Decision Analysis Affinity Group 2009

May 18, 2009

Intelligent Adversary Risk Analysis: Defender-Attacker-Defender Probabilistic Risk Analysis Models

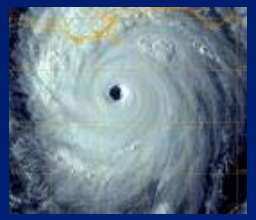
Dr. Greg Parnell
Professor of Systems Engineering
Department of Systems Engineering
United States Military Academy at West Point
gregory.parnell@usma.edu
&
Senior Principal, Innovative Decisions Inc.
gparnell@innovativedecisions.com

MAJ Chris Smith
Department of Mathematical Sciences
Dr. Fred Moxley
Department of Electrical Engineering and Computer Science
United States Military Academy at West Point

Disclaimer

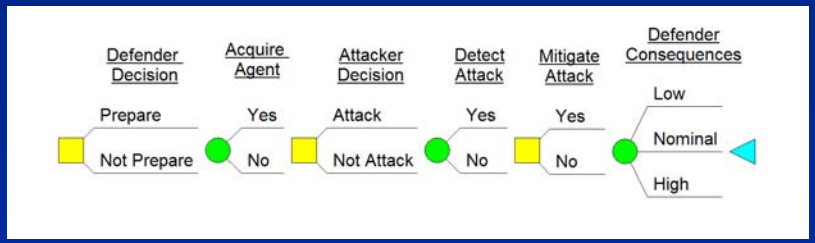
The views expressed in this presentation are those of the authors and do not reflect the official policy or position of the United States Army, the Department of Defense, Innovative Decisions, Inc., the National Research Council, or the Department of Homeland Security.

Purpose

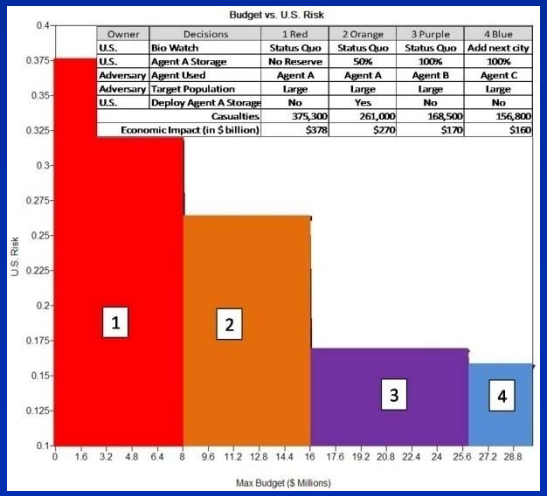



- Understand that intelligent adversary risk analysis is fundamentally different than natural and engineering hazard risk analysis

- Describe the fundamental structure of the intelligent adversary risk analysis using probabililstic risk analysis



- Demonstrate that decision trees implemented in COTS software can model the defender-attacker-defender structure and provide a risk management tool (illustrated with bioterrorism risk analysis using notional data)



Outline

- Background
  - Risk analysis definitions
  - Bioterrorism threat
- DHS Bioterrorism risk assessment
  - Event tree model
  - National Research Council report (2008)
- Intelligent adversary risk analysis
  - Defender-Attacker-Defender
  - Decision tree model
  - Risk management applications
  - Alternative modeling assumptions

Definitions

- **Risk** is the probability of a bad outcome
- **Risk analysis**
  - Includes risk assessment, risk communication, and risk management
  - Considers the threat, vulnerability, and consequences
- **Threat** includes capability and intent
- **Intelligent adversary risk analysis**
  - Risk analysis that models adversaries making decisions to maximize the potential to achieve their objectives based on dynamic information
- **Probabilistic intelligent adversary risk analysis**
  - Assesses probabilities for capabilities, vulnerabilities, and consequences
  - Solves for intent probabilities (decisions) based on dynamic information available to adversary and defender

Bioterrorism Background

- Definition of Bioterror*
  - The deliberate release of viruses, bacteria or other germs (agents) used to cause illness or death in people, animals or plants
- Concerns
  - 1984 Rajneeshee BioTerror attack; The Dalles, Oregon, 751 infected, 45 hospitalized with salmonella for political reasons
  - 2001 Congress and Media Anthrax Letters, 17 infected, 5 deaths; Anthrax; est $6 billion effect on economy due to fear (Commission Report, pg 8)
  - Soviet and Iraq old Bioweapons programs have numerous unaccounted for Bioweapons
  - Bioweapons can be cheap (relative to nuclear or suicide bombers) and create mass hysteria with a small amount of material

*CDC Website, Bioterrorism Overview. <http://emergency.cdc.gov/bioterrorism/overview.asp >01 Oct 08

Views on bioterrorism threat

"One of our greatest concerns continues to be that a terrorist group or some other dangerous group might acquire and employ biological agents…to create casualties greater than September 11."

Michael McConnell, Director of National Intelligence
World at Risk: The Report of the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, Vintage Books, NY. 2008. pg. 4.

"The commission believes that unless the world community acts decisively and with great urgency, it is more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013… The Commission further believes that terrorists are more likely to be able to obtain and use a biological weapon than a nuclear weapon."

World at Risk: The Report of the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, Vintage Books, NY. 2008. pg. xv.

