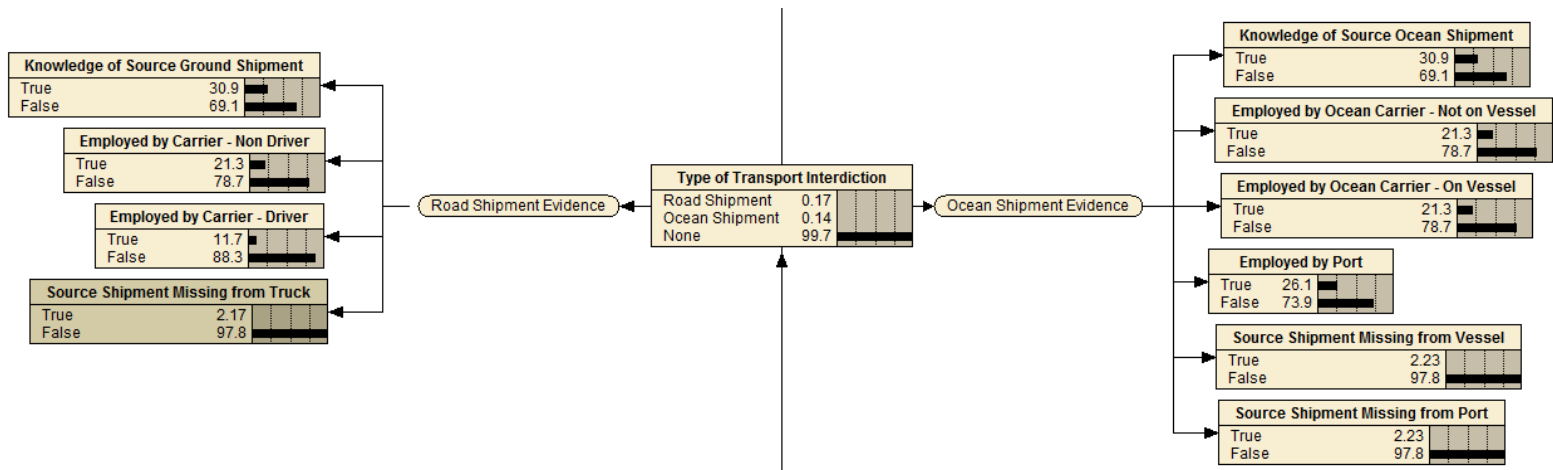


Fig. 25. Transport interdiction portion of radioactive material acquisition section.

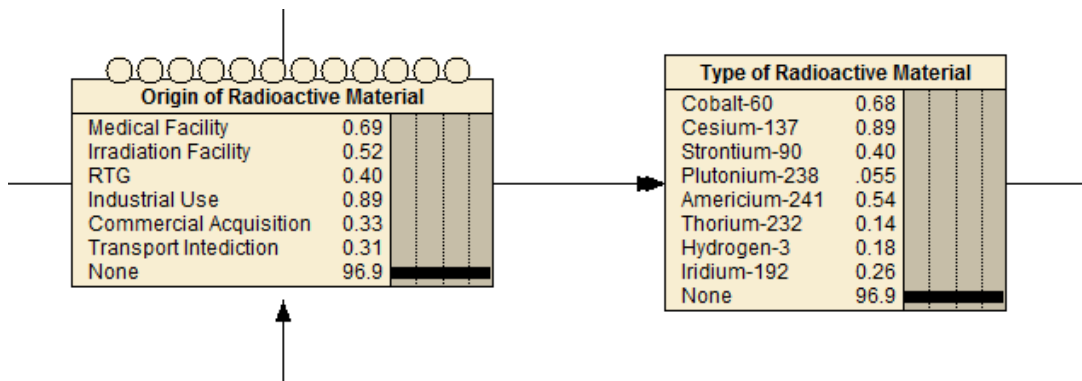


Fig. 26. Radioactive material summary portion of radioactive material acquisition section.

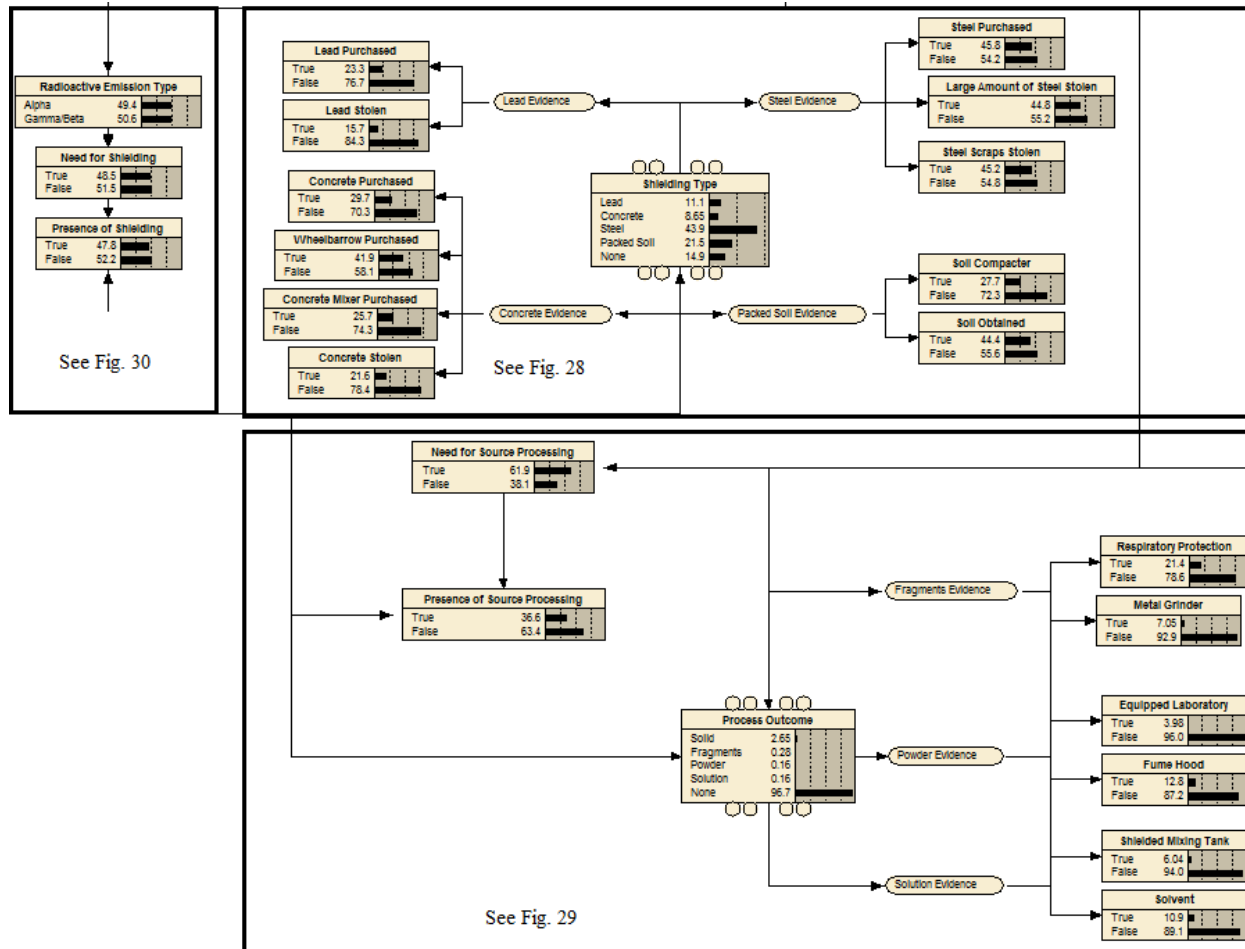


Fig. 27. Overview of source weaponization section.

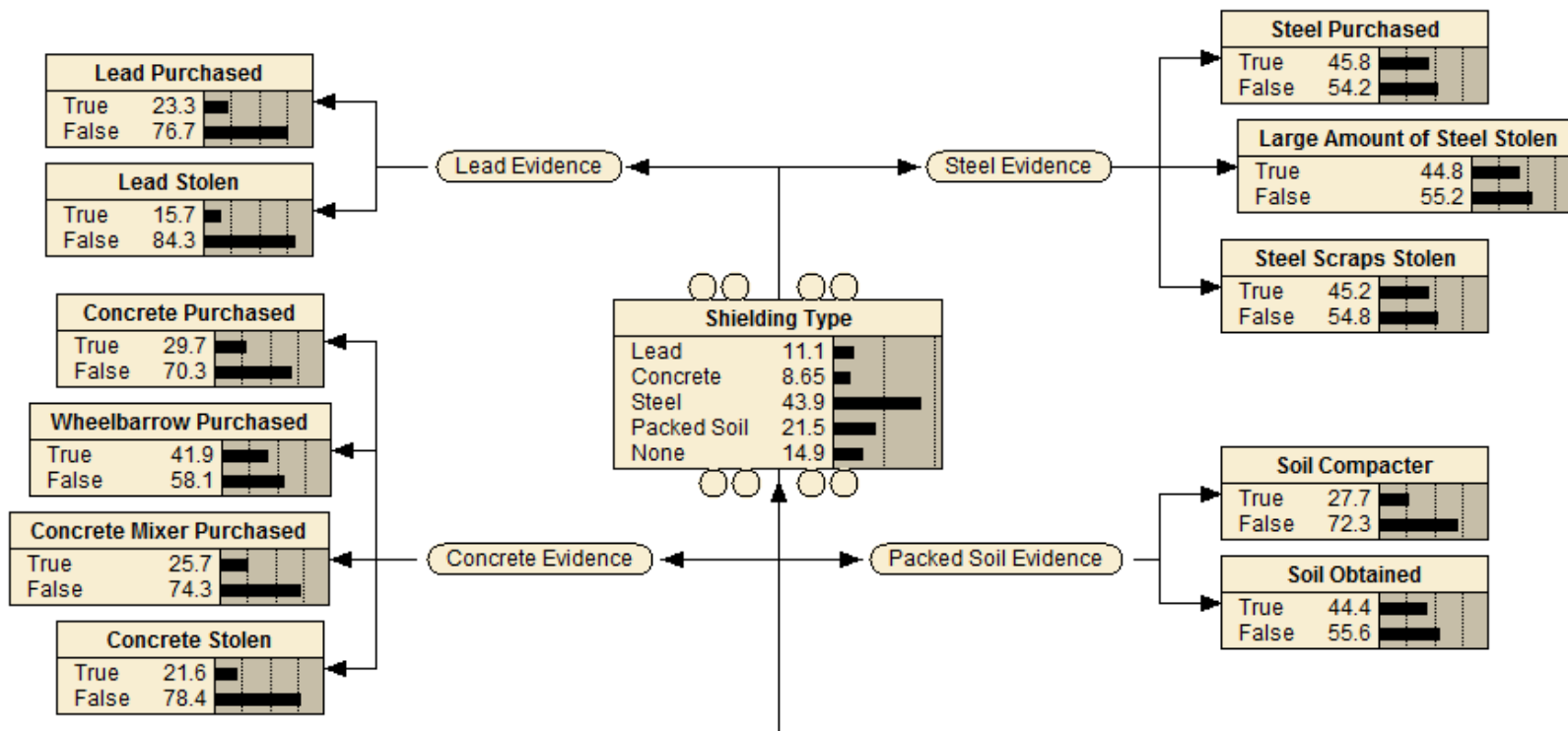


Fig. 28. Source shielding portion of source weaponization section.

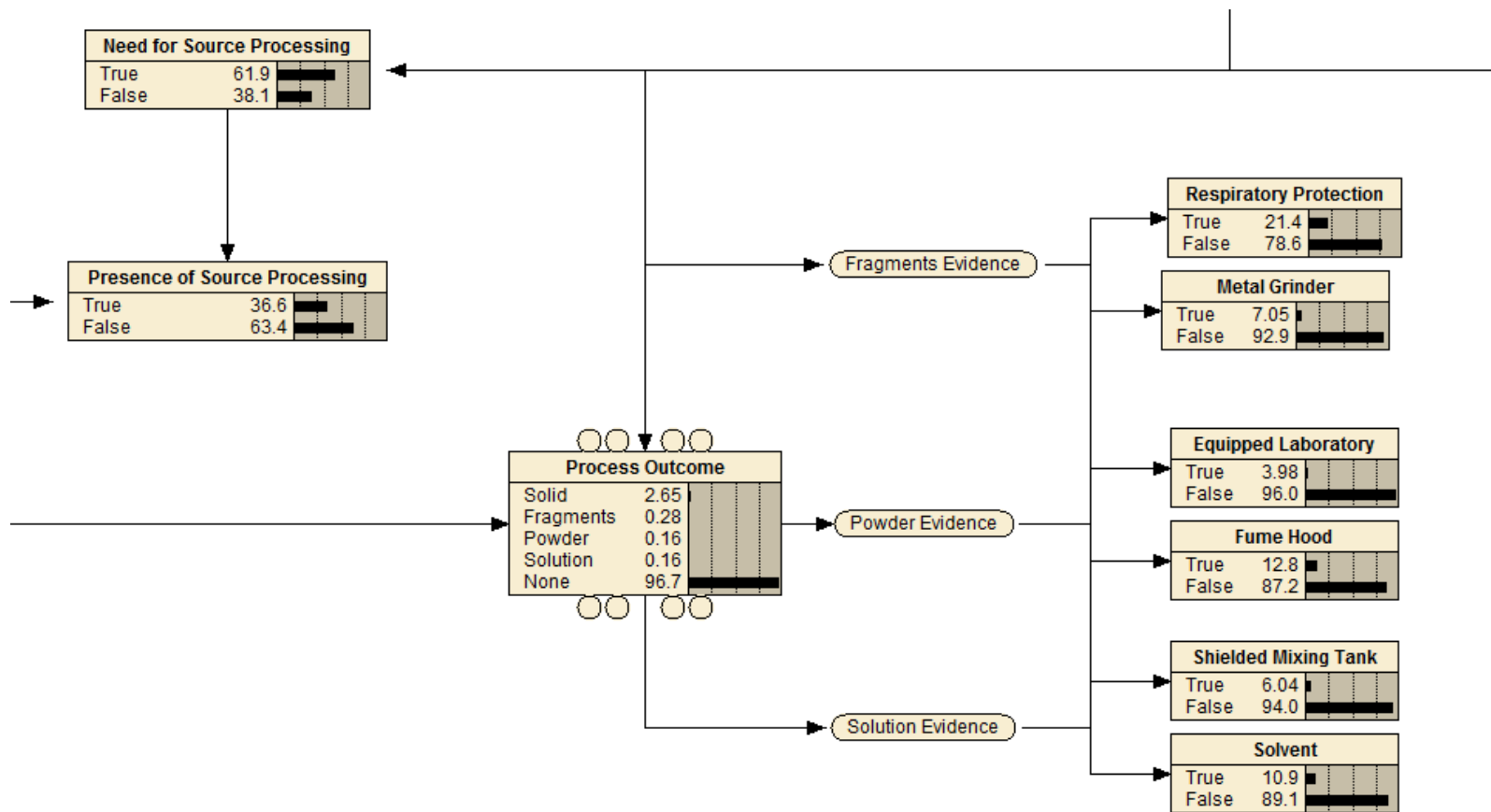


Fig. 29. Source processing portion of source weaponization section.

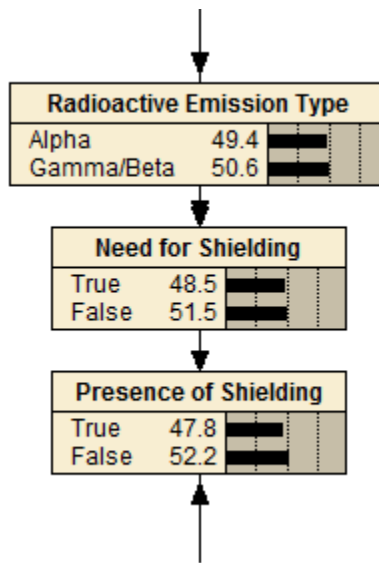


Fig. 30. Source weaponization input portion of source weaponization section.

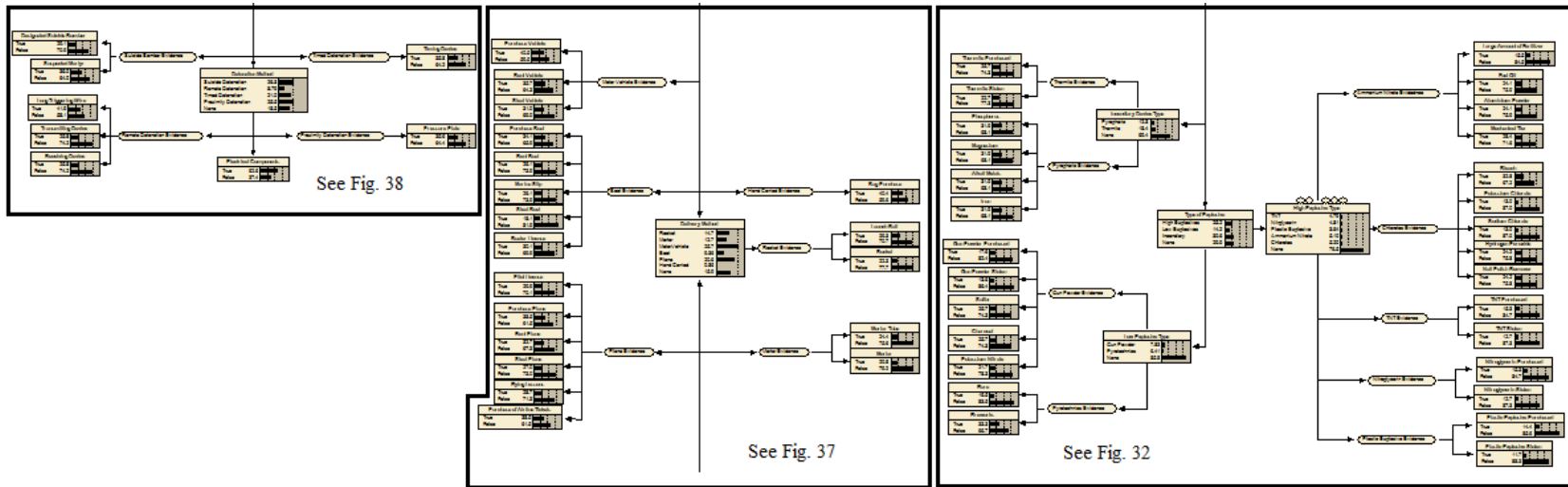


Fig. 31. Overview of assembly and detonation section.