Outline

- Background
  - Risk analysis definitions
  - Bioterrorism threat
- DHS Bioterrorism risk assessment
  - Event tree model
  - National Research Council report (2008)
- Intelligent adversary risk analysis
  - Defender-Attacker-Defender
  - Decision tree model
  - Risk management applications
  - Alternative modeling assumptions

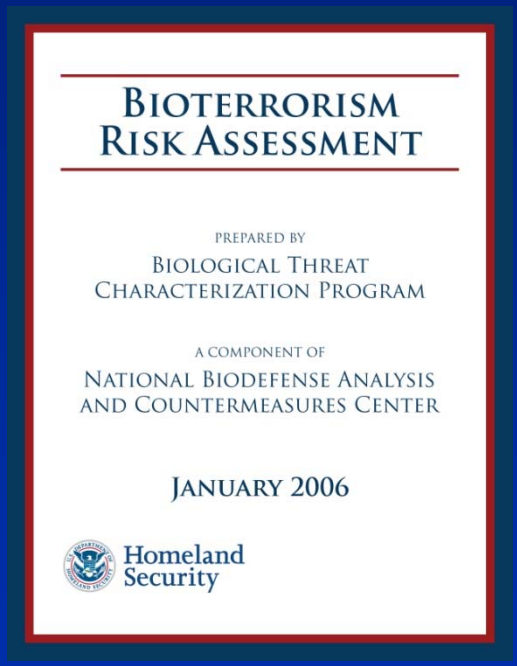
Risk assessments are required by Homeland Security Presidential directives

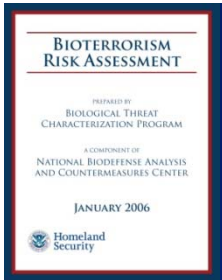
HSPD-10: Biodefense for the 21st Century, April 28, 2004. Another critical element of our biodefense policy is the development of periodic assessments of the evolving biological weapons threat. First, the United States requires a continuous, formal process for conducting routine capabilities assessments to guide prioritization of our on-going investments in biodefense-related research, development, planning, and preparedness.

HSPD-18: Medical Countermeasures against Weapons of Mass Destruction: January 31, 2007. The Secretary of Homeland Security shall develop a strategic, integrated all-CBRN risk assessment that integrates the findings of the intelligence and law enforcement communities with input from the scientific, medical, and public health communities.

2006 DHS Bioterrorism Risk Assessment (BTRA) Model

- Managed by National Biodefense Analysis and Countermeasures Center, Science & Technology Directorate, DHS
- Developed by Battelle, Columbus
- Completed Jan 31, 2006, released Oct 2006
- Prioritizes groups of biological threat agents
- Combines Probabilistic Risk Assessment (PRA), event trees, expert elicitation, and susceptible, exposed, infected, and recovered (SEIR) models of consequence to produce normalized measures of risk



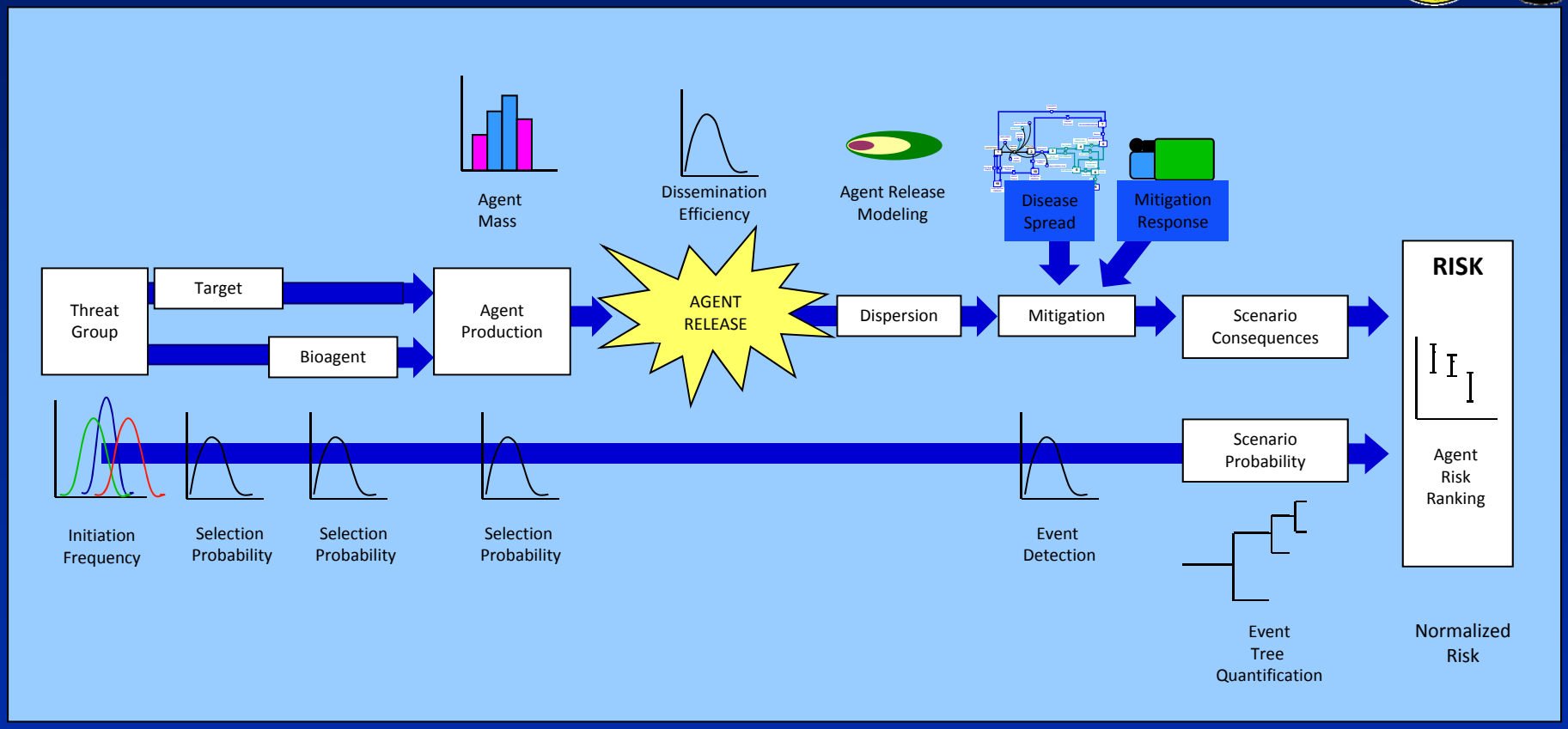


28 bioagents were considered.

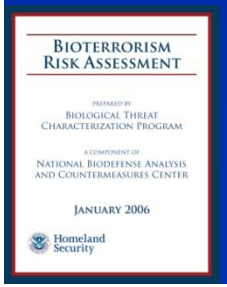
CDC Category A Agents: (9 agents)	CDC Category B Agents: (15 agents)	CDC Category C Agents: (3 agents)	Genetically Engineered Agents: (1 agent)
• *Bacillus anthracis* • *Clostridium botulinum* toxin • Ebola virus (a VHF) • *Francisella tularensis* • Junin virus (a VHF) • Lassa virus (a VHF) • Marburg virus (a VHF) • Variola major • *Yersinia pestis*	• *Brucella suis* • *Burkholderia mallei* • *Burkholderia pseudomallei* • *Chlamydia psittaci* • *Clostridium perfringens* epsilon toxin • *Coxiella burnetii* • *Cryptosporidium parvum* • Eastern equine encephalitis virus • *Escherichia coli* O157:H7 • *Rickettsia prowazekii* • Ricin • *Salmonella typhi* • Shigella toxin • Staphylococcal enterotoxin B • *Vibrio cholerae*	• Bovine Spongiform Encephalopathy • Nipah virus • Rift Valley Fever virus	• MDR *Bacillus anthracis*

Centers for Disease Control, www.bt.cdc.gov/Agent/Agentlist.asp

2006 DHS Bioterrorism Risk Assessment (BTRA) used probabilistic risk analysis with event trees



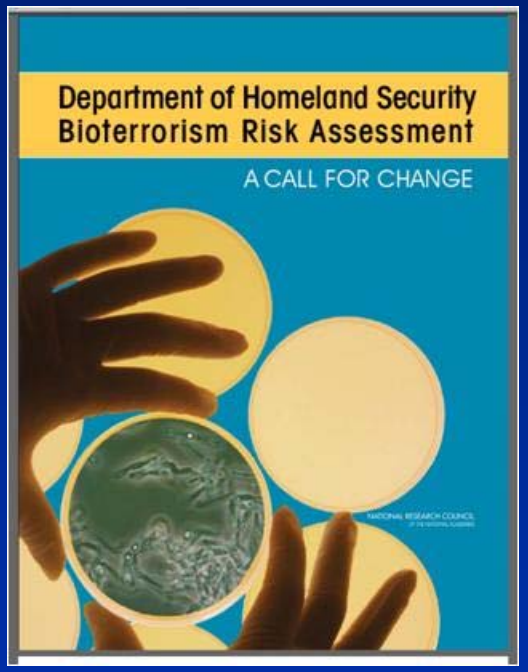
The chart is a simplification of the 17-step event-tree (18 step with consequences) that could lead to the deliberate exposure of civilian populations for each of the 28 pathogens.



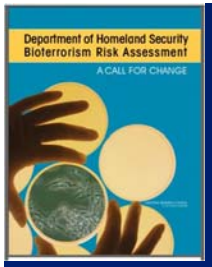
DHS (Department of Homeland Security). 2006. *Bioterrorism Risk Assessment*. Biological Threat Characterization Center of the National Biodefense Analysis and Countermeasures Center. Fort Detrick, Md.

NRC Report: DHS Bioterrorism Risk Assessment

- NRC conducted a review of the 2006 DHS Bioterrorism Risk Assessment
- Twelve committee members with expertise in risk analysis, public health, microbiology and infectious disease, epidemiology, statistics, operations research, and economics.
- Tasked with assessing and identifying recommendations for improvement
- Study recommended significant changes, specifically the study provided 11 recommendations for improvement
  - Model intelligent adversaries
  - Focus on risk management
- Published Sep 26, 2008



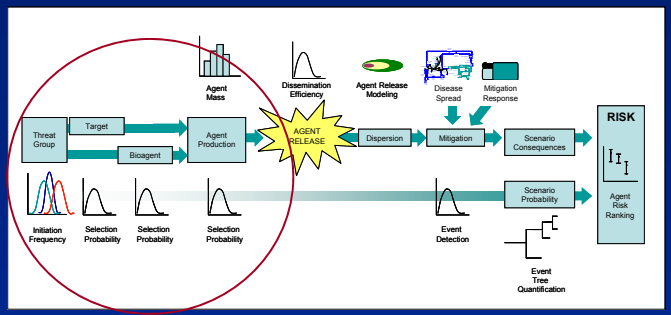
Department of Homeland Security's Bioterrorism Risk Assessment: A Call for Change, Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis, National Research Council of the National Academies, 2008, The National Academy Press, Washington, DC, http://www.nap.edu/catalog.php?record_id=12206



Improve modeling of intelligent adversaries and focus on risk management.

Findings: Terrorists are intelligent adversaries who will react to U.S. preparations and actions. Terrorists do not assign probabilities to their decisions. Instead, they make decisions to maximize the potential to achieve their objectives. Techniques are available to model terrorists actions dynamically.

Recommendation: In addition to using event trees, DHS should explore alternative models of terrorists as intelligent adversaries who seek to maximize the achievement of their objectives.



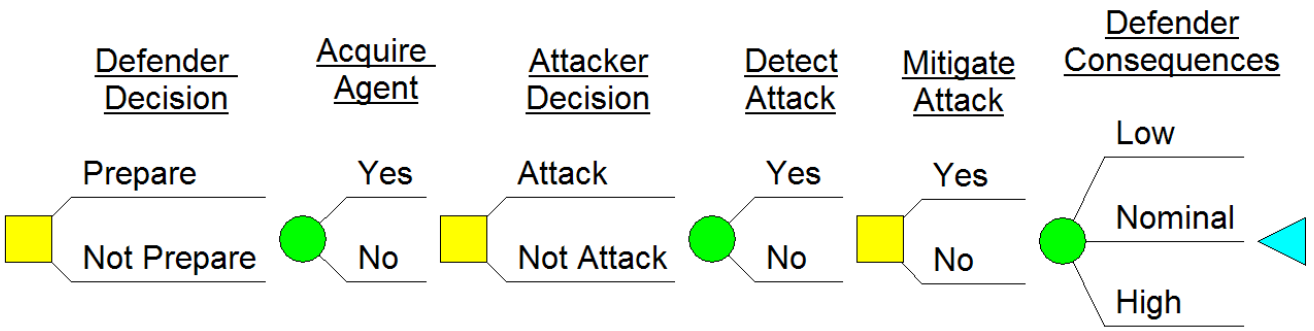
Findings: Risk assessment alone has no direct impact on risk reduction; only the implementation of effective risk management strategies can reduce risk.