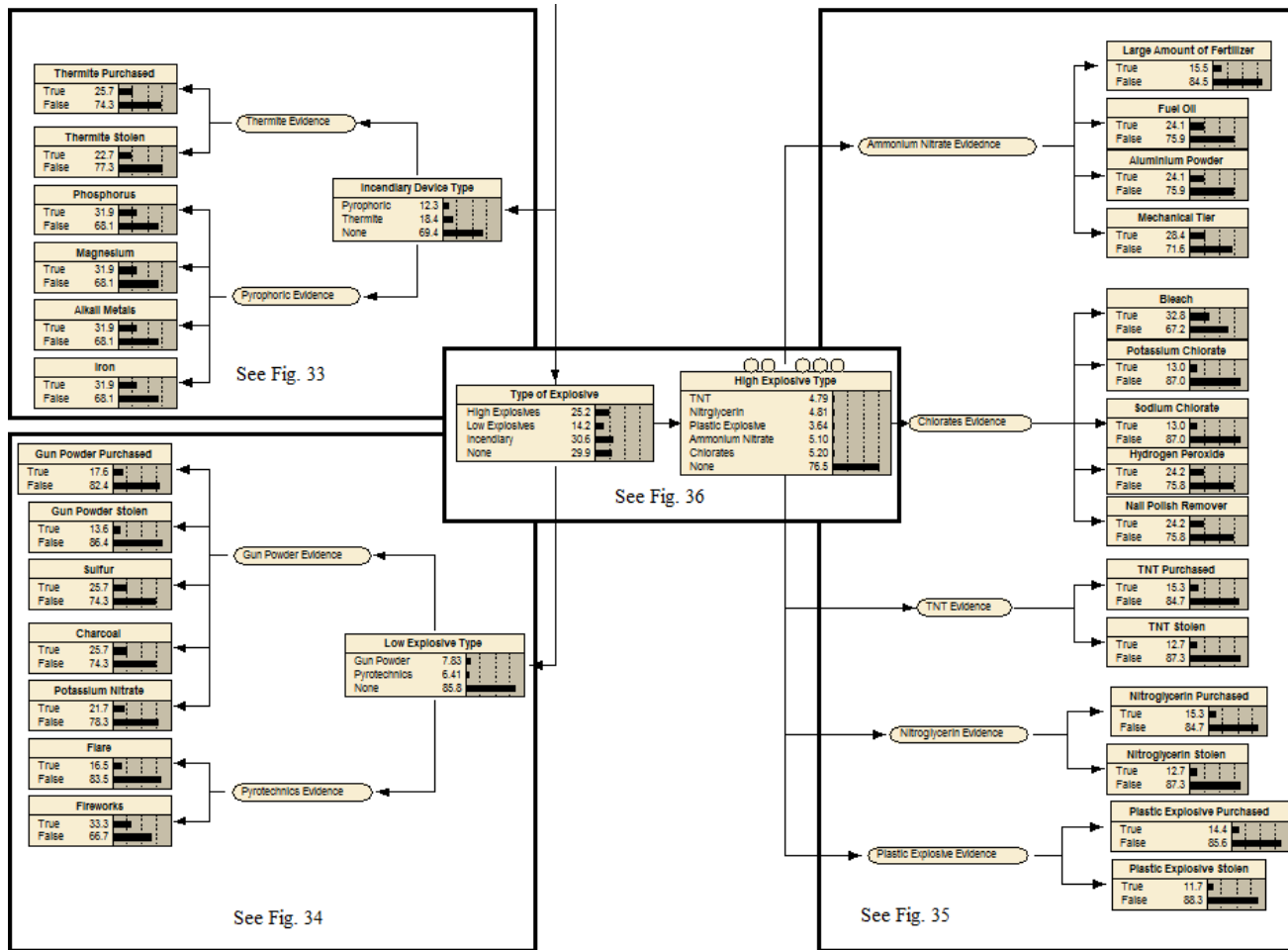


Fig. 32. Overview of explosives portion of assembly and detonation section



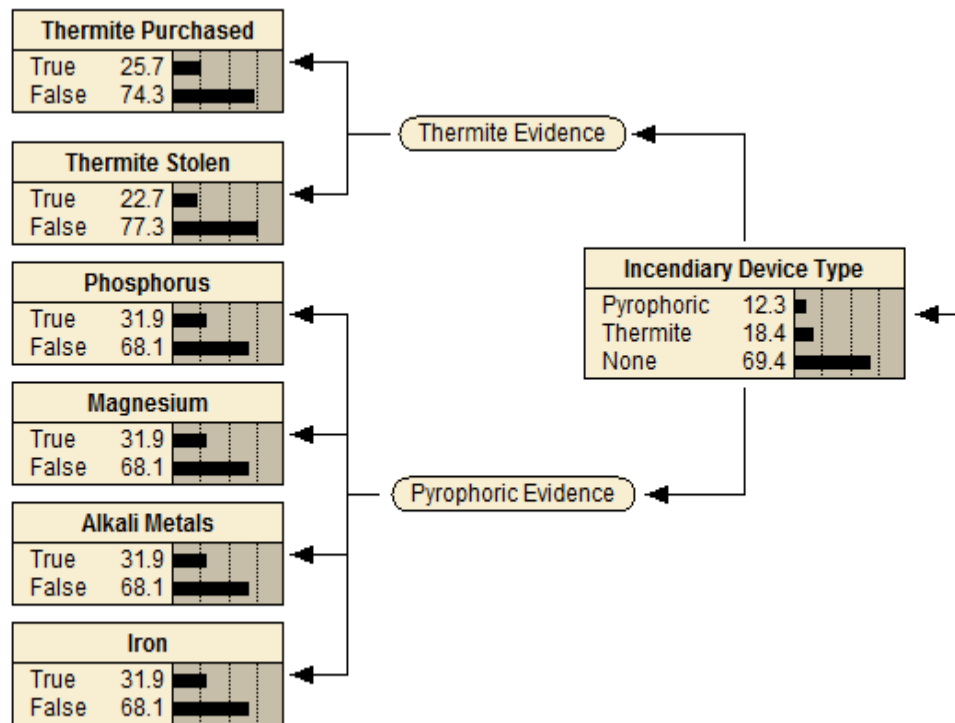


Fig. 33. Incendiary device portion of assembly and detonation section.

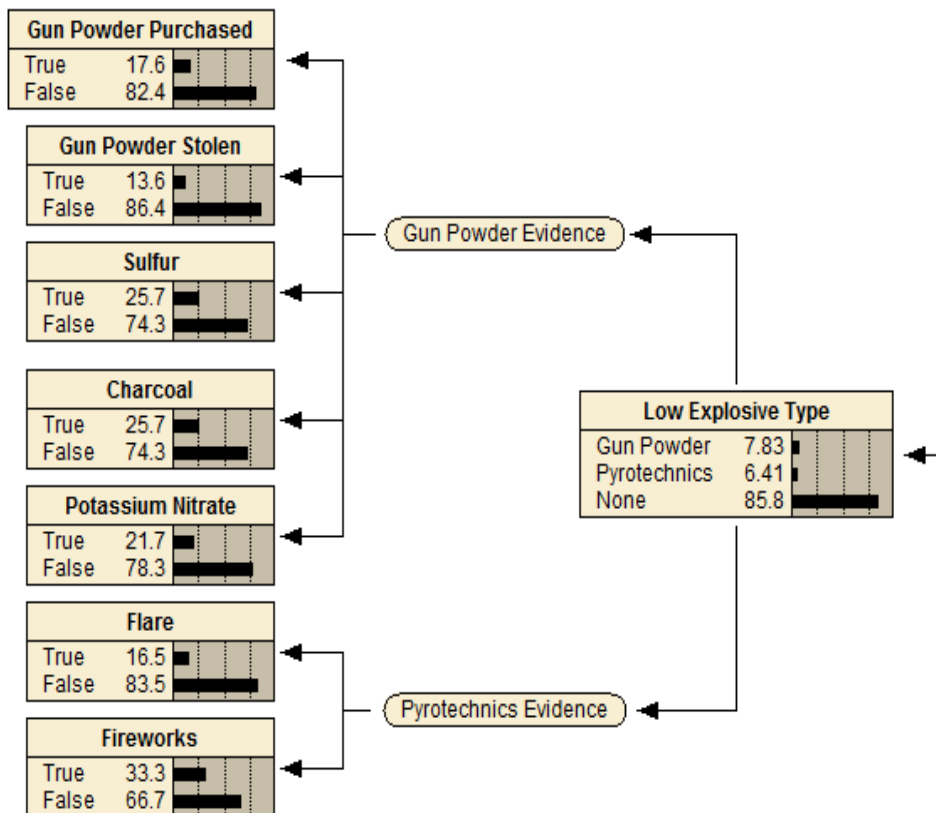


Fig. 34. Low explosive portion of assembly and detonation section.

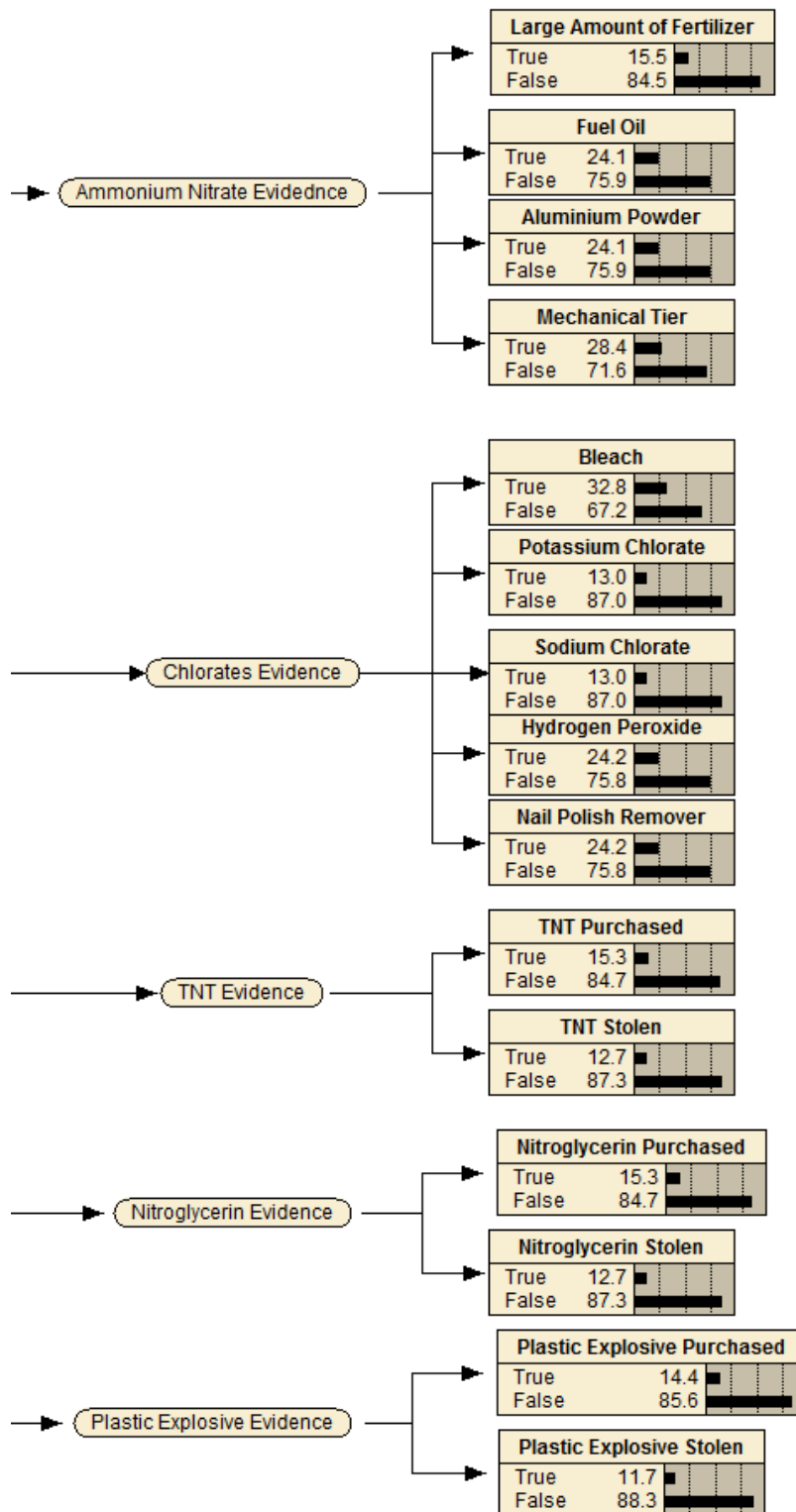


Fig. 35. High explosive portion of assembly and detonation section.

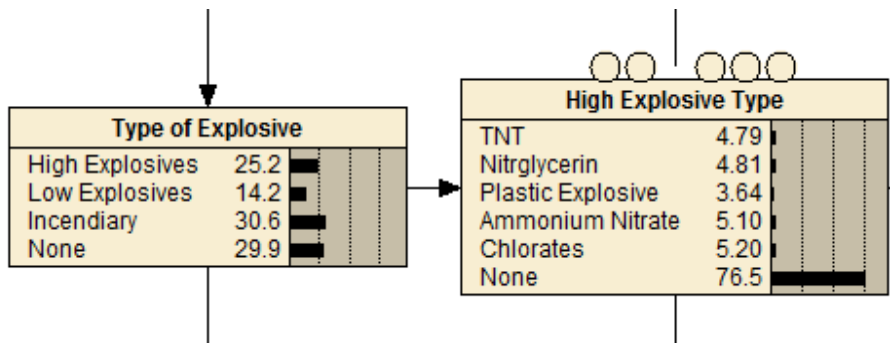


Fig. 36. Explosive summary portion of assembly and detonation section.

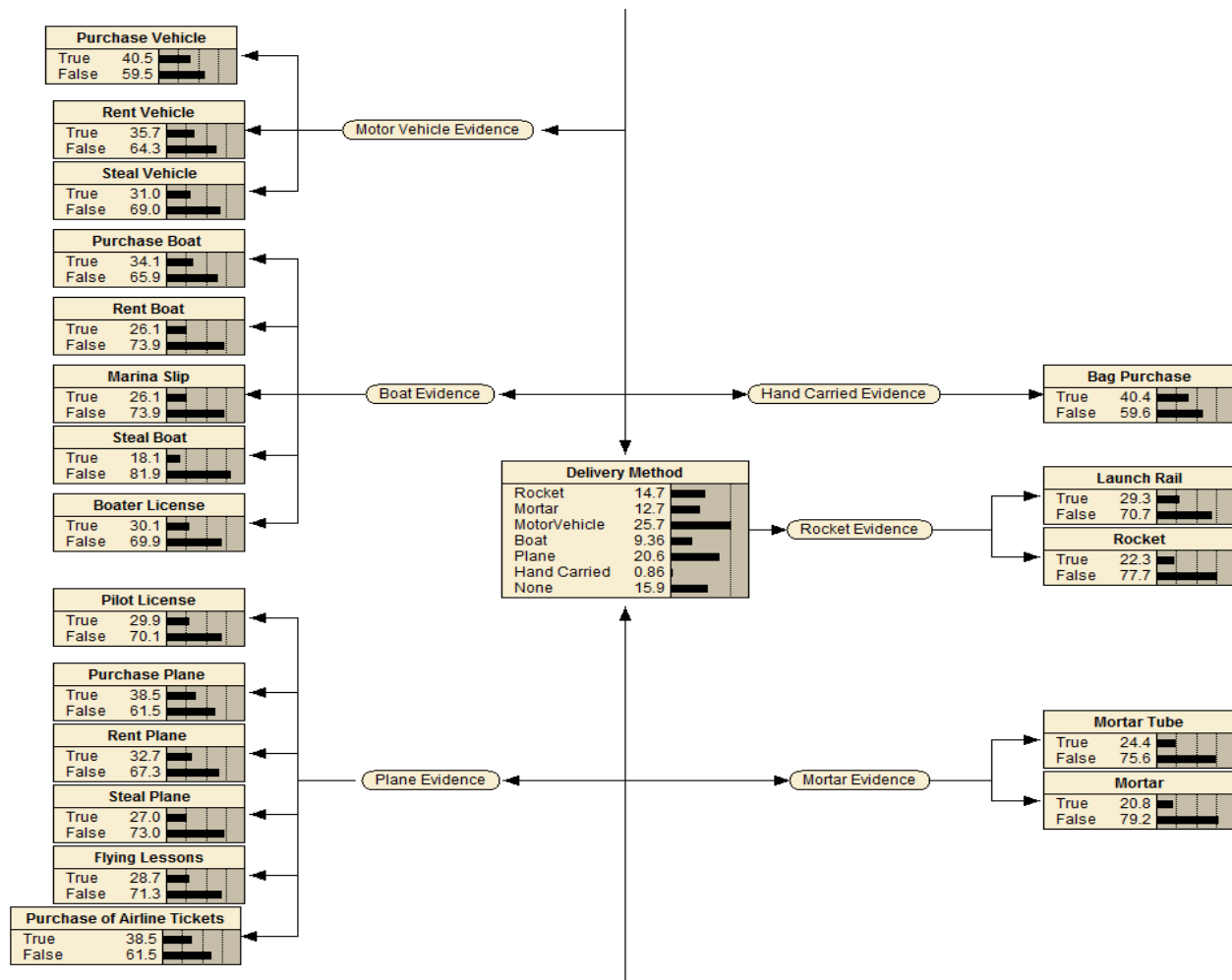


Fig. 37. Delivery method portion of assembly and detonation section.