Recommendation: Subsequent revision of the BTRA should increase emphasis on risk management. An increased focus on risk management will allow the BTRA to better support the risk-informed decisions that homeland security stakeholders are required to make.

Outline

- Background
  - Risk analysis definitions
  - Bioterrorism threat
- DHS Bioterrorism risk assessment
  - Event tree model
  - National Research Council report (2008)
- Intelligent adversary risk analysis
  - Defender-Attacker-Defender
  - Decision tree model
  - Risk management applications
  - Alternative modeling assumptions

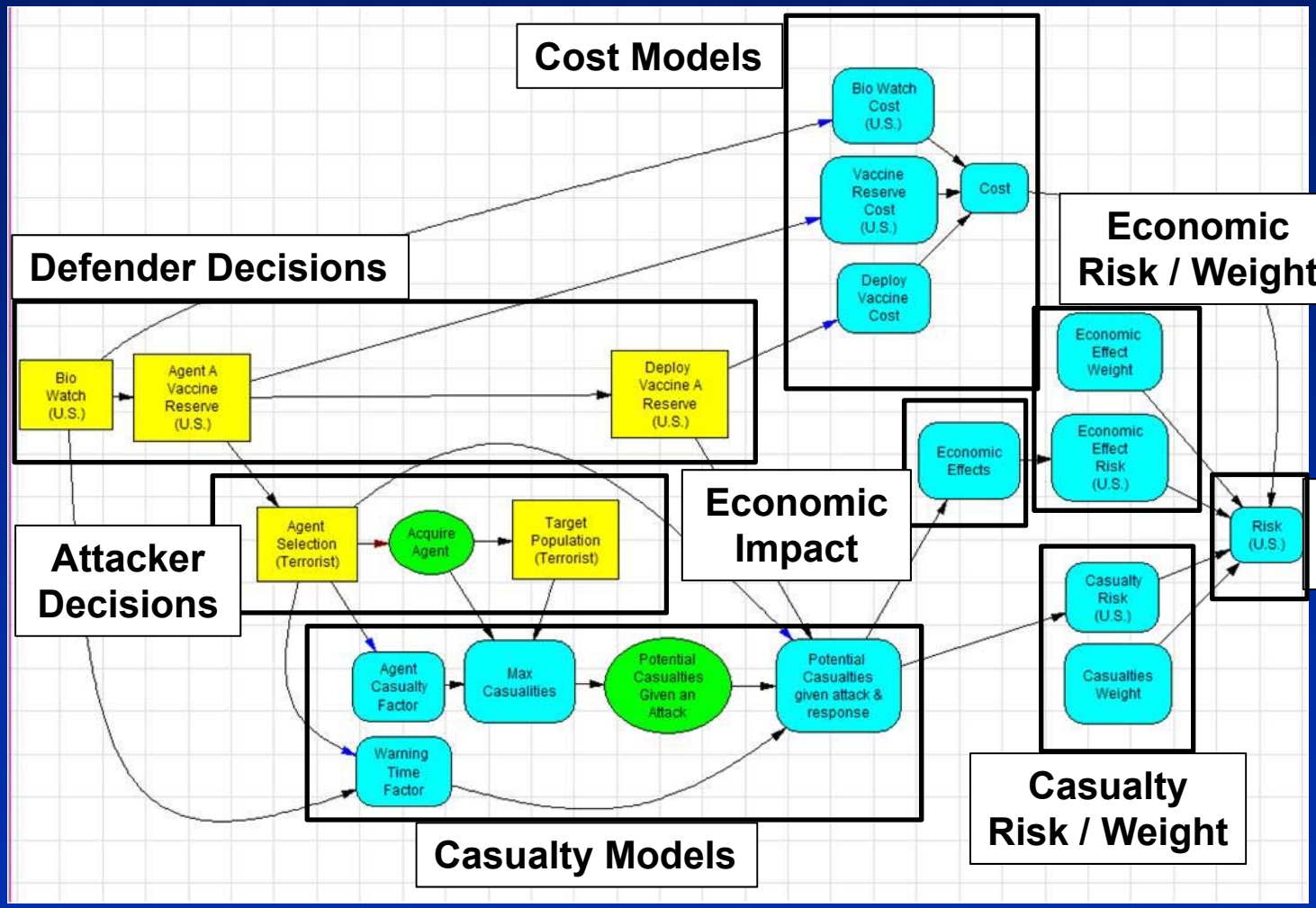
Defender-Attacker-Defender Decision Tree Model*



- Defender makes decisions to prepare for possible attacks
- Uncertainty is attacker's capability to attack
- Attacker decides to attack or not
- Uncertainty in defender ability to detect an attack
- Defender decides to mitigate the effects of the attack given detection
- Uncertainty in the potential causalities
- Defender wants to minimize risk and attacker wants to maximize risk

This concept is draws on Appendix D, Bioterrorism Risk Analysis with Decision Trees, G. Parnell, and Appendix E, Optimizing Department of Homeland Security Defense Investments: Applying Defender-Attacker (-Defender) Optimization to Terror Risk Assessment and Mitigation, Gerald G. Brown, W. Matthew Carlyle, R. Kevin Wood of Department of Homeland Security's Bioterrorism Risk Assessment: A Call for Change, Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis, National Research Council of the National Academies, 2008, The National Academy Press, Washington, DC

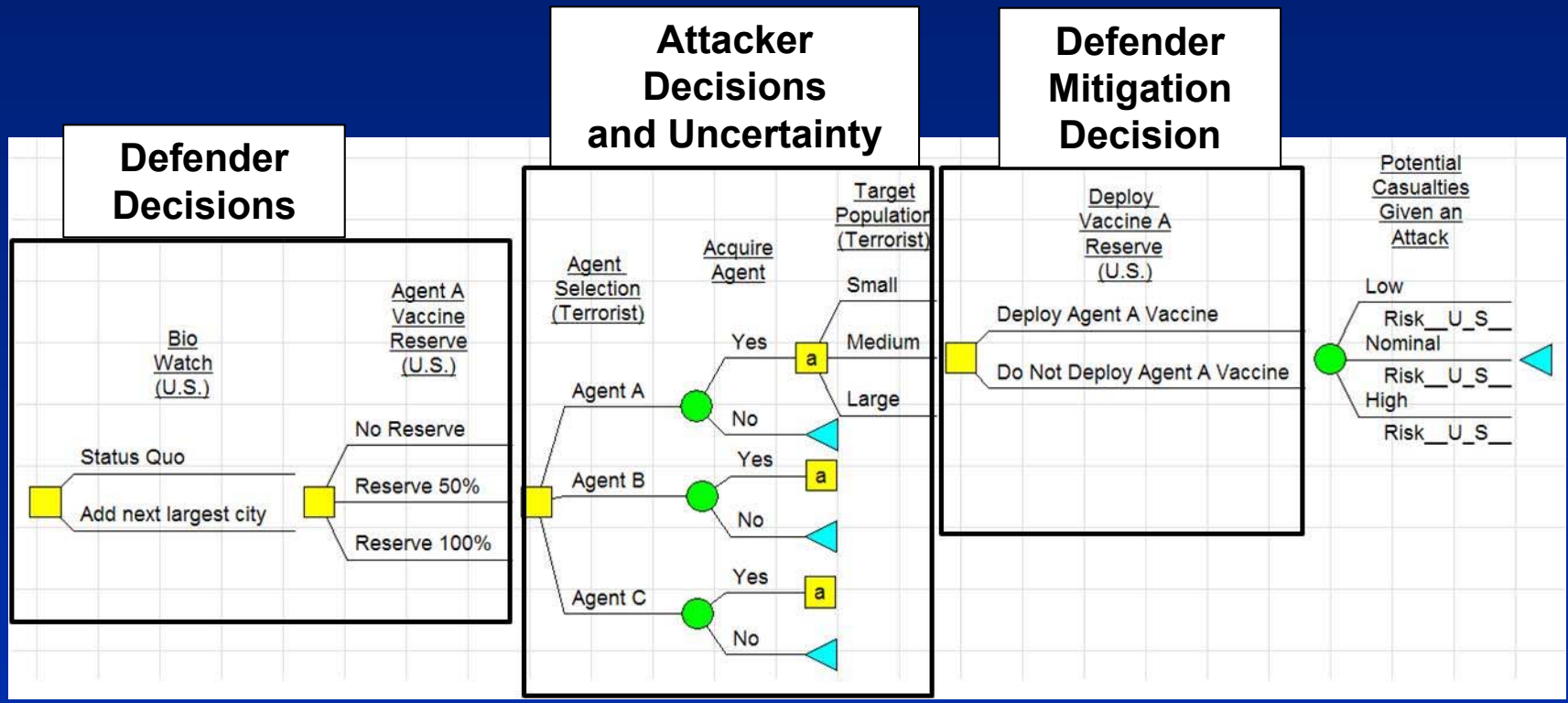
Canonical Bioterrorism Defender-Attacker-Defender Influence Diagram Model



Modeled using DPL 7.0 Software from Syncopation Software.
http://www.syncopationsoftware.com

Parnell, G.S., Smith, C. M., Moxley, F. I., Intelligent Adversary Risk Analysis: A Bioterrorism Risk Management Model, Submitted to *Risk Analysis*, February 20, 2009

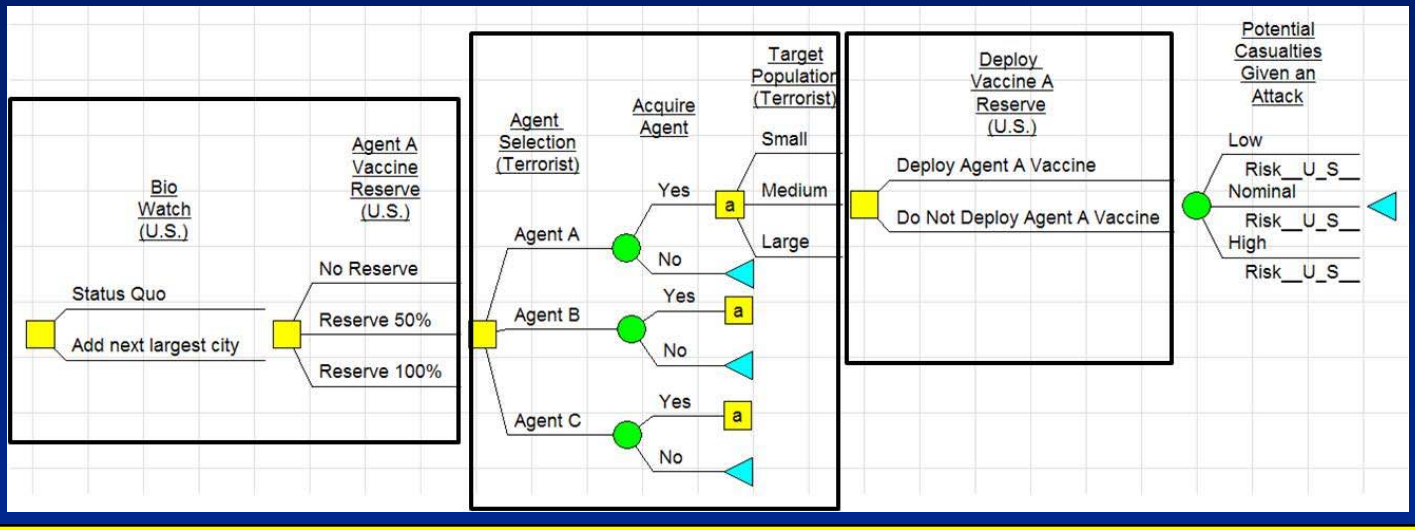
Components of Canonical Bioterrorism Defender-Attacker-Defender Decision Tree Model