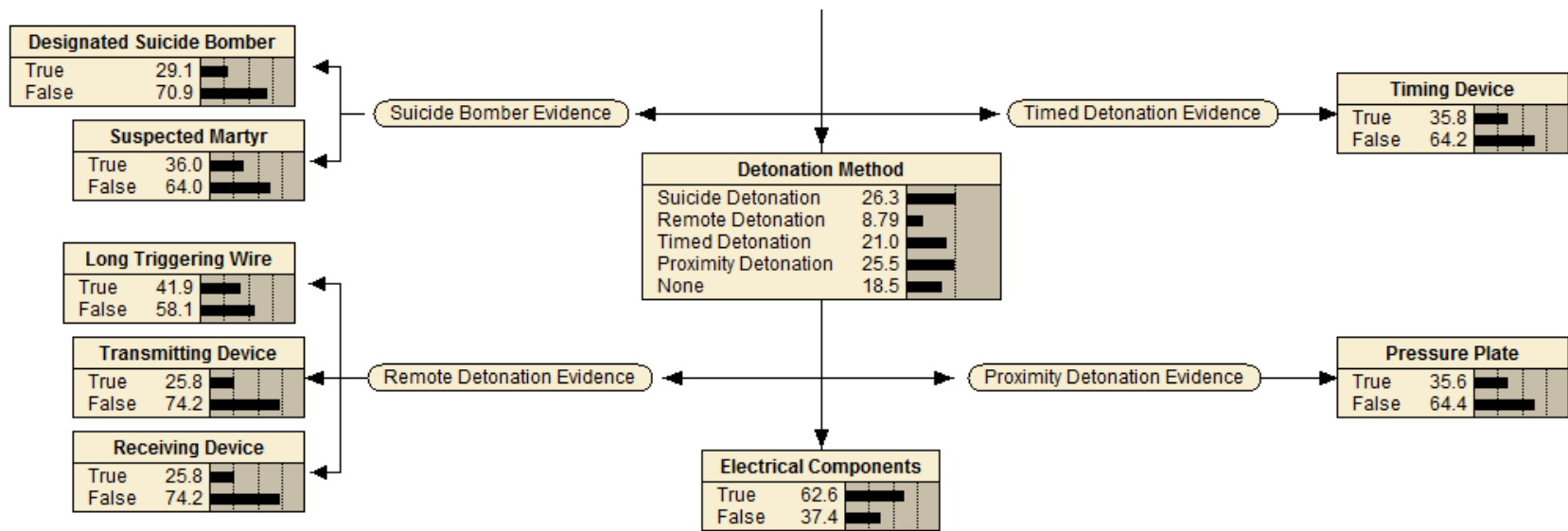


Fig. 38. Detonation portion of assembly and detonation section.

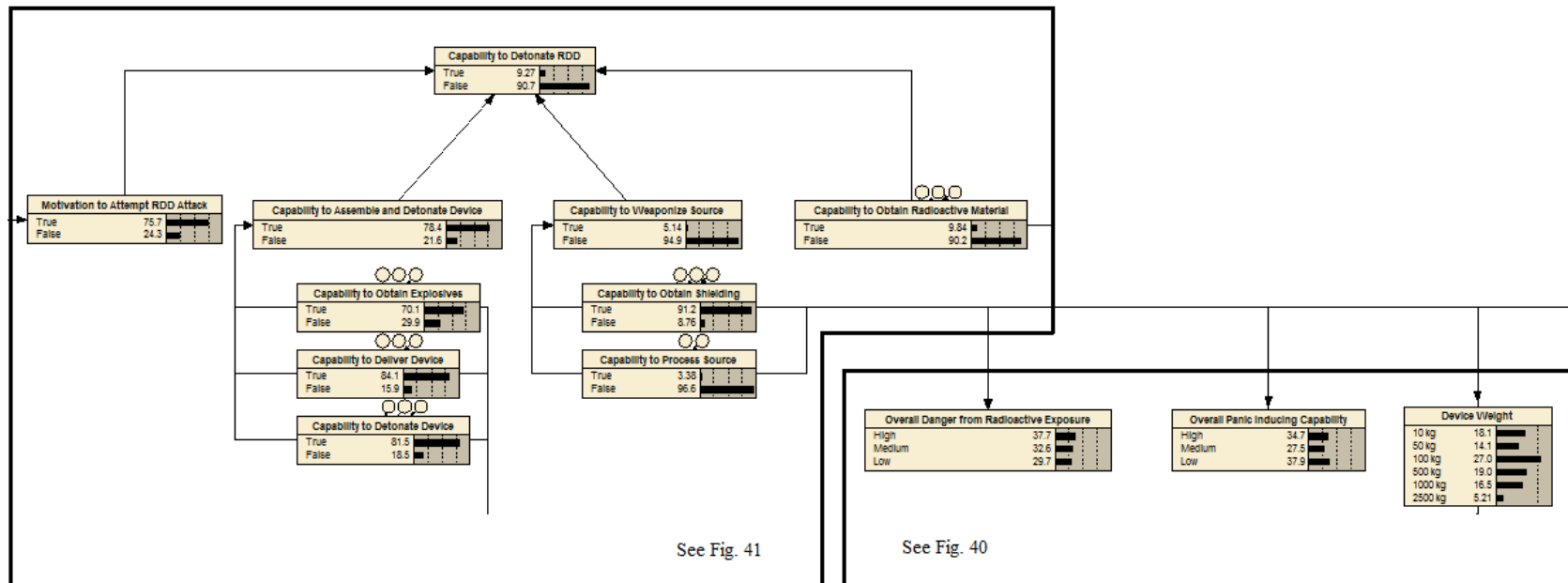


Fig. 39. Overview of final RDD design characteristics and overall chance of success section.

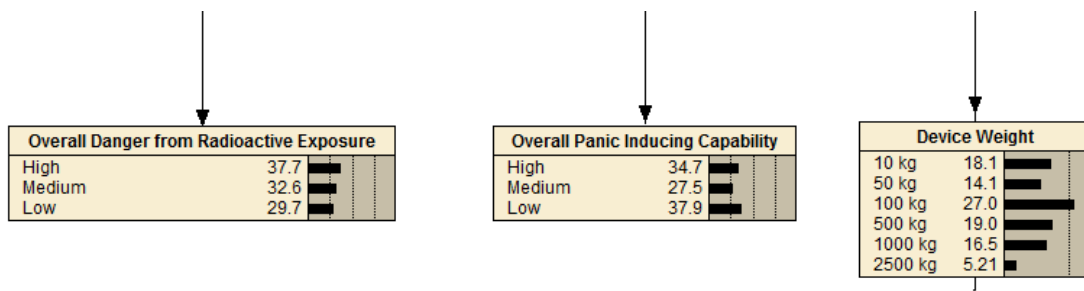


Fig. 40. Final RDD design characteristics portion of RDD design characteristics and overall chance of success section.



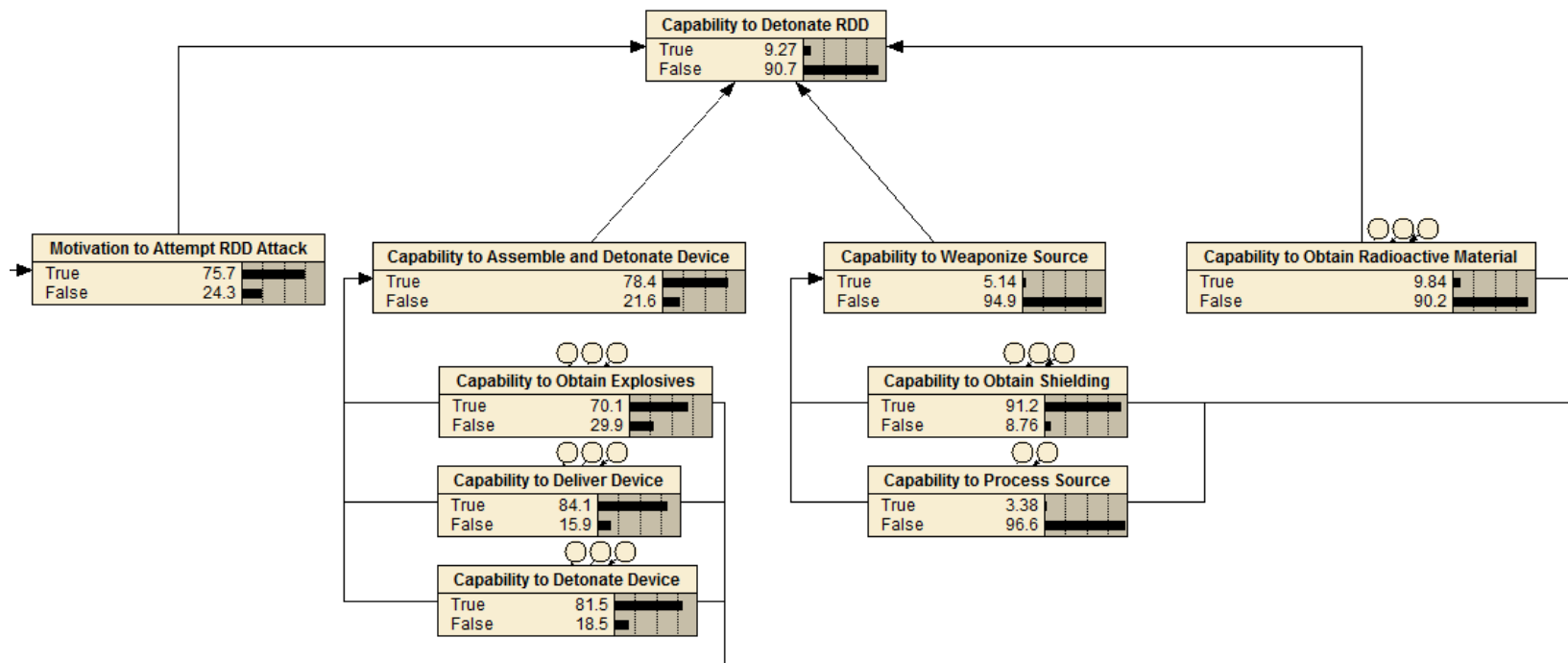


Fig. 41. Overall chance of success portion of RDD design characteristics and overall chance of success section.

## CHAPTER III

### NETWORK VERIFICATION

A series of case studies was first analyzed in order to verify that the Bayesian RDD acquisition network operated as expected. Additionally, these case studies serve to highlight many features of the network. Some of these features include the addition and removal of evidence for certain acquisition pathways and the effect of changing the resources available to an adversary. Also, two extreme case studies were analyzed to determine the limitations of this methodology. It is important to note that the probabilities listed as results of the following case studies are not absolute. Instead, they represent the relatively likelihood of success among various plots. Also, these probabilities do not account for any interdiction efforts by law enforcement agencies. However, suggested interdiction efforts are highlighted when they present themselves within the analysis.

#### **Plot 1: Homegrown, Al-Qaeda Influenced Plot**

The first case examined is a homegrown, Al-Qaeda influenced RDD plot. This plot can be considered analogous to the May 2010 attempted Times Square bombing by the Pakistani-American, Faisal Shahzad.<sup>25</sup> Acting alone or in a small cell with no military experience and minimal Al-Qaeda connections, the adversaries have novice tactical capabilities, and technical capabilities equivalent to those found in a garage lab. Since a small amount of funding is provided by overseas Pakistan-based terrorist sources, the adversaries devote \$10,000 to the plot. The primary motivations are a

Jihadi-based religious imperative and a desire to cause mass chaos and devastation. Fig. 42 depicts the adversary inputs and motivations. The two motivations suggest only a 25.6% desire for even source dispersal, a 13.7% desire for an easily deliverable device, a 92.1% desire to settle for a crude design, and only a 5.40% need of an IAEA category 1 source. These RDD characteristics are expected for a poorly funded plot primarily concerned with causing devastation in accordance with a religious imperative.

The predicted RDD plot characteristics are seen in Table II. Analysis suggests that the adversary will attempt to obtain  $^{137}\text{Cs}$  from a device utilized in an industrial facility. Radioactive sources in industrial facilities, such as well-logging devices or flow gauges, are typically less secured. An adversary with little tactical capability would find these devices easier to steal than larger sources in well secured facilities. Shielding would be included with a 47.8% probability as the activity of industrial sources is relatively low. An adversary with few technical capabilities would only have a 32.2% chance of processing the source. The low probability of source processing explains the use of an incendiary explosive to vaporize the source into an aerosol. The RDD would be delivered with a motor vehicle and detonated by a suicide bomber. The overall danger of the plot is predicted to be medium with a 35% probability due to low source activity and absence of source processing. Use of explosives in a motor vehicle would have a high chance of inducing panic with a 38.9% probability. Device weight is expected to be only 100 kg due to moderate source shielding.

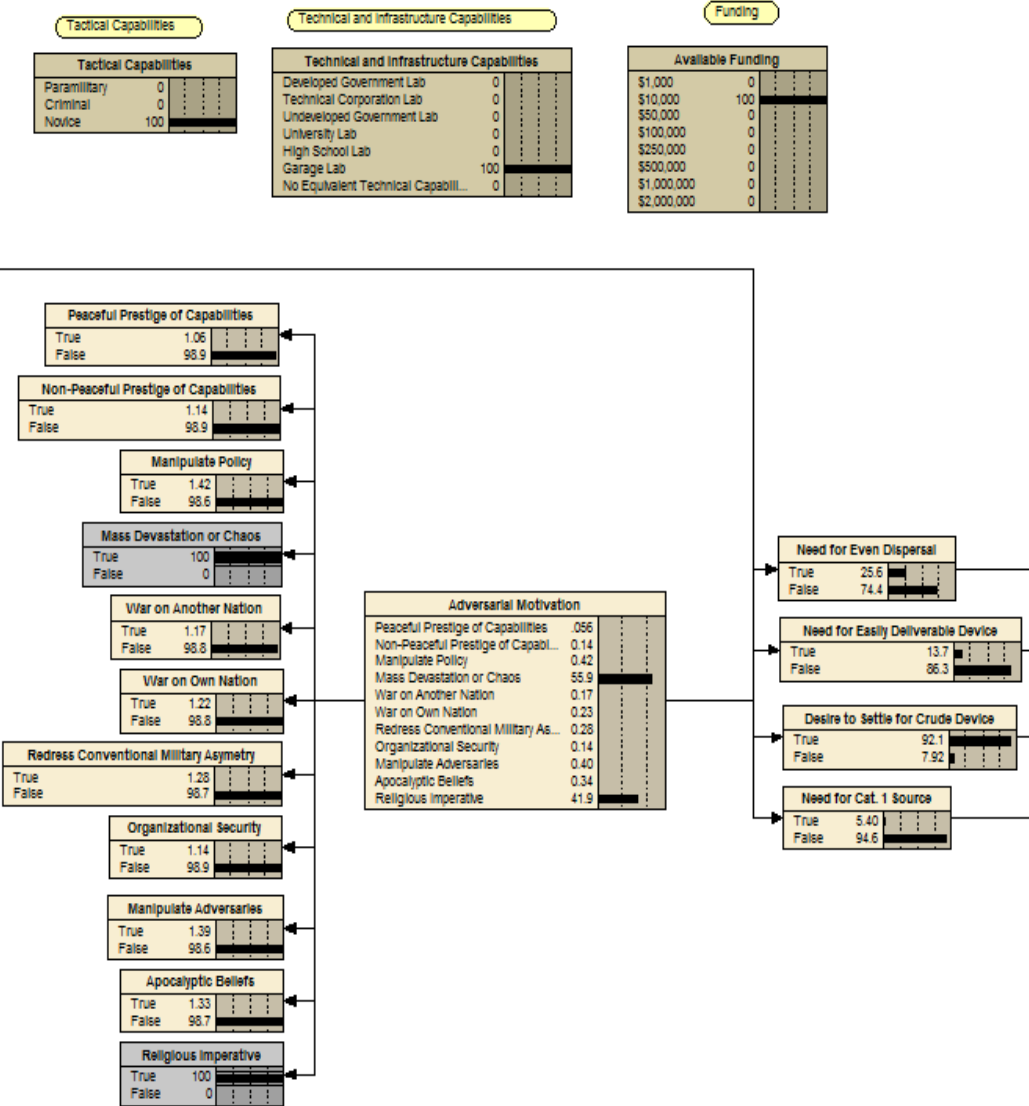


Fig. 42. Inputs for homegrown, Al-Qaeda influenced RDD plot.

TABLE II  
Homegrown Al-Qaeda influenced RDD plot characteristics.

Plot Characteristics	Network Output
Radioactive Material Origin:	Industrial Facility
Radioactive Material Type:	$^{137}\text{Cs}$
Presence of Shielding:	47.8%
Shielding Type:	Steel
Presence of Source Processing:	32.2%
Source Processing Type:	Solid
Explosive Type:	Incendiary (Thermite)
Delivery Method:	Motor Vehicle
Detonation Type:	Suicide
Danger from Radioactive Material:	Medium (35%)
Capability to Induce Panic:	High (38.9%)
Device Weight:	100 kg

The overall chance of success for such a plot is shown in Fig. 43. Analysis shows the relative probability of success for a homegrown, Al-Qaeda influenced RDD plot is only 12.4%. Such an adversary would have a high motivation for undertaking an RDD attack, but few resources hamper the ability to obtain radioactive material and nearly nullify any chance of successful source weaponization.

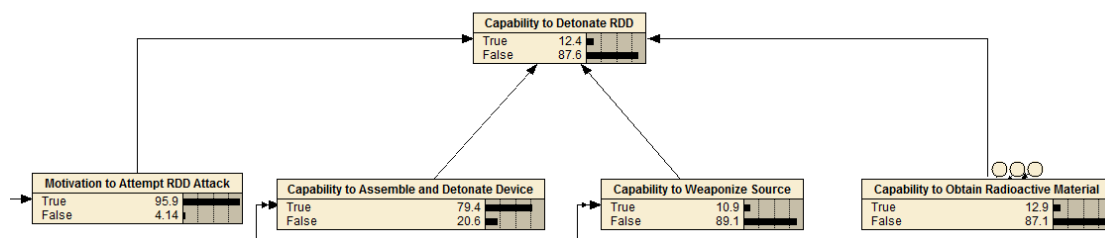


Fig. 43. Overall chance of success for a homegrown, Al-Qaeda influenced RDD plot.