Modeled using DPL 7.0 Software from Syncopation Software. http://www.syncopationsoftware.com

Parnell, G.S., Smith, C. M., Moxley, F. I., Intelligent Adversary Risk Analysis: A Bioterrorism Risk Management Model, Submitted to *Risk Analysis*, February 20, 2009

Defender-Attacker-Defender solution algorithm



$$\min_{w}\left(\min_{v}\left(\max_{a}\left(\sum_{a}\text{Prob}(ac_a)\times\max_{t}\left(\min_{d}\left(\sum_{ac}\text{Prob}(pc_{ac})\times r(x)\right)\right)\right)\right)\right)$$

- v = store vaccine A at percent {0%, 50%, 100%}
- a = agent {A, B, C}
- t = target populations {1k, 100k, 1m}
- d = deploy reserve vaccine {0,1}
- c = potential casualties {60%, 80%, 99%}

given agent chosen

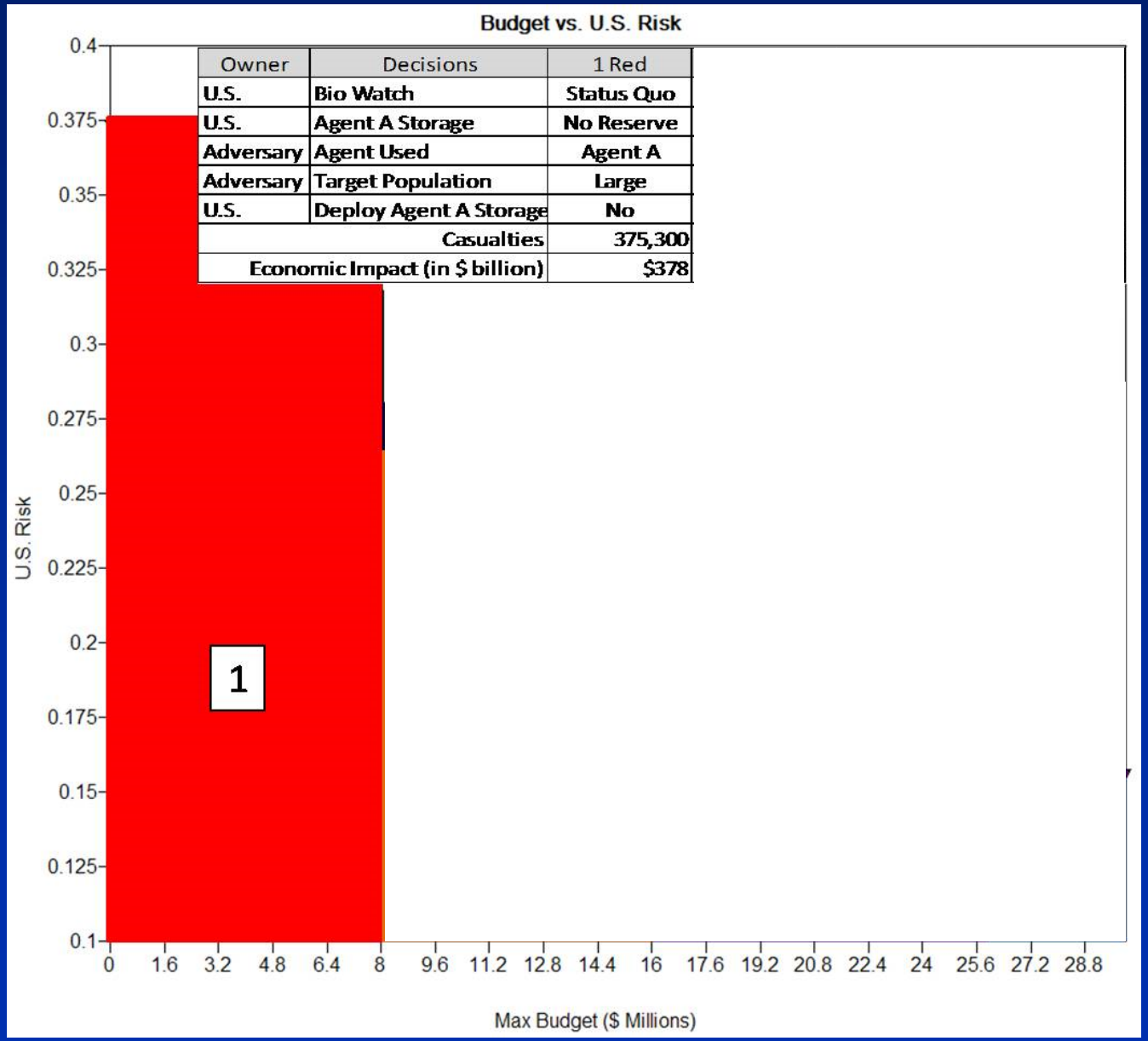
- Prob (pc_{ac}) = probability of casualties given agent chosen