### *Effect of Evidence for Delivery Methods*

This plot was examined by including evidence that the adversary had previously purchased a vehicle to be used in the attack. Figure 44 depicts the effects of this evidence on the overall chance of success for the homegrown, Al-Qaeda influenced plot. The evidence of a vehicle purchase increases the probability of successful assembly and detonation of the RDD from 79.4% to 80.9%. Additionally, the inclusion of this evidence only increases the overall probability of success from 12.4% to 12.5%. These results reflect the fact that obtaining a vehicle to deliver an RDD is not an inherently difficult task for an adversary. However, it is interesting to note that the inclusion of this evidence increases likely device weight to 500 kg. Evidence of a vehicle purchase further suggests that the device cannot be hand-carried or delivered remotely.

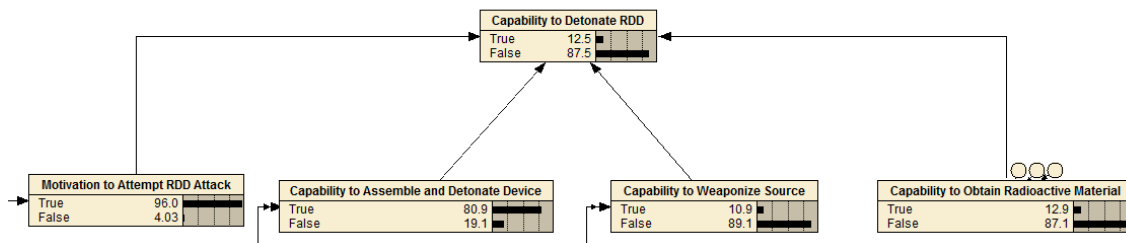


Fig. 44. Overall chance of success for a homegrown, Al-Qaeda influenced RDD plot with evidence of a vehicle purchase.

*Effect of Evidence for Source Processing*

Next, this plot was further examined by including evidence of a fume hood and metal grinder. These devices indicate the presence of source processing. Table III depicts the updated homegrown, Al-Qaeda influenced RDD plot characteristics. The probability of source processing has increased from 32.3% to 55.2%. Presence of a fume hood and a metal grinder, along with the adversary's poor technical capabilities, suggest that the source is only processed into fragments. Also, the likely explosive has changed from incendiary thermite to high explosive ammonium nitrate. The use of a high explosive is better suited in dispersing a processed radioactive source. Finally, evidence of source processing has changed the RDD's radioactive danger from medium to a 48.7% chance of high. Figure 45 shows the overall success probability for the homegrown, Al-Qaeda influenced plot with source processing evidence. Probability of source weaponization jumps from 10.9% to 41.6% with the evidence inclusion. The overall probability of success increased slightly from 12.4% to 12.7%. Evidence of source processing increases the radioactive danger of the RDD plot, but it fails to reduce the difficulty of actually obtaining radioactive materials.

TABLE III  
Homegrown, Al-Qaeda influenced RDD plot characteristics with evidence of source processing.

Plot Characteristics	Network Output
Radioactive Material Origin:	Industrial Facility
Radioactive Material Type:	$^{137}\text{Cs}$
Presence of Shielding:	47.8%
Shielding Type:	Steel
Presence of Source Processing:	55.2%
Source Processing Type:	Fragments
Explosive Type:	High (Ammonium Nitrate)
Delivery Method:	Motor Vehicle
Detonation Type:	Suicide
Danger from Radioactive Material:	High (48.7%)
Capability to Induce Panic:	High (42.3%)
Device Weight:	100 kg

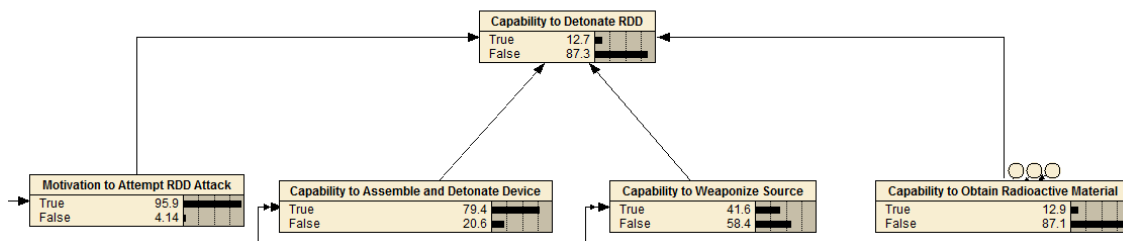


Fig. 45. Overall chance of success for a homegrown, Al-Qaeda influenced RDD plot with evidence of source processing.

### *Effect of Evidence for Radioactive Material Acquisition*

Introducing evidence of radioactive material acquisition significantly influences the chance of success for the plot. Radioactive material acquisition nodes were adjusted



to account for the penetration of a blood irradiator facility and the removal of a blood irradiator source. These two pieces of evidence indicate the adversary may have obtained a radioactive source. The results of this evidence can be seen in Fig. 46. As expected, the probability of radioactive material acquisition increases from 12.9% to 22.3%. The overall probability of success increases from 12.4% to 20.9%. These results demonstrate two important characteristics of the created RDD Bayesian network. First, final RDD success probability is heavily weighted towards the acquisition of radioactive material acquisition. Possessing other capabilities to employ an RDD, such as delivery and weaponization, are useless without radioactive material. Secondly, the integration of real-time intelligence, such as a medical facility penetration, into the RDD network's evidence nodes can significantly change the likelihood of a successful plot.

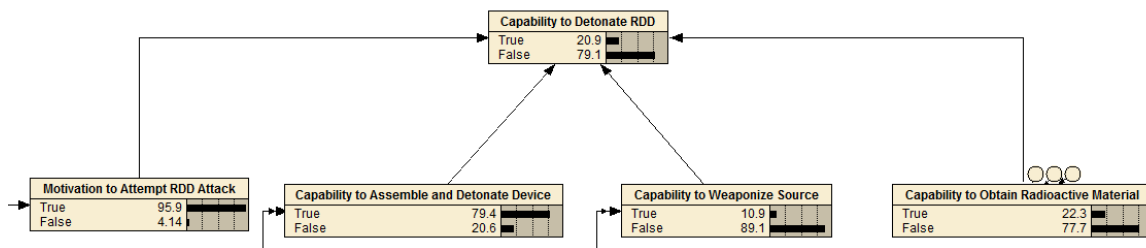


Fig. 46. Overall chance of success for a homegrown, Al-Qaeda influenced RDD plot with evidence of radioactive material acquisition.

## **Plot 2: Apocalyptic Group Plot**

The second case examined is an apocalyptic, religious group RDD plot. The adversary is similar to the mostly defunct Japanese terrorist group Aum Shinrikyo. Responsible for the 1995 Sarin gas attack on the Tokyo subway, Aum Shinrikyo was extremely well-funded through legitimate businesses and technically competent enough to produce homemade hallucinogens and nerve gas.<sup>26</sup> The apocalyptic group has novice tactical capabilities. However, they have technical capabilities equivalent to those found in the lab of a technical corporation, and devote \$2,000,000 to the RDD plot. The adversary's primary motivations are an apocalyptic belief and a religious imperative. Fig. 47 depicts adversarial inputs and motivations. The two motivations suggest a low 23.6% need for even source dispersal, an 11.2% need for an easily deliverable source, an 89.1% desire to settle for a crude device, and only a 4.52% need for an IAEA category 1 source. These device characteristics are expected for an apocalyptically motivated adversary with little need for a well-designed, deliverable RDD.

The apocalyptic group RDD plot characteristics are seen in Table IV. The analysis suggests that the most likely pathway to obtain radiological material is commercial acquisition. An apocalyptic group, with \$2,000,000 in funding, would likely be able to acquire a source license and legitimately purchase a radioactive source. Technical capabilities equivalent to those found in the lab of a technical corporation indicate the adversary may be sophisticated enough to pass regulating inspections prior to the issuance of a source license. Additionally, an adversary with novice tactical skills would likely be unsuccessful in an attempt to steal a source. The radioactive material

obtained through commercial acquisition is  $^{241}\text{Am}$ . The use of such an alpha-emitter, coupled with a 91.4% chance of source processing into a powder, indicates a devastating RDD with a high danger level and a high chance of inducing panic. The moderately probable presence of shielding, at 50.4%, is a result of the low penetration ability of alpha particles.  $^{241}\text{Am}$  also emit a low energy gamma ray at 60 keV, but the relatively low energy of the gamma ray means it can also easily be shielded.

TABLE IV  
Apocalyptic group RDD plot characteristics.

<b>Plot Characteristics</b>	<b>Network Output</b>
Radioactive Material Origin:	Commercial Acquisition
Radioactive Material Type:	$^{241}\text{Am}$
Presence of Shielding:	50.4%
Shielding Type:	Lead
Presence of Source Processing:	91.4%
Source Processing Type:	Powder
Explosive Type:	High (Plastic Explosive)
Delivery Method:	Motor Vehicle
Detonation Type:	Suicide
Danger from Radioactive Material:	High (72.6%)
Capability to Induce Panic:	High (67.4%)
Device Weight:	500 kg

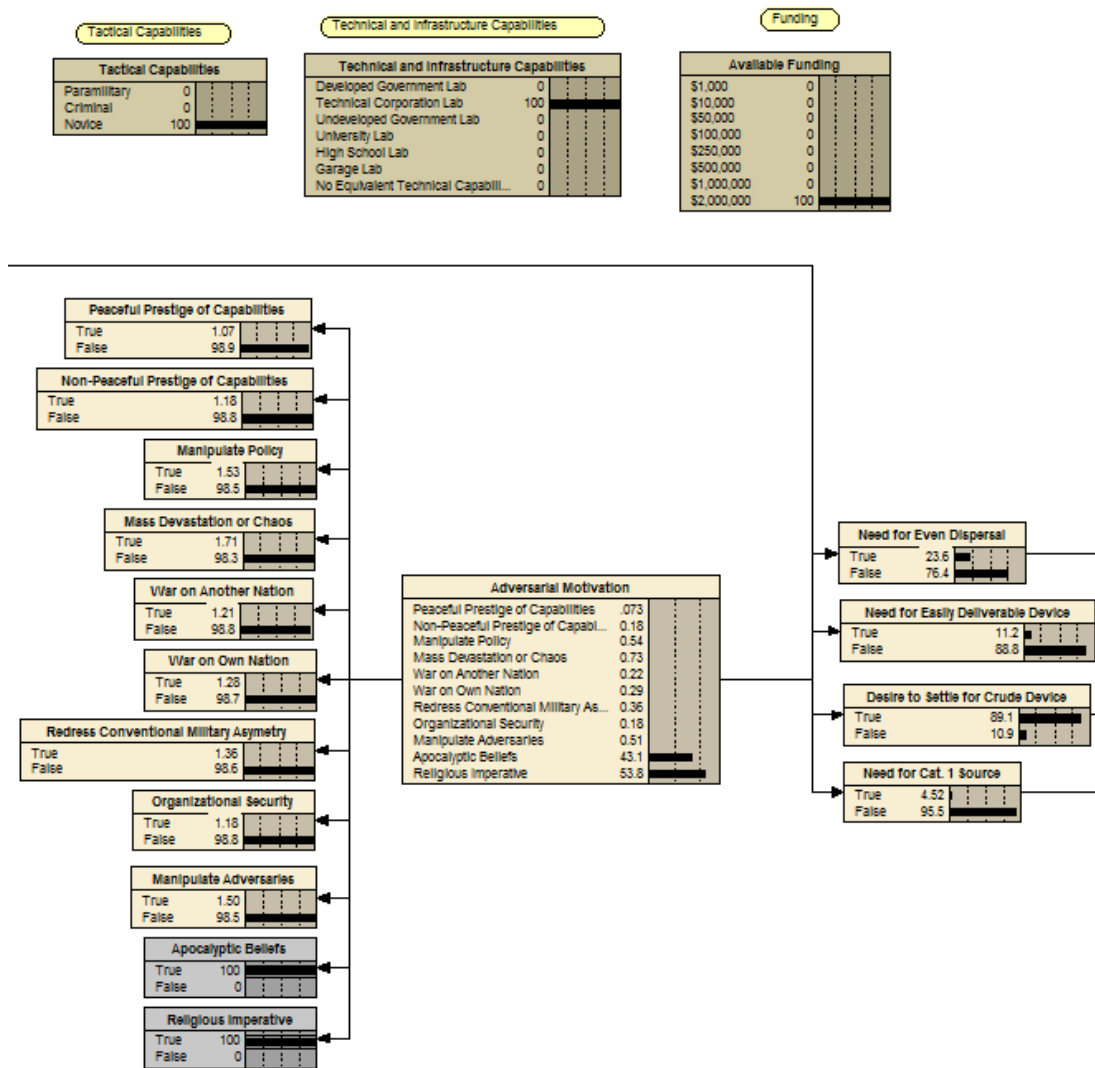


Fig. 47. Inputs for apocalyptic group RDD plot.

The overall chance of success for an apocalyptic group RDD plot is shown in Fig. 48. Analysis shows that this plot has a relative success probability of 69.1%. Examination of other nodes in the figure shows that a well-funded and technically competent apocalyptic group has a high probability of weaponizing a source and

assembling and detonating an RDD. The 70.9% probability of radioactive source acquisition, significantly greater than a homegrown, Al-Qaeda influenced plot, is mainly a reflection of the adversary's significant funding.

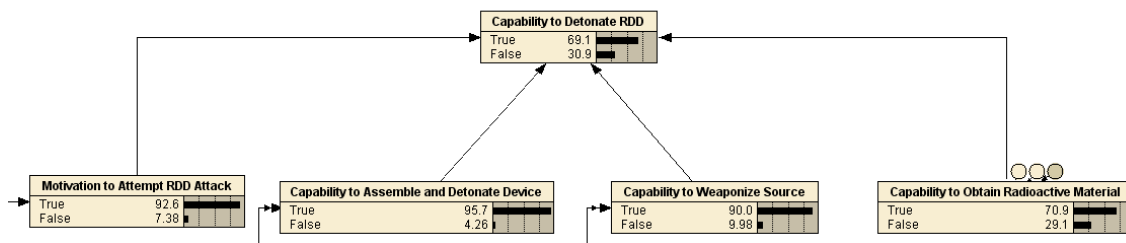


Fig. 48. Overall chance of success for an apocalyptic group RDD plot.

### *Effect of Evidence for Radioactive Material Acquisition*

The introduction of evidence for radioactive material acquisition significantly affects the adversary's likelihood of success. A node adjustment within the network added evidence that the apocalyptic group maintains a legitimate front company. Many applications for radioactive source licenses require onsite regulator inspections. Consequently, the presence of a known front company increases the likelihood that a source license for radioactive material could be obtained. Fig. 49 shows that the probability of radioactive material acquisition increases from 70.9% to 84.3%. In addition, the relative success probability increases from 69.1% to 81.9%. An increase in the probability of radioactive material acquisition results in a nearly linear increase in relative success probability.

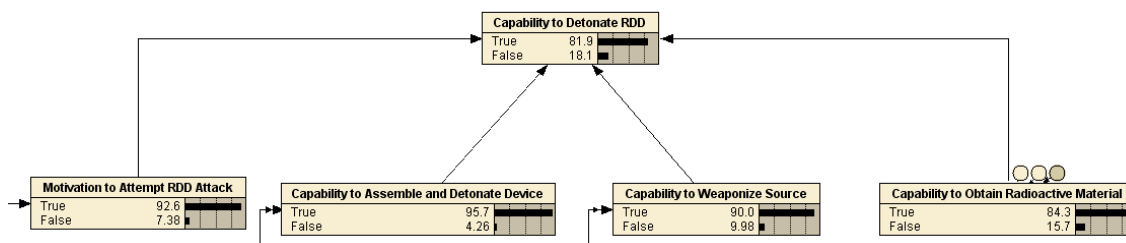


Fig. 49. Overall chance of success for an apocalyptic group RDD plot with evidence of radioactive material acquisition.

### *Effect of Evidence against Source Processing*

The apocalyptic group network was next analyzed by adding evidence against source processing. The lack of source processing could be attributed to a hurried adversary timeline or a lack of certain laboratory facilities. A node adjustment changed the probability of source processing to 0%. Consequently, the lack of source processing left the  $^{241}\text{Am}$  in a solid form. The introduction of this evidence had widespread effects seen across many pathways in the network. Table V demonstrates the effects of adding evidence against source processing. The first notable effect was the acquisition pathway branched to include thermite explosives instead of plastic explosives. In the absence of source processing, the adversary would likely employ an incendiary device to aerosolize the alpha emitting source to permit inhalation and ingestion. The delivery and detonation pathway does not change with the addition of evidence against source processing. However, the danger from radioactive material drops from high with a 72.6% chance to medium with a 46.3% chance. This example shows the dependence of

device danger on source processing. The lack of source processing, especially for a weakly-penetrating alpha emitter, significantly reduces the RDD's radiological effects.

TABLE V  
Apocalyptic group RDD plot characteristics with evidence against source processing.

<b>Plot Characteristics</b>	<b>Network Output</b>
Radioactive Material Origin:	Commercial Acquisition
Radioactive Material Type:	<sup>241</sup> Am
Presence of Shielding:	51.3%
Shielding Type:	Lead
Presence of Source Processing:	0%
Source Processing Type:	None
Explosive Type:	Incendiary (Thermite)
Delivery Method:	Motor Vehicle
Detonation Type:	Suicide
Danger from Radioactive Material:	Medium (46.3%)
Capability to Induce Panic:	High (54%)
Device Weight:	500 kg

The overall chance of success for an apocalyptic group RDD plot with evidence against source processing is seen in Fig. 50. As expected, the chance of source weaponization drops from 90.0% to only 13.9%. It is interesting to note that even though the chance of source processing node was set to 0%, the chance of source weaponization stays at 13.9%. This can be attributed to the fact that source weaponization includes both source processing and shielding. Consequently, the remaining 13.9% reflects the probability of the adversary successfully obtaining

shielding. The overall chance of success of the RDD plot drops from 69.1% to 67.9% after the addition of evidence against source processing. A 1.2% change in overall success probability represents a surprisingly small difference after the addition of such significant evidence. However, the overall chance of a successful RDD plot is heavily weighted towards radioactive material acquisition. An adversary with the ability to commercially acquire  $^{241}\text{Am}$  has a probable chance of success in an RDD plot, regardless of source processing capabilities. The effects of evidence against source processing are primarily seen in the diminished device danger from radioactive material.

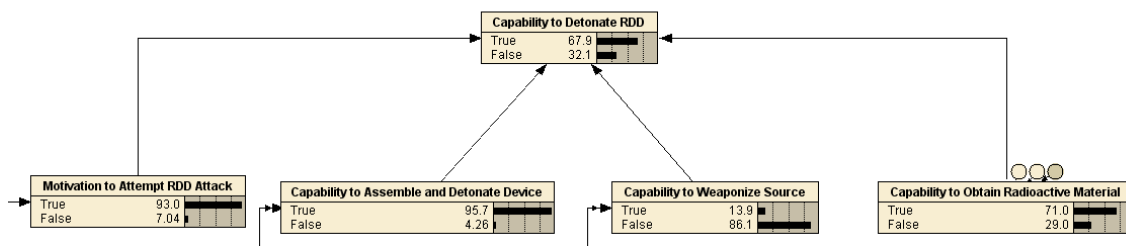


Fig. 50. Overall chance of success for an apocalyptic group RDD plot with evidence against source processing.

### *Effect of Evidence for Radioactive Material Acquisition and Subsequent Plot Flags*

The addition of evidence to the RDD acquisition network clearly demonstrates how specific adversarial actions affect the eventual design and overall success of an RDD plot. However, this Bayesian implementation can also be used to predict likely adversarial actions prior to the node where evidence is added into the network. Analysis of nodes prior to evidence introduction allows a law enforcement agency to narrow an



investigation to focus on likely actions within an adversary's RDD plot. This allows for a greater leverage of resources against a probable set of adversarial actions.

Evidence was added to the apocalyptic group RDD plot to demonstrate the presence of plot flags and subsequent focusing of law enforcement resources. For example, consider that the apocalyptic group has expressed a desire to interdict a radioactive source during a land or ocean shipment. Fig. 51 shows this evidence added into the node titled "Origin of Radioactive Material." This evidence changes the likely radioactive material obtained from  $^{241}\text{Am}$  to  $^{60}\text{Co}$  since a given shipment of radioactive materials is most likely to contain cobalt. The introduction of this evidence certainly increases the adversary's chance of obtaining radioactive material and overall chance of success.

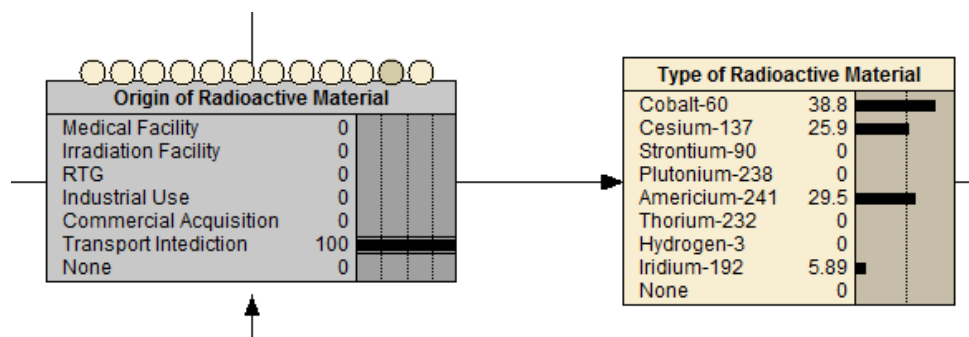


Fig. 51. Transport interdiction evidence added to an apocalyptic group RDD plot.

On the other hand, Fig. 52 demonstrates the effect this evidence has on other evidence nodes describing transport interdiction. The network shows that the adversary

is most likely to interdict a road shipment with a 55% probability, while the probability of an ocean shipment interdiction has a 45% probability. Furthermore, the probabilities of potential road shipment evidence nodes have also changed with the addition of the transport interdiction evidence. The network suggests that the adversary will have knowledge of ground source shipments with a probability of 51.9%, will be employed by a ground transport carrier as a non-driver with a 52.9% probability, will be employed by a ground transport carrier as a driver with a 53.8% probability, and a source shipment will be missing with a 54.8% probability. Based on these automatic node adjustments within the network, law enforcement agencies now have a much narrower investigative focus. Employees of trucking companies should be cross-checked against known members of the apocalyptic group. Those with intimate knowledge of truck shipment schedules, such as employees of radioactive source suppliers and consumers, should be investigated. Finally, documented cases of missing source shipments should be analyzed for possible connection to the apocalyptic group RDD plot.

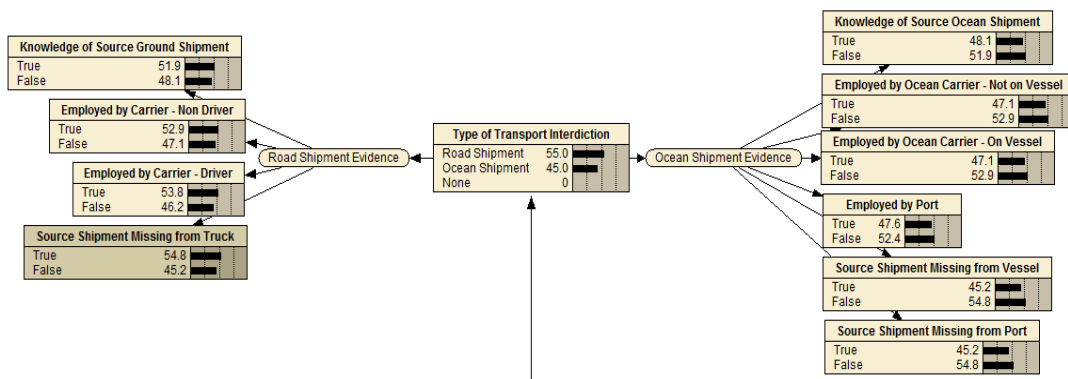


Fig. 52. Likely apocalyptic group actions based on evidence of radioactive material acquisition through transport interdiction.

Plot flags derived from the introduction of evidence into the RDD network can be used both passively and actively. Passive utilization involves comparing probable plot flags to criminal activities that may have already occurred. This would provide a good measure of where an adversary is located on the pathway to a successful RDD detonation. Consider introduction of evidence into the network that suggests the adversary will attempt to obtain a radioactive source from a blood irradiator. If investigators find that a blood irradiation machine was scavenged in the adversary's known area of operation, then it can be assumed that the adversary has successfully completed pathways describing radioactive material acquisition. Active utilization involves planning law enforcement actions against probable plot flags predicted by the network. Consider introduction of evidence into the network that suggests the adversary plans to travel to Russia to acquire a remotely located RTG. By cross-checking known members of the adversarial group with flight manifests to Russian cities close to the Baltic, those adversaries can be arrested in the airport and the plot can be halted.

### **Plot 3: Drug Cartel Plot**

The third case examined was a drug cartel RDD plot. The adversary is analogous to the numerous Mexican drug cartels along the US-Mexican border who vie for control of areas from government and rival cartels in order to smuggle drugs. Mexican cartels

have carried out terrorist attacks south of the border, to include shootings, assassinations, and car bombings.<sup>27</sup> The cartel has paramilitary tactical capabilities due to wide access to military arsenals and thorough training from police and military defectors. With technical capabilities equivalent to those found in a rudimentary garage lab, they are able to devote \$250,000 to an RDD plot aimed against American soil. The adversary's primary motivations are war on its own nation and war on another nation. Network inputs and adversarial motivations can be seen in Fig. 53. The two motivations suggest a 62.0% need for even dispersal, a 90.3% need for a deliverable device, only a 19.7% desire to settle for a crude design, and an 87.8% need for an IAEA category 1 source. The drug cartel, waging a nearly conventional war against nearby governments, would probably require an RDD that can be delivered easily and from a remote location. The cartel's motivations imply they will need a large amount of radioactive material to effectively wage a war, congruent with the prediction of the cartel's need for an IAEA category 1 source.

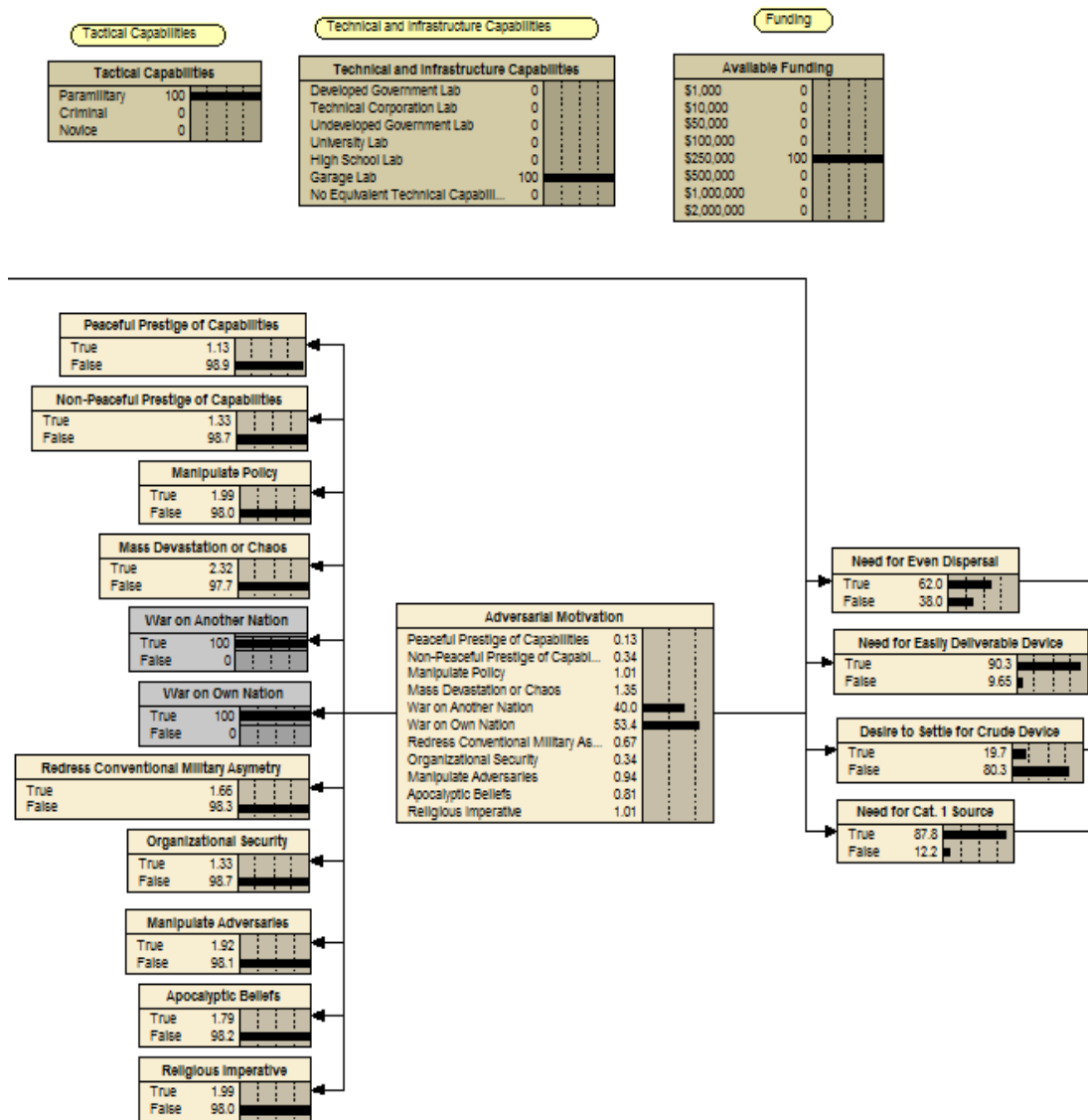


Fig. 53. Inputs for drug cartel RDD plot.

The drug cartel RDD plot characteristics are seen in Table VI. The network suggests that the adversary will obtain radioactive material through transport interdiction. A paramilitary tactical capability implies the cartel would likely be able to hijack a source during transportation. Additionally, few technical capabilities and only

moderate funding would prevent commercial acquisition. The most probable radioactive material is  $^{60}\text{Co}$ . Cobalt shipments are typically IAEA category 1 material. Shielding will be present with a 65% probability, and the chance of source processing is 63.5%. The large amount of  $^{60}\text{Co}$  certainly dictates the necessity of shielding. The cartel's need for even dispersal and an easily deliverable device requires some amount of source processing. However, minimal technical capabilities explain the prediction that the cartel may not be able to process the cobalt pencils past a large, solid form. The network suggests the use of the high explosive nitroglycerin. Nitroglycerin would be readily available in a budget of \$250,000. The predicted delivery and detonation method is by a proximity detonated rocket. A rocket would allow a stand-off capability, and would ensure even source dispersal if the rocket is programmed to detonate above its target. The network suggests the RDD plot will have a high danger from radioactive material with a 58.5% probability, and a medium chance of inducing panic at 36.5%. Due to a rocket delivery, the weight of the device is only 10 kg. An inbound rocket, with a minimal amount of explosives, would likely induce less panic than a vehicle delivery method.

TABLE VI  
Drug cartel RDD plot characteristics.

<b>Plot Characteristics</b>	<b>Network Output</b>
Radioactive Material Origin:	Transport Interdiction
Radioactive Material Type:	<sup>60</sup> Co
Presence of Shielding:	65%
Shielding Type:	Steel
Presence of Source Processing:	63.50%
Source Processing Type:	Solid
Explosive Type:	High (Nitroglycerin)
Delivery Method:	Rocket
Detonation Type:	Proximity
Danger from Radioactive Material:	High (58.5%)
Capability to Induce Panic:	Medium (36.5%)
Device Weight:	10 kg

The overall chance of success for a drug cartel RDD plot is seen in Fig. 54. The adversary has a 56.6% chance of successfully obtaining radioactive materials. Greater than the homegrown, Al-Qaeda influenced plot but less than the apocalyptic group plot, the cartel's high tactical capabilities are offset by only a moderate amount of funding and a low technical capability. Consequently, the 56.6% chance of obtaining radioactive material hinges on the cartel's ability to forcefully steal a source in transport. The adversary has a mere 29.9% chance of successfully weaponizing the radioactive material. While the cartel has a significant need for source weaponization, poor technical capabilities hamper this portion of the network. Assembly and detonation should be easily accomplished with an 85.5% chance of success. The overall chance of success for a drug cartel RDD plot is 47.3%.

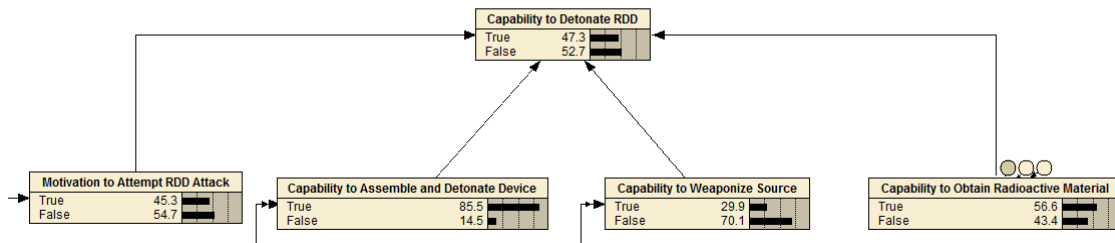


Fig. 54. Overall chance of success for a drug cartel RDD plot.

### *Effect of Increased Funding*

The drug cartel RDD plot was analyzed by introducing increased funding into the Bayesian network. This change was implemented by changing the plot funding from \$250,000 to \$1,000,000. A sudden increase in plot funding could be attributed to collusion with other cartels, or money recovered from a related bank robbery. The significant effects of increased funding are seen in Table VII. Initially acquiring radioactive material through transport interdiction, the network now suggests the adversary will attempt commercial acquisition of  $^{137}\text{Cs}$ . An influx of money certainly increases the probability the cartel would be capable of paying license fees and purchasing a source. The presence of source processing increases moderately from 63.5% to 70.8%, and the additional funding would likely permit the cartel to process the source into small fragments. Most importantly, the danger from radioactive material increases from high at 58.5% to high at 63.6%. More potent plastic explosives, coupled with source processing into easily dispersible fragments, accounts for the increase in danger. As expected, the overall panic inducing ability remains constant.



TABLE VII  
Drug cartel RDD plot characteristics with increased funding.

<b>Plot Characteristics</b>	<b>Network Output</b>
Radioactive Material Origin:	Commercial Acquisition
Radioactive Material Type:	<sup>137</sup> Cs
Presence of Shielding:	71%
Shielding Type:	Lead
Presence of Source Processing:	70.80%
Source Processing Type:	Fragments
Explosive Type:	High (Plastic Explosive)
Delivery Method:	Rocket
Detonation Type:	Proximity
Danger from Radioactive Material:	High (63.6%)
Capability to Induce Panic:	Medium (36.9%)
Device Weight:	10 kg

The overall success of a drug cartel RDD plot with increased funding is shown in Fig. 55. Additional funding results in a higher probability of success for radioactive material acquisition and source weaponization. The probability of success for radioactive material acquisition increases from 56.6% to 71.6%. The probability of success for source weaponization increases from 29.9% to 44.0%. These significant changes are reflected in the overall plot success chance increasing from 47.3% to 60.4%. Therefore, an increase in funding has a substantial effect on the overall likelihood of a successful RDD plot. This example emphasizes the importance of correctly quantifying the funding available to an adversary. Underestimating available funding skews the chance of plot success, and could result in uniformed conclusions about the adversary.

Additionally, law enforcement agencies using this tool should be cognizant of additional funding being funneled into an RDD plot.

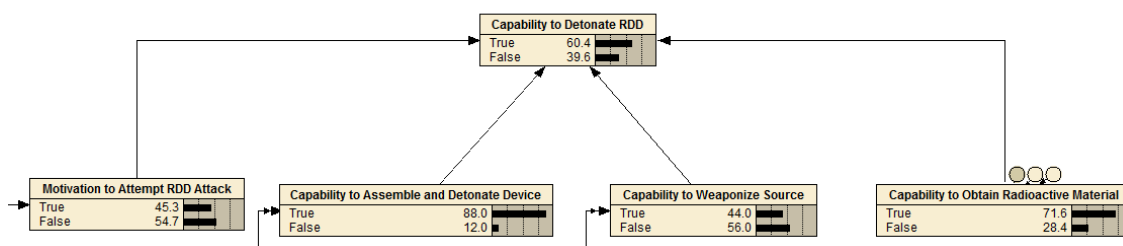


Fig. 55. Overall chance of success for a drug cartel RDD plot with increased funding.