Defender Risk

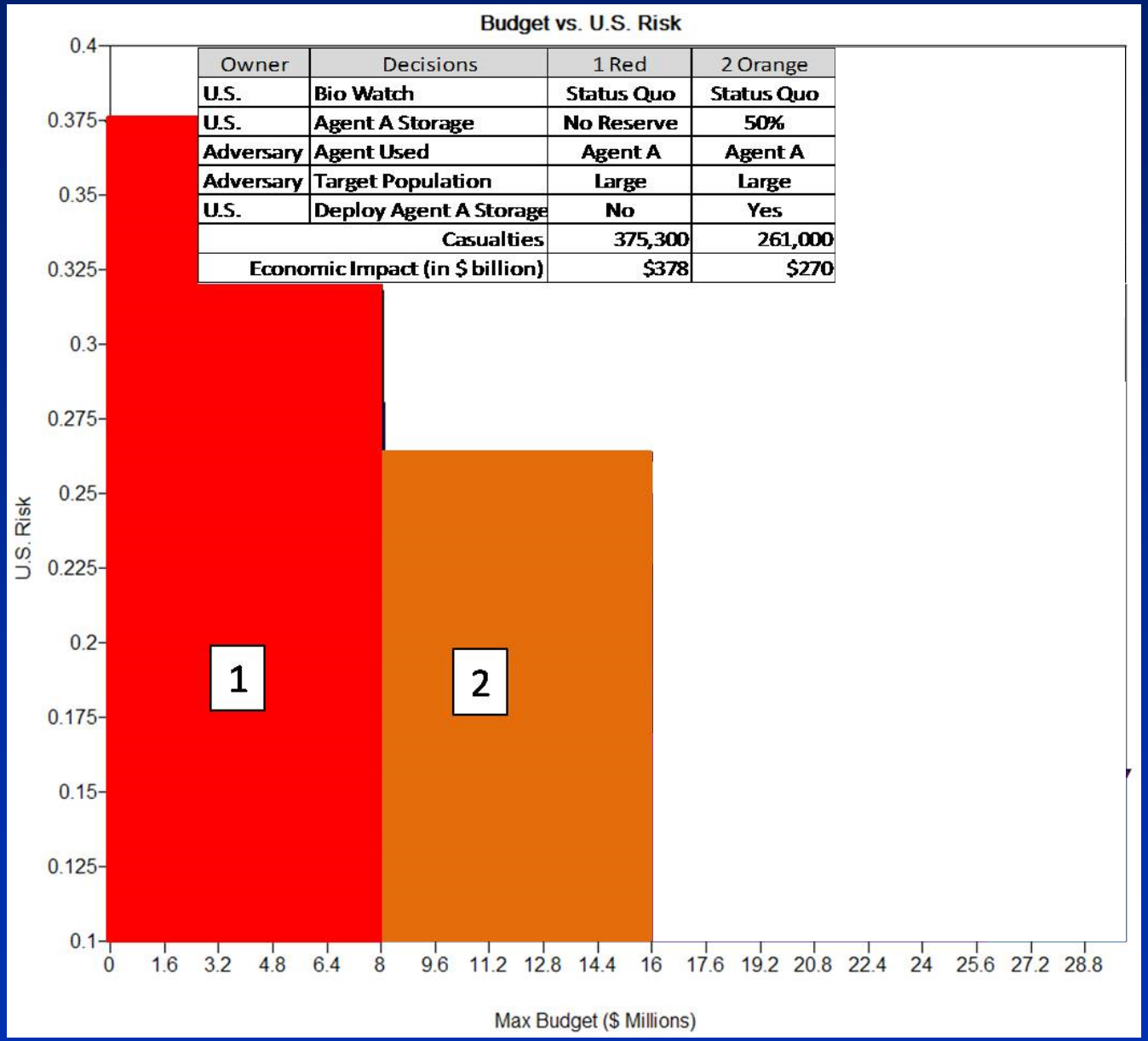
- r(x) includes casualties and economic effects

The decision tree is solved for several budget levels.

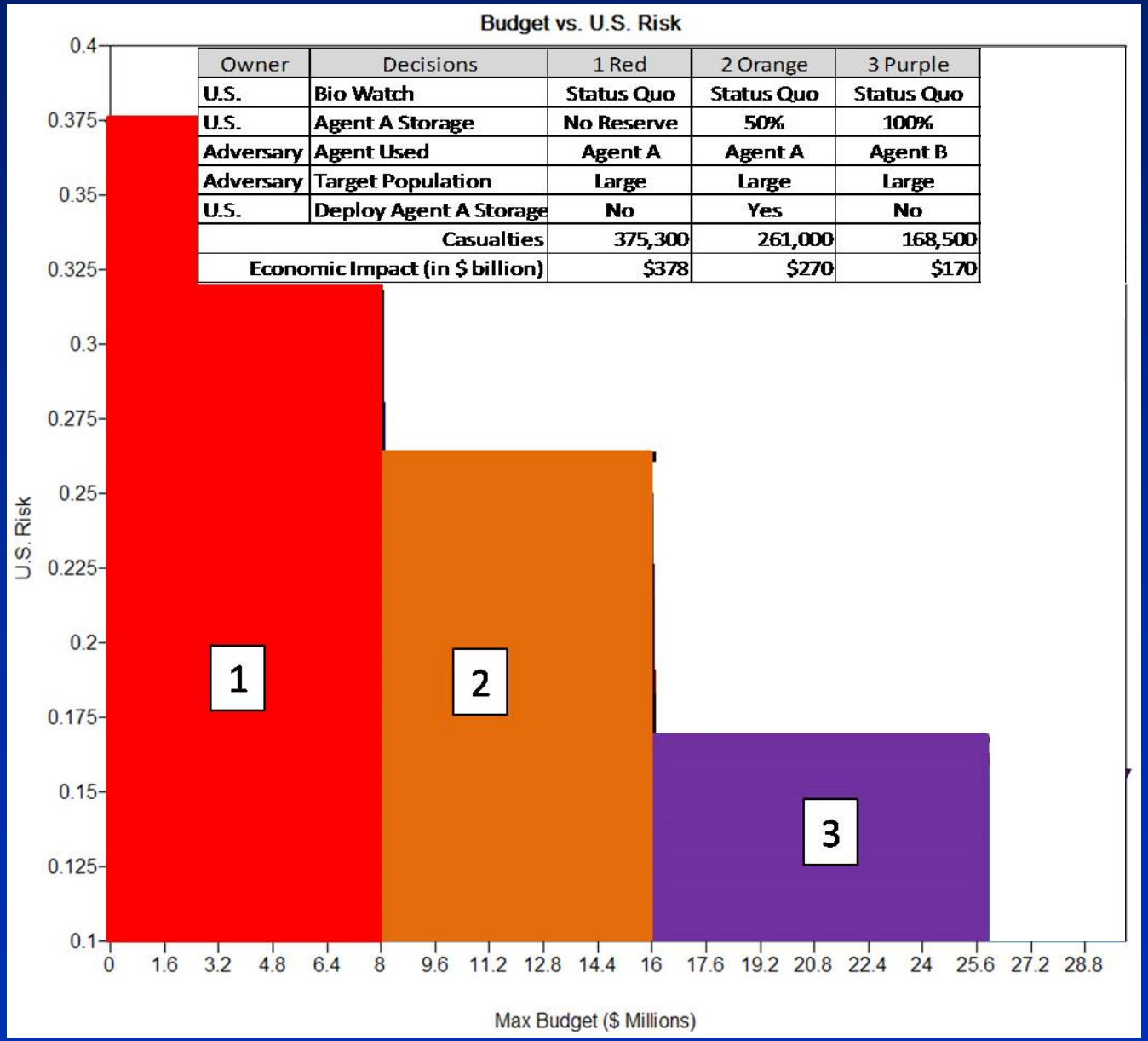
Plot of budget vs risk shows risk shifting. (Notional data)