### *Effect of Change in Adversarial Motivation and Evidence of Specific Target*

The drug cartel RDD plot was further analyzed by adjusted the adversarial motivation and including evidence of a specific target. These changes were implemented by activating the “Mass Devastation/Chaos” motivation node and adding evidence that suggested the cartel planned to attack a target in a waterfront city. It is reasonable to assume an adversary may change its motivations mid-plot. Or, law enforcement agencies may have originally mischaracterized the drug cartel’s motivations. The drug cartel may want to exact vengeance on an American target after police raids captured a significant number of low-level drug smugglers. Additionally, intelligence tips may report the cartel wants to attack a waterfront city, such as San Diego, with an RDD. Table VIII shows how the motivation change and evidence

inclusion affect the drug cartel RDD plot. Means of radioactive material acquisition and the specific isotope obtained remain constant from the original drug cartel RDD plot. However, the probability of source processing drops from 63.5% to 46.5%. This result reflects the fact that an adversary aiming for mass devastation would be less concerned about even source dispersal. Another significant change lies in the assembly and detonation portions of the network. The proximity of the cartel's target to the water suggests device delivery by boat. Additionally, the detonation method has switched from proximity to suicide. The device weight has increased to 100 kg. Finally, the capability to induce panic has increased from medium with a 36.5% chance to high with a 41.6% chance. The increase in panic inducing capability reflects a greater amount of explosives and delivery by boat in a populated area.

TABLE VIII  
Drug cartel RDD plot characteristics with a change in motivation and a waterfront city as a target.

<b>Plot Characteristics</b>	<b>Network Output</b>
Radioactive Material Origin:	Transport Interdiction
Radioactive Material Type:	<sup>60</sup> Co
Presence of Shielding:	54%
Shielding Type:	Steel
Presence of Source Processing:	46.50%
Source Processing Type:	Solid
Explosive Type:	High (Nitroglycerin)
Delivery Method:	Boat
Detonation Type:	Suicide
Danger from Radioactive Material:	High (43.1%)
Capability to Induce Panic:	High (41.6%)
Device Weight:	100 kg

The overall chance of success for the drug cartel RDD plot with a motivation change and evidence of a waterfront target city is seen in Fig. 56. The chance of successfully obtaining radioactive material and successfully performing source weaponization does not change from the initial drug cartel RDD plot. However, the motivation to attempt an RDD attack has increased dramatically from 45.3% to 98.6%. The overall chance of successfully detonating an RDD has increased from 47.3% to 53.4%. An RDD is better suited to serve an ultimate motivation of mass devastation and chaos. On the other hand, the dangerous and difficult process of weaponizing and evenly dispersing a radioactive source makes an RDD less useful to an adversary warring with a nation.

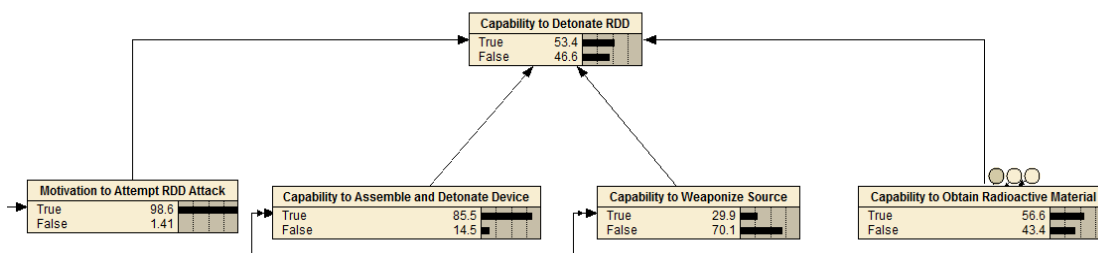


Fig. 56. Overall chance of success for a drug cartel RDD plot with a change in motivation and a water front city as a target.

### Extreme Plot 1: Adversary with Maximum Resources

The next section of case studies examines extreme plots where the adversary is given either the maximum or minimum amount of resources. These case studies do not represent current, real-life adversaries. However, they are useful in analyzing the network's ability to model emerging threats. Also, they help to establish the limiting

cases of the network, and can help elucidate which parts of the network are most sensitive to different types of resources. The first extreme plot analyzed was an adversary with the maximum amount of available resources. This adversary has paramilitary tactical capabilities, developed government lab technical capabilities, and \$2,000,000 of funding for the RDD plot. No motivations were selected for this analysis. The inputs for this case study can be seen in Fig. 57.

The RDD plot characteristics for the extreme case of an adversary with maximum resources can be seen in Table IX. As expected, significant funding and technical capabilities result in a predicted radioactive material acquisition pathway of commercial purchase of  $^{137}\text{Cs}$ . It is interesting to note that the device has only a 65% chance of utilizing lead shielding. This is most likely due to the fact that the adversary also has a high probability of obtaining  $^{241}\text{Am}$ , an alpha emitter, through commercial acquisition. The final device has a 99.2% chance of source processing. Weaponization of the radioactive material is easily achieved with maximum technical capabilities. The network suggests that the RDD will likely be delivered by motor vehicle and detonated by a suicide bomber. Without any specific motivations, the adversary would have no need for a more sophisticated delivery method such as a rocket. Finally, the RDD plot has an extremely high danger of radioactive material and a high chance of inducing panic within the target population.

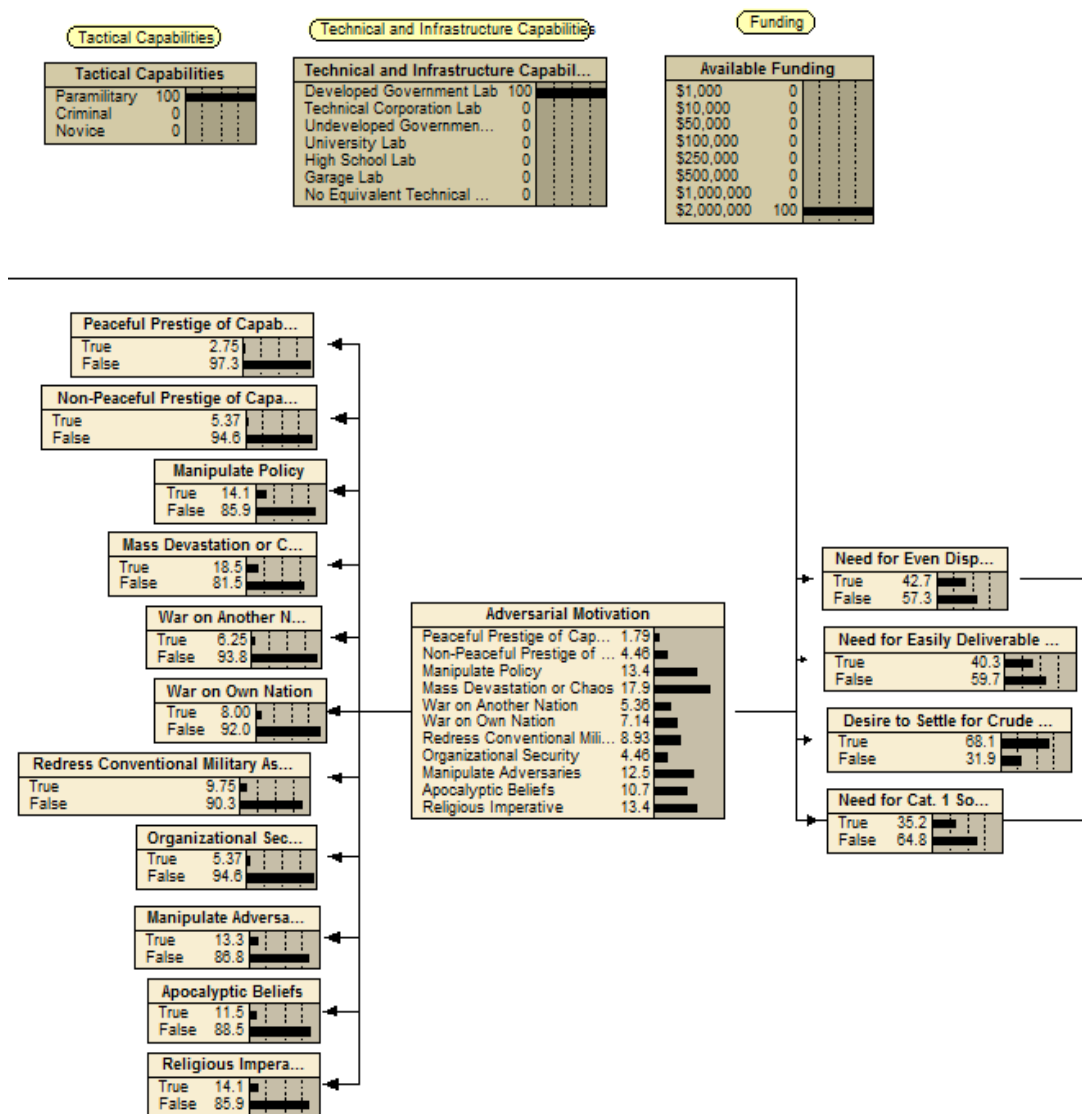


Fig. 57. Inputs for extreme case with maximum resources.

TABLE IX  
RDD plot characteristics for an adversary with maximum resources.

<b>Plot Characteristics</b>	<b>Network Output</b>
Radioactive Material Origin:	Commercial Acquisition
Radioactive Material Type:	<sup>137</sup> Cs
Presence of Shielding:	65%
Shielding Type:	Lead
Presence of Source Processing:	99.20%
Source Processing Type:	Powder
Explosive Type:	High (Plastic Explosive)
Delivery Method:	Motor Vehicle
Detonation Type:	Suicide
Danger from Radioactive Material:	High (80.0%)
Capability to Induce Panic:	High (63.3%)
Device Weight:	500 kg

Studying the first extreme plot provides some interesting insight into the operation of the created Bayesian network. Fig. 58 depicts the overall chance of success for an adversary given the maximum amount of resources. The adversary has a 100% chance of assembling and detonating the device and a 99.9% chance of weaponizing the source. Both of these tasks should be easily completed by an adversary with maximum resources. The adversary has a 97.6% chance of obtaining radioactive materials to utilize in the RDD. It should be noted that even with the maximum amount of resources, it's not guaranteed that an adversary would be able to obtain radioactive materials. This is representative of the fact that an extremely sophisticated adversary may not be willing to settle for smaller, more easily obtainable, radioactive sources. On the other hand, acquiring a significantly strong radioactive source is still a daunting task, even for an

adversary with the maximum amount of resources. The adversary has a 91.6% overall chance of success. This probability appears low, relative to the high chance the adversary has of completing the other required tasks of an RDD plot. However, this low overall chance of success is due to the fact that no motivations were selected as an input into the network. Without a motivation requiring RDD usage, a given adversary, even with maximum resources, is less likely to attempt an RDD plot. This nuance emphasizes the overall importance adversarial motivation has to the created Bayesian RDD acquisition network.

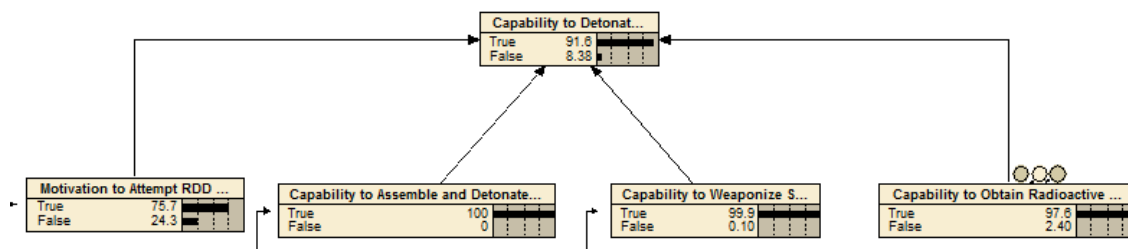


Fig. 58. Overall chance of success for adversary with maximum resources.

## Extreme Plot 2: Adversary with Minimum Resources

The next extreme plot analyzed was an adversary given the minimum amount of resources. This adversary has novice tactical capabilities, no equivalent technical capabilities, and only \$1,000 devoted to the RDD plot. Also, no motivations were selected for this adversary. The network input information for the minimally funded



adversary can be seen in Fig. 59. Similar to the first extreme plot, this case study has no real-life equivalence. However, analyzing an adversary possessing only the minimum amount of resources available in the network is still useful. This type of plot analysis can provide information about which portions of the network are the easiest to accomplish for a poorly resourced adversary.

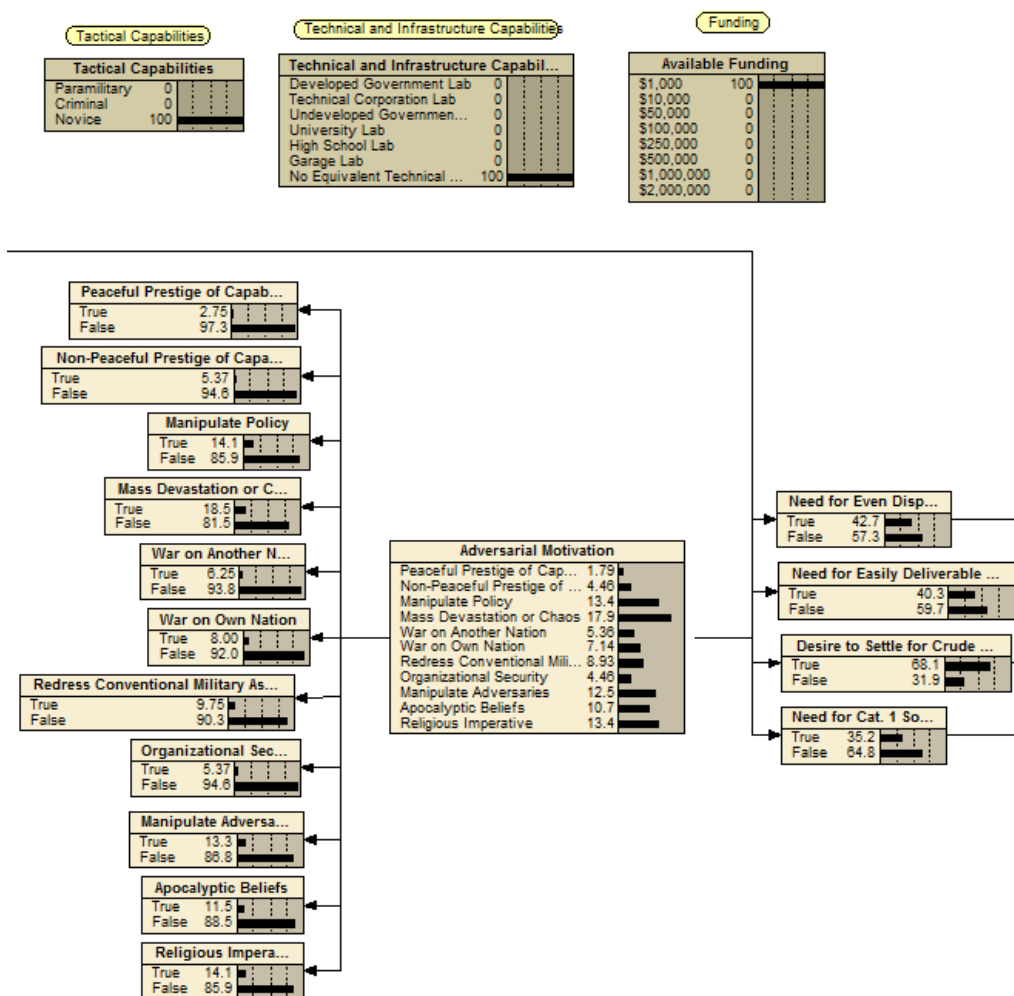


Fig. 59. Inputs for extreme case with minimal funding.

RDD plot characteristics for an adversary with the minimum amount of resources is seen in Table X. The network suggests that the most likely pathway for radioactive material acquisition is from an industrial use facility. Numerous low activity and poorly secured radioactive sources in industrial facilities would represent the highest probability of success for an adversary with few resources. The adversary has a 48% likelihood of utilizing shielding and only a 36.6% chance of processing the source. Any successful source processing would not convert the radioactive source past its original solid form. The likely RDD design includes chlorate high explosives. Chlorate explosives, typically homemade and composed from readily available chemicals, represent the least sophisticated and least expensive explosives pathway. The device would be delivered by motor vehicle and detonated by a suicide bomber. It is interesting to note that this delivery and detonation method is identical to the methods predicted for the adversary with maximum funding. These results emphasize the utility of a suicide car bomb for all types of adversaries. Finally, the device has a high danger from radioactive material and a low capability of inducing panic. For a minimally funded adversary, a highly dangerous RDD would not be expected. However, the network's prediction for radioactive danger provided a nearly uniform distribution between overall danger levels: high at 37.7%, medium at 32.6%, and low at 29.7%. The high prediction should be analyzed in the context of the adversary's overall chance of success.

TABLE X  
RDD plot characteristics for an adversary with minimum resources.

Plot Characteristics	Network Output
Radioactive Material Origin:	Industrial Use
Radioactive Material Type:	$^{137}\text{Cs}$
Presence of Shielding:	48%
Shielding Type:	Steel
Presence of Source Processing:	36.60%
Source Processing Type:	Solid
Explosive Type:	High (Chlorates)
Delivery Method:	Motor Vehicle
Detonation Type:	Suicide
Danger from Radioactive Material:	High (37.7%)
Capability to Induce Panic:	Low (37.9%)
Device Weight:	100 kg

The overall chance of success for an adversary with the minimum amount of resources is seen in Fig. 60. The network predicted the adversary would have a 78.4% chance of successfully assembling and detonating a device. A high probability prediction in this node, even for a minimally resourced adversary, is expected due to the relatively simple tasks of obtaining explosives and wiring the RDD to detonate. On the other hand, the adversary has almost no chance of obtaining radioactive materials or weaponizing the source. In fact, the adversary has a greater chance of obtaining radioactive materials, at 9.84%, than weaponizing the source, at 5.14%. This result demonstrates an interesting behavior of the Bayesian network at low resource levels. Obtaining a low activity, industrial use, radioactive source might be possible for such an adversary. However, successfully weaponizing the source is extremely unlikely.

Successful source weaponization, at low resource levels, is very dependent on technical capabilities. Finally, the minimally funded adversary would have only a 9.27% chance of successfully completing an RDD plot. This chance of success is nearly identical to the adversary's chance of successfully obtaining radioactive materials. At such a low resource level, final RDD plot completion is nearly entirely dependent on the adversary's ability to obtain radioactive material.

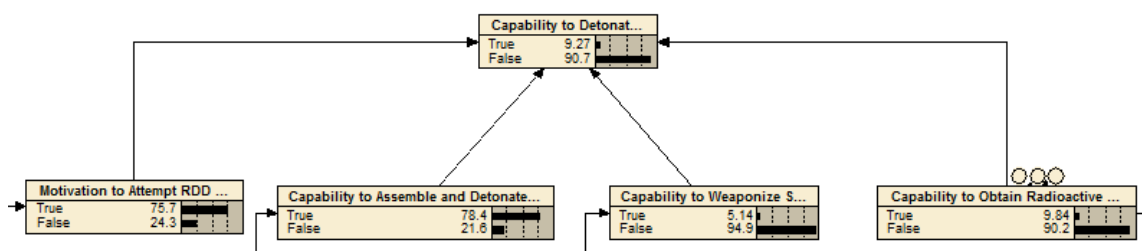


Fig. 60. Overall chance of success for an adversary with minimal funding.

The study of the network at extreme resource levels provides insight into how the model might respond to emerging and future terrorist plots. A recent upswing in domestic and homegrown terrorism likely represents a significant portion of emerging threats. These small plots, orchestrated by a single individual or a small cell, operate with a minimal level of resources. Consequently, effective operation of the Bayesian network at low resource levels is imperative to its eventual utility. The results of the second extreme plot analyzed show that for poorly resourced adversaries, the overall

chance of plot completion is significantly dependent upon radioactive material acquisition. On the other hand, an increasing level of collusion between state actors and terrorist organizations introduces the possibility of an extremely well resourced adversary. In this case, the above analysis suggests that efforts against the adversary must be expanded to include interdiction of source weaponization efforts.

### **Plot Comparison**

The analysis of case studies demonstrates a few important conclusions about this work. Most importantly, the predicted plot probabilities and RDD device characteristics for each case study provided the expected results. Achieving the expected results implies the network is operating properly and can now be applied to emerging RDD threats. Unfortunately, a true calibration of the created network cannot be performed since no historical case studies exist. However, the probabilities of the created network can be adjusted if actual case study data becomes available.

An overview of the RDD characteristics for each of the five case studies is seen in Table XI. Generally, the Bayesian analysis predicted a different pathway for each case study. The predictions include the use of  $^{137}\text{Cs}$  in three of the five cases. The recurring presence of  $^{137}\text{Cs}$  can be attributed to its widespread use in a varying amount of medical and industrial devices, as well as its inherently dispersible form. Consequently, this analysis suggests that efforts to secure radiological materials should first focus on  $^{137}\text{Cs}$  sources. Delivery and detonation methods also remain relatively constant across the five case studies. A motor vehicle delivery with suicide detonation was predicted for

four of the five case studies. The use of a motor vehicle allows for a significantly higher device weight and the flexibility to deliver the RDD inconspicuously. Furthermore, the presence of suicide detonation reaffirms the desperation of many terrorist adversaries, and represents a nearly foolproof method of detonating the RDD at the desired time and place. This result emphasizes the importance of building delay and vehicle standoff devices around vulnerable areas and likely targets.

A comparison of the RDD plot probabilities for the five case studies is seen in Table XII. As expected, the case with maximum resources has the highest probability of success, and the case with minimum resources has the lowest probability of success. These probabilities are 91.6% and 9.3%, respectively. An apocalyptic group has the next highest chance of success at 69.1%. A homegrown, Al-Qaeda influenced plot has the second lowest chance of success at 12.4%. These results convey a few general conclusions about the overall threat of an RDD attack. An RDD attack by the most likely adversaries is unlikely to succeed. Conversely, an RDD attack by the least likely adversaries is more likely to succeed. This feature is similar to the threat of terrorist attacks utilizing nuclear weapons and other WMD. Counter-terrorism efforts have always struggled with this problem. How do you best leverage resources against a terrorist plot that, although extremely unlikely, would have devastating consequences? The question becomes even more convoluted in the case of an RDD attack; a rudimentary and simple device can have the same panic inducing capability as an exceptionally well engineered device. While the developed methodology fails to address

this philosophical question, it does succeed in quantifying the threat posed by such an elusive weapon.

TABLE XI  
Comparison of RDD plot probabilities.

<b>RDD Plot Component</b>	<b>Homegrown, Al-Qaeda Influenced</b>	<b>Apocalyptic Group</b>	<b>Drug Cartel</b>	<b>Maximum Resources</b>	<b>Minimum Resources</b>
Motivation to Attempt RDD Attack:	95.9%	92.6%	45.3%	75.7%	75.7%
Capability of Obtaining Radioactive Materials:	79.4%	95.7%	85.5%	97.6%	9.8%
Capability of Weaponizing Source:	10.9%	90.0%	29.9%	99.9%	5.1%
Capability of Assembling and Detonating Device:	12.9%	70.9%	56.6%	100.0%	78.4%
Probability of Success:	12.4%	69.1%	47.3%	91.6%	9.3%

TABLE XII  
Comparison of RDD plot characteristics.

<b>Plot Characteristic</b>	<b>Homegrown, Al-Qaeda Influenced</b>	<b>Apocalyptic Group</b>	<b>Drug Cartel</b>	<b>Maximum Resources</b>	<b>Minimum Resources</b>
Radioactive Material Origin:	Industrial Facility	Commercial Acquisition	Transport Interdiction	Commercial Acquisition	Industrial Use
Radioactive Material Type:	<sup>137</sup> Cs	<sup>241</sup> Am	<sup>60</sup> Co	<sup>137</sup> Cs	<sup>137</sup> Cs
Presence of Shielding:	47.80%	50.40%	65%	65%	48%
Shielding Type:	Steel	Lead	Steel	Lead	Steel
Presence of Source Processing:	32.20%	91.40%	63.50%	99.20%	36.60%
Source Processing Type:	Solid	Powder	Solid	Powder	Solid
Explosive Type:	Incendiary (Thermite)	High (Plastic Explosive)	High (Nitroglycerin)	High (Plastic Explosive)	High (Chlorates)
Delivery Method:	Motor Vehicle	Motor Vehicle	Rocket	Motor Vehicle	Motor Vehicle
Detonation Type:	Suicide	Suicide	Proximity	Suicide	Suicide
Danger from Radioactive Material:	Medium (35%)	High (72.6%)	High (58.5%)	High (80.0%)	High (37.7%)
Capability to Induce Panic:	High (38.9%)	High (67.4%)	Medium (36.5%)	High (63.3%)	Low (37.9%)
Device Weight:	100 kg	500 kg	10 kg	500 kg	100 kg



## CHAPTER IV

### SENSITIVITY ANALYSIS

The Bayesian network was next studied by performing a sensitivity analysis on various portions of the network. The purpose of a sensitivity analysis is to determine how nodes within the network interact with each other. Many interactions within the network are inherently obvious. For example, subsequent nodes in an acquisition pathway will have a significant effect on each other. However, in a complex network other important interactions may not appear so obvious. Subtle relationships between nodes far apart in the network, or nodes in parallel pathways, can extensively affect each other. These interactions reveal which nodes have the greatest weight in determining the success or failure of other nodes within the network. Consequently, a sensitivity analysis of a certain pathway can uncover which nodes within the pathway are most important to the ultimate completion of that pathway.

This type of analysis is extremely useful in the context of RDD acquisitions. To complete a given portion of the RDD acquisition network, the adversary must successfully navigate a long series of tasks. Some of these tasks may be mandatory to complete the pathway. Others may be optional. For example, an adversary must obtain radioactive materials to successfully detonate an RDD; however, processing the source is not a requirement. How can a law enforcement agency determine which actions to focus on to best halt the RDD plot? A sensitivity analysis provides a quantitative answer to this important question.

A feature programmed into the *Netica* software package easily performs a sensitivity analysis on any Bayesian belief network. The user first selects a node on which to perform the sensitivity analysis. Any node within the network can be selected for the analysis, but nodes providing probabilities of pathway completion and RDD characteristics are the best options. Next, the operation “Sensitivity to Findings” is selected under the “Network” menu option. *Netica* then provides a sensitivity report with two parts. The first part describes how each node in the network affects the selected node using several different sensitivity measures. The second portion of the report summarizes how every node within the network affects the findings node. The summary includes three columns: mutual information, percent, and variance of beliefs. Percent describes what percentage of the selected node’s results are due to other nodes in the network. This measure was utilized in the sensitivity analysis.

A sensitivity analysis was first performed on the node titled “Overall Danger from Radioactive Exposure”. This analysis can be seen in Fig. 61. For this and the remaining sensitivity analyses, it should be noted that only the top ten affecting nodes were plotted in pie charts. Also, the percentages are not normalized to 100% since each portion of the plot represents the degree to which the listed node influences the selected node. Fig. 61 shows that the presence of source processing has the greatest effect on the overall danger from radioactive exposure. A finely processed source is easily dispersed, and subsequently inhaled and ingested by the target population. Radioactive emission type has the next greatest effect on danger from radioactive exposure. Depending on the level of source processing, the overall danger could vary depending on what type of

radiation the source emits. This analysis demonstrates that in order to mitigate health effects of an RDD plot, law enforcement agencies should focus on preventing the adversary from weaponizing the radioactive source.

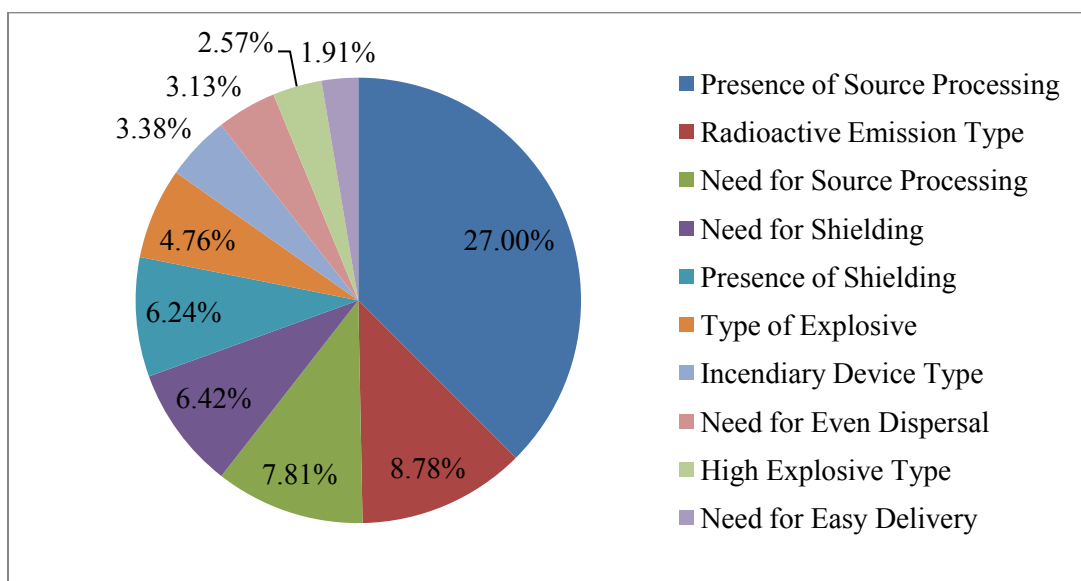


Fig. 61. Sensitivity findings for “Overall Danger from Radioactive Exposure” node.

Figure 62 shows the results for a sensitivity analysis of the “Panic Inducing Capability” node. This node quantifies the overall ability of a given RDD plot to induce panic among the target population. Fig. 62 shows that the chosen delivery method has the greatest effect on panic inducing capability. An RDD delivered by a motor vehicle is larger, likely to contain more explosives, and has a greater chance of disrupting an urban population. On the other hand, a smaller RDD delivered by rocket or mortar would contain a smaller amount of explosives and result in less disruption. Other nodes influencing the panic inducing capability of the RDD include the type of explosive

utilized in the design. The detonation of high explosives produces a shockwave that can travel for many city blocks. Conversely, incendiary devices burn slower than the speed of sound and do not produce shockwaves. This analysis demonstrates that law enforcement agencies attempting to mitigate the disrupting abilities of an RDD should be less concerned about radioactive material acquisition. Instead, they should focus on the delivery method and type of explosives used in the device.

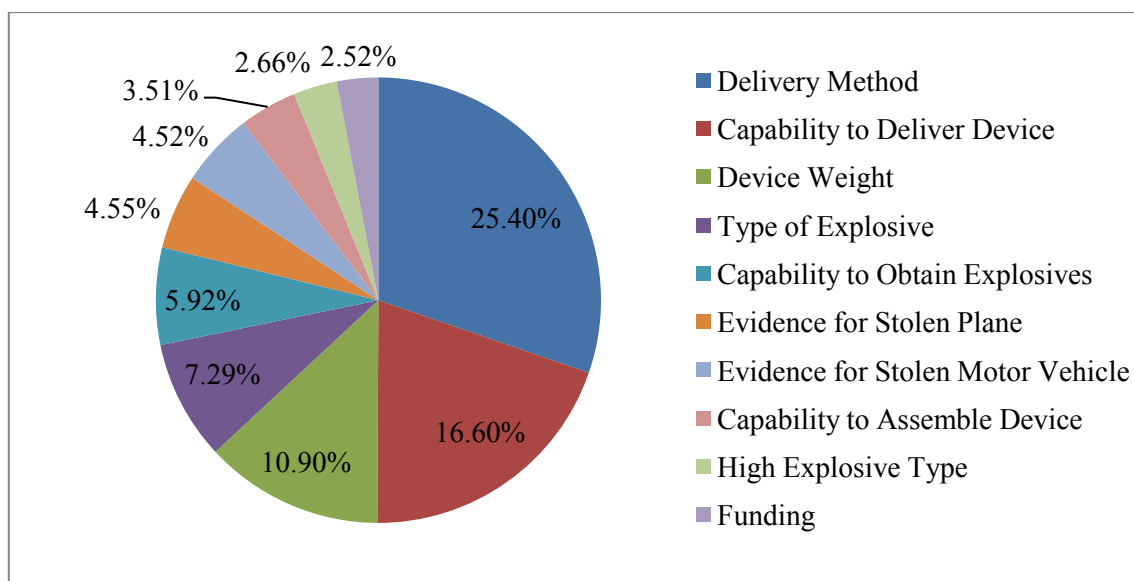


Fig. 62. Sensitivity findings for “Panic Inducing Capability” node.

Figure 63 shows the results of a sensitivity analysis for the “Capability to Weaponize Source” node. This node represents the adversary’s overall ability to weaponize radioactive material for use in an RDD. Source weaponization includes both source processing—changing the physical form of the source to increase dispersion—and acquisition of shielding material. The plot shows that the two most influential nodes

within the network are “Capability to Process Source” and “Source Processing Type.” These findings reflect the fact that successful source weaponization is heavily weighted towards source processing since obtaining radioactive shielding is usually not a difficult task. The third and fourth most influential nodes are “Funding” and “Technical Capabilities.” These nodes represent two adversary characteristics. Successful source weaponization requires laboratory facilities and significant funding to handle the difficult process of grinding or dissolving a highly dangerous radioactive source. These results demonstrate a few useful generalizations the constructed Bayesian network implies. First, source processing is not likely for a poorly funded adversary with few technical capabilities. Law enforcement agencies should instead focus on countering this type of adversary’s plot by preventing the acquisition of radioactive material. Second, well-resourced adversaries may be most vulnerable to law enforcement action during the source weaponization process. These types of adversaries will likely expend a great deal of resources to attempt source weaponization. Indicators of source processing, such as laboratory equipment purchases, can be used to identify and take action against the adversary.

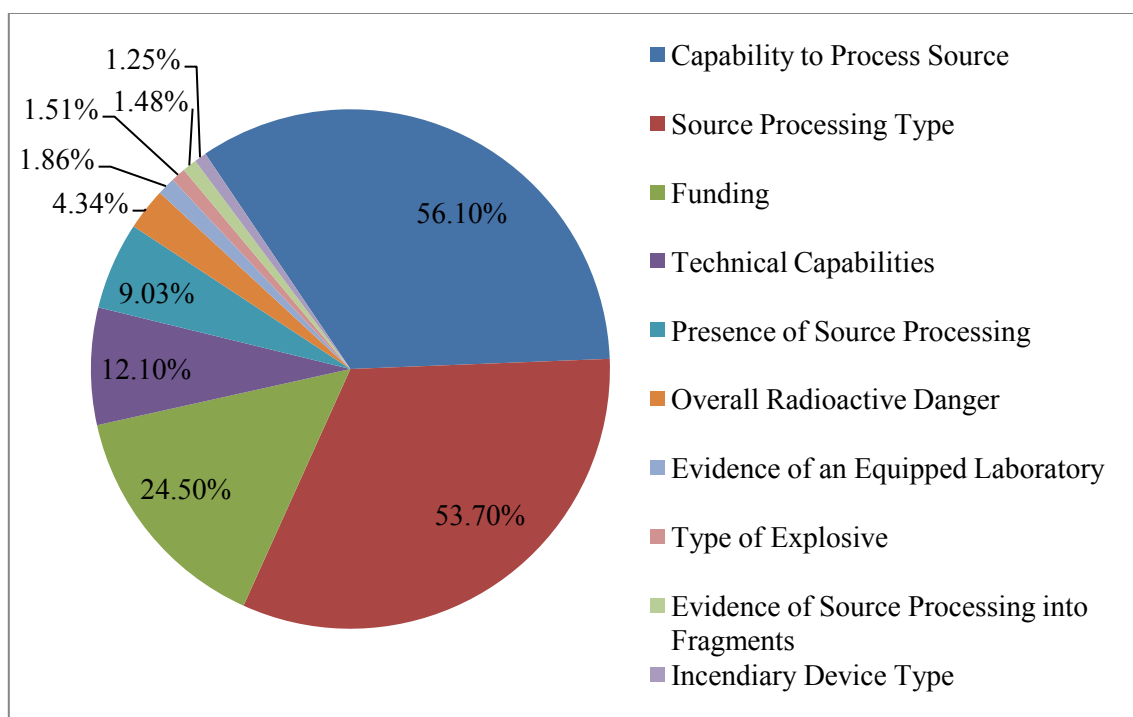


Fig. 63. Sensitivity findings for “Capability to Weaponize Source” node.

Figure 64 displays the results of a sensitivity analysis on the “Capability to Assemble and Detonate Device” node. This node represents the overall chance of success the adversary has in obtaining explosives, devising a delivery method, and detonating an RDD. The figure shows that the two most influential nodes are “Type of Explosive” and “Capability to Obtain Explosives.” Obtaining explosives to utilize in an RDD is more difficult than both delivering and detonating the device. However, the other eight nodes listed in Fig. 64 have a relatively similar influence on the adversary’s capability to assemble and detonate the device. This result demonstrates the serial nature of this node. An adversary must complete all three steps of assembly and detonation in a sequential manner. Consequently, successful law enforcement actions

against either the adversary's attempt to obtain explosives, a delivery method, or detonation components all have similar affects on interrupting the RDD plot.

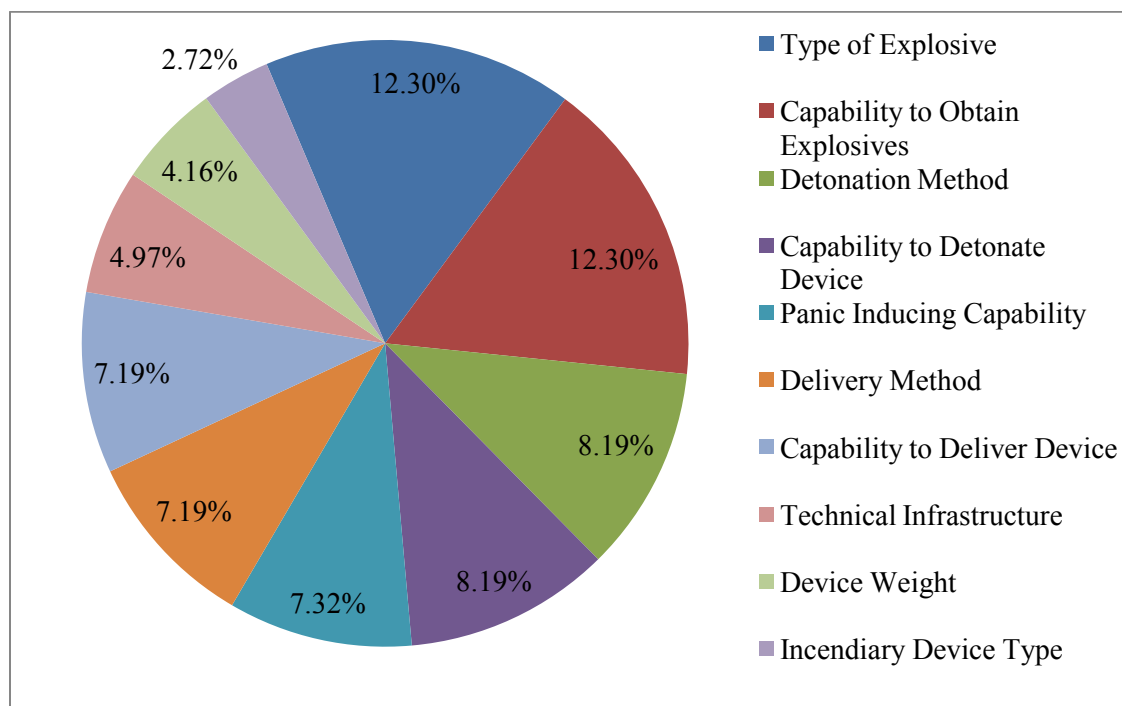


Fig. 64. Sensitivity findings for “Capability to Assemble and Detonate Device” node.

Figure 65 shows the results of a sensitivity analysis on the “Overall Probability of RDD Plot Success” node. This node represents the adversary's chance of completing all required pathways to RDD detonation and gives an overall chance of plot success. As expected, the node is extremely dependent upon the adversary's capability to obtain radioactive material. This reinforces the fact that a successful RDD cannot be constructed without radioactive materials. The second and third most influential nodes are “Type of Radionuclide” and “Radioactive Material Origin.” These nodes further

reflect the importance of radioactive material acquisition on final RDD plot completion. The fourth, fifth, and sixth most influential nodes are “Technical Capabilities,” “Funding,” and “Tactical Capabilities.” These nodes represent the three adversary characteristics defined as inputs into the Bayesian network. It is interesting to note that in terms of final plot success, obtaining radioactive material is vastly more important than the characteristics of the adversary. A terrorist organization with no technical or tactical capabilities and no funding can still pose a significant RDD threat if they have successfully obtained radioactive material. On the other hand, an adversary with exceptional capabilities and funding will pose little danger without successful acquisition of radioactive material. The sensitivity analysis presented in Fig. 65 demonstrates that law enforcement agencies should generally focus their efforts on preventing adversaries from obtaining radioactive materials. Also, these results emphasize the importance of securing radioactive materials in mitigating the RDD threat.



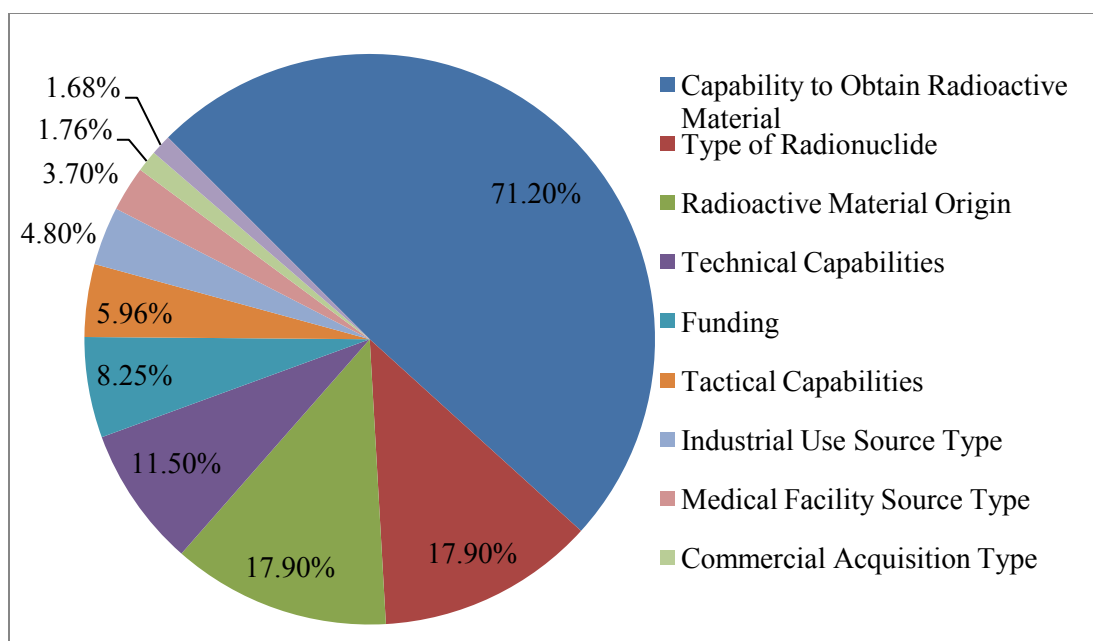


Fig. 65. Sensitivity findings for “Overall Probability of RDD Plot Success” node.

The above sensitivity analysis serves to highlight important conclusions that can be drawn from the created Bayesian network. Unlike a case study analysis, where conclusions are drawn about a specific adversary, the results of a sensitivity analysis are applicable to all cases and all possible adversaries. Consequently, the results can be used to derive general conclusions about the RDD threat. These conclusions can be summarized in a few key points:

1. Law enforcement agencies should focus on preventing source weaponization in order to mitigate the ultimate health effects of an RDD plot.

2. For a poorly funded adversary, law enforcement agencies should mainly focus on preventing radioactive material acquisition.
3. Well-resourced adversaries may be most vulnerable during attempts at source weaponization.
4. Successful law enforcement actions against either the adversary's attempt to obtain explosives, a delivery method, or detonation components all have similar effects on interrupting the RDD plot.
5. Without specific knowledge of the adversary, law enforcement agencies should almost always focus their efforts on preventing adversaries from obtaining radioactive materials.
6. The most important step in mitigating the RDD threat involves securing radioactive materials.

## CHAPTER V

### CONCLUSIONS

This work accomplished multiple objectives with the purpose of countering radiological terrorism in the form of RDDs. The first objective was to develop a comprehensive network of all available pathways to RDD acquisition. The second objective was to develop an analysis tool capable of predictive modeling of RDD acquisitions by various adversaries. Lastly, the network suggested generalized law enforcement actions in order to combat the wide range of RDD plots. This was not an initial objective of the work, but manifested itself after the performance of a sensitivity analysis. The developed methodology is capable of evaluating the RDD threat posed by various terrorist adversaries and integrating with real-time intelligence in order to provide an evolving assessment of how close an adversary may be to RDD acquisition.

The methodology was implemented in a Bayesian belief network constructed in the *Netica* software package. The network includes five sections that comprise the pathway to RDD acquisition: adversary motivations and inputs, radioactive material acquisition, source weaponization, assembly and detonation, and final RDD probabilities and characteristics. Additionally, three separate constant nodes allow the user to adjust characteristics describing specific adversaries. These characteristics include tactical capabilities, technical capabilities, and funding. Numerous evidence nodes within the network describe flags or signals that may indicate an adversary is pursuing a particular pathway. These evidence nodes can be turned on and off by the user to customize the model to specific threats. Finally, a set of nodes describes the probabilities of pathway

completion and draws information from within the network to predict the danger level and panic inducing capability of a successful RDD acquisition.

Verification of the developed methodology demonstrated that the Bayesian RDD acquisition network was operating as expected. First, three case studies were analyzed. Each of these case studies utilized the network's customizable inputs to represent likely terrorist adversaries. The case studies demonstrated various features of the constructed Bayesian RDD acquisition network and provided evidence of which terrorist RDD plots are most likely to succeed. Next, extreme cases with either maximum or minimum adversary resources were studied in order to determine the limitations of the constructed Bayesian network. Finally, a sensitivity analysis was performed on those nodes representing overall success probabilities and final device characteristics. These results showed which portion of the network were most vulnerable to law enforcement efforts in disrupting a terrorist plot. The sensitivity analysis produced six general conclusions:

1. Law enforcement agencies should focus on preventing source weaponization in order to mitigate the ultimate health effects of an RDD plot.
2. For a poorly funded adversary, law enforcement agencies should mainly focus on preventing radioactive material acquisition.

3. Well-resourced adversaries may be most vulnerable during attempts at source weaponization.
4. Successful law enforcement actions against either the adversary's attempt to obtain explosives, a delivery method, or detonation components all have similar effects on interrupting the RDD plot.
5. Without specific knowledge of the adversary, law enforcement agencies should almost always focus their efforts on preventing adversaries from obtaining radioactive materials.
6. The most important step in mitigating the RDD threat involves securing radioactive materials.

The main limitation of this work stems from the fact that an RDD has yet to be successfully employed by a terrorist organization. The lack of historical case studies presented a significant hurdle when attempting to verify the operation of the Bayesian network. However, the network was successfully verified against intuitive and likely terrorist plots to develop the conditional probability tables that govern the network's calculations. Future use of this tool should consider any successful RDD acquisitions, and assess whether the network operates correctly in the presence of actual case study data. Another limitation of this work included a relatively limited number of evidence

nodes. While the evidence nodes included in the network reflect the most likely signals of RDD pathway completion, they do not characterize adversary collaboration or deception efforts. Future work on this tool could include the following tasks:

1. Add additional input nodes to increase the characterization of various adversaries.
2. Investigate a method to account for collaboration between different adversaries. This addition could allow for resource and knowledge sharing.
3. Include further evidence nodes that more fully characterize all aspects of RDD acquisition.
4. Upon a successful RDD acquisition, update conditional probability tables to ensure proper network operation.

This work presents the first probabilistic modeling of RDD acquisition pathways. It will not be a universal solution to the threat of an RDD attack. However, its generalized and adaptable approach will help to focus counter-terrorism efforts in a world with innumerable, and often unsecured, radiological sources and a frighteningly large amount of individuals willing to do harm to the United States.

## REFERENCES

1. G. J. Van Tuyle, "Assessing the Radiological Dispersal Devices Threat and Addressing the Vulnerabilities," submitted to International Approaches to Nuclear And Radiological Security, LA-UR-02-5567 (2002).
2. B. M. Jenkins, "Terrorist Radicalization in the United States Since September 11, 2001," Occasional Paper, RAND Corporation, (2010).
3. R. Esposito and B. Ross, "EXCLUSIVE: Photos of the Northwest Airlines Flight 253 Bomb," *ABC News*, WWW Document , (<http://abcnews.go.com/Blotter/northwest-airlines-flight-253-bomb-photos-exclusive/story?id=9436297>), accessed August 2010.
4. "Raids net 3 suspected of funding Times Square bombing attempt," WWW Document, ([http://www.washingtonpost.com/wpdyn/content/gallery/2010/05/04/GA20100504\\_02214.html](http://www.washingtonpost.com/wpdyn/content/gallery/2010/05/04/GA20100504_02214.html)), accessed August 2010.
5. R. A. Hudson, "The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why?," Washington DC: Federal Division Library of Congress, (1999).
6. P. D. Zimmerman and C. Loeb, "Dirty Bombs: The Threat Revisited," *Defense Horizons*, **38**, 1-11, (2004).
7. C. R. Freeman, "Bayesian Network Analysis of Nuclear Acquisitions," M.S. Thesis, Nuclear Engineering, Texas A&M University, College Station, TX (2008).
8. D. G. Ford, "Assessment Tool for Nuclear Material Acquisition Pathways" M.S. Thesis, Nuclear Engineering, Texas A&M University, College Station, TX (2008).
9. Personal communication with I. L. Eaton and K. A. Miller, Los Alamos National Laboratory, August 15, 2010.
10. J. W. Poston, "Current Challenges in Countering Radiological Terrorism," Warren K. Sinclair Keynote Address, *Health Physics Society*, **89**, (5), 450 (2005).
11. H. R. Elder, "Polonium-210 as a Poison on an Aircraft," M.S. Thesis, Nuclear Engineering, Texas A&M University, College Station, TX (2008).

12. E. P. MacKerrow, "Understanding Why—Dissecting Radical Islamist Terrorism with Agent-based Simulation," *Los Alamos Science*, **28**, 184 (2003).
13. J. L. Darby, "Evaluation of Risk for Acts of Terrorism Using Belief and Fuzzy Sets," *Journal of Nuclear Materials Management*, **35**, 19-34 (2007).
14. "Categorization of Radioactive Sources," *IAEA Safety Standards*, Safety Guide No. RS-G-1.9, (2005).
15. G. J. Van Tuyle, T. L. Strub, H. A. O'Brien, C. F. V. Mason, S. J. Gitomer, "Reducing RDD Concerns Related To Large Radiological Source Applications," Los Alamos National Laboratory, LA-UR-03-6664 (2003).
16. Testimony before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, U.S. Senate, "Nuclear Security: Actions Taken by NRC to Strengthen Its Licensing Process for Sealed Radioactive Source Are Not Effective," *Government Accountability Office*, (2007).
17. J. L. Ford, "Radiological Dispersal Devices: Assessing the Transnational Threat," *Strategic Forum*, **136** (1998); available on the Internet at (<http://www.au.af.mil/au/awc/awcgate/ndu/forum136.htm>).
18. "Najibullah Zazi Pleads Guilty to Conspiracy to Use Explosives Against Persons or Property in U.S., Conspiracy to Murder Abroad, and Providing Material Support to Al-Qaeda," *Press Release*, United States Department of Justice, (2010).
19. B. W. Morgan, *An Introduction to Bayesian Statistical Decision Processes*, Prentice-Hall, Inc., Englewood Cliffs, NJ (1968).
20. C. Howson, *Scientific Reasoning: The Bayesian Approach*, Open Court, Chicago (2006).
21. D. Nikovski, "Constructing Bayesian Networks for Medical Diagnosis from incomplete and Partially Correct Statistics," *Knowledge and Data Engineering*, **12**, 509-516 (2000).
22. T. Bayes, "An Essay towards Solving a Problem in the Doctrine of Chances," *Phil. Trans. Roy. Soc.*, **53**, 370 (1763).
23. Z. Ni, L. D. Phillips, and G. B. Hanna. "The Use of Bayesian Networks in Decision-Making," *Key Topics in Surgical Research and Methodology*, Springer-Verlag, Berlin Heidelberg (2010).



24. Netica, Bayesian Network Software, Norsys Software Corp; available on the Internet at (<http://www.norsys.com>).
25. T. Karon, M. Calabresi, M Thompson, “Times Square Bomb Arrest Raises U.S. Security Questions,” *TIME*, (2010); available on the Internet at (<http://www.time.com/time/nation/article/0,8599,1987126,00.html>).
26. “Combating Nuclear Terrorism: Lessons from Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor,” Research Brief, Rand Corporation, (2005).
27. A. G. Schaefer, B. Bahney, K. J. Riley, “What are U.S. Policy Options for Dealing with Security in Mexico?,” Rand Corporation, (2009).

**VITA**

Name: Grant Richard Hundley

Address: Texas A&M University  
Department of Nuclear Engineering  
3133 TAMU  
College Station, TX 77843-3133

E-mail Address: [grhundley@comcast.net](mailto:grhundley@comcast.net)

Education: B.S., Physics, United States Naval Academy, 2009  
M.S., Nuclear Engineering, Texas A&M University, 2010