Plot of budget vs risk shows risk shifting. (Notional data)

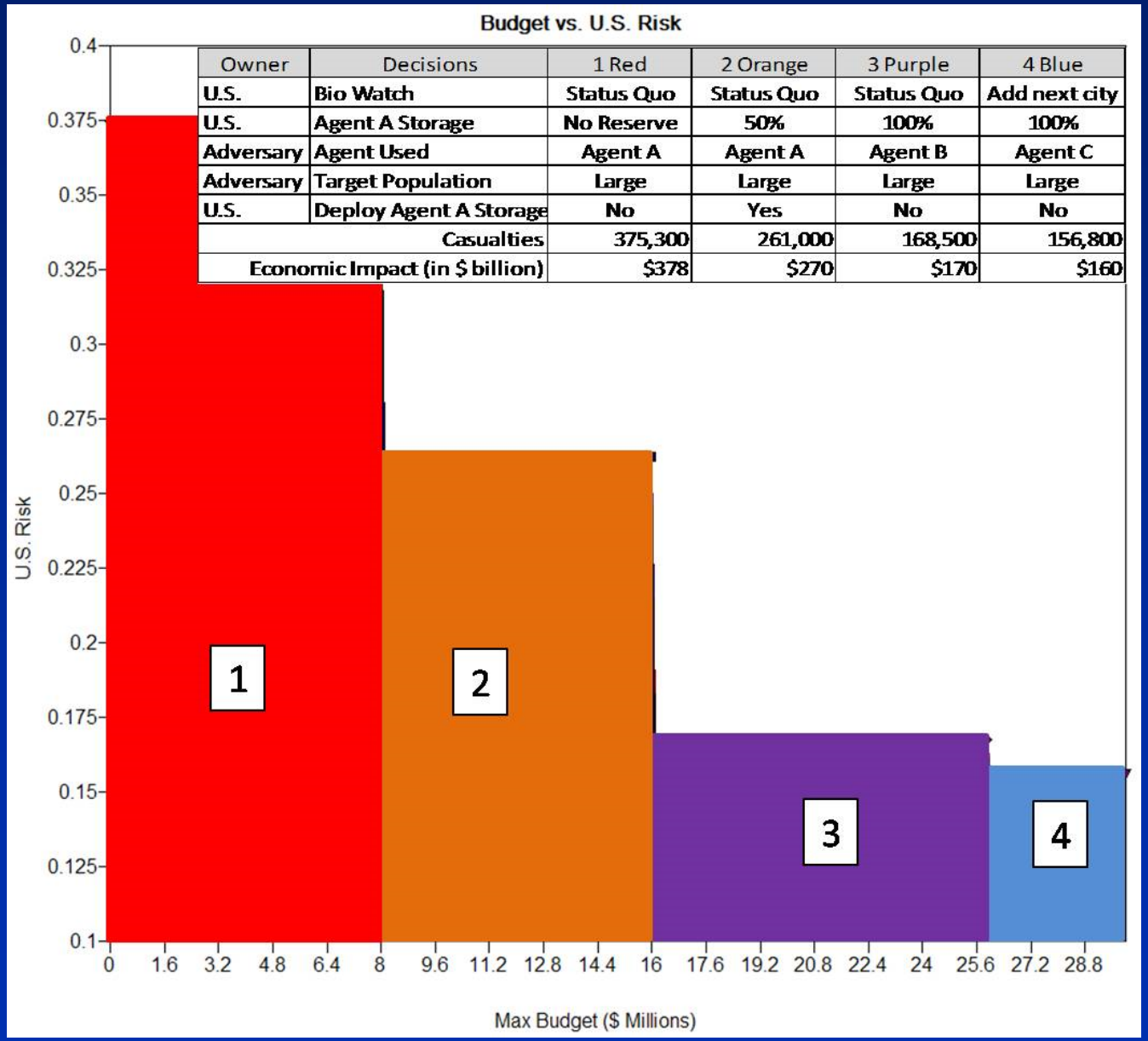


Plot of budget vs risk shows risk shifting. (Notional data)



Owner	Decisions	1 Red	2 Orange	3 Purple
U.S.	Bio Watch	Status Quo	Status Quo	Status Quo
U.S.	Agent A Storage	No Reserve	50%	100%
Adversary	Agent Used	Agent A	Agent A	Agent B
Adversary	Target Population	Large	Large	Large
U.S.	Deploy Agent A Storage	No	Yes	No
	Casualties	375,300	261,000	168,500
	Economic Impact (in $ billion)	$378	$270	$170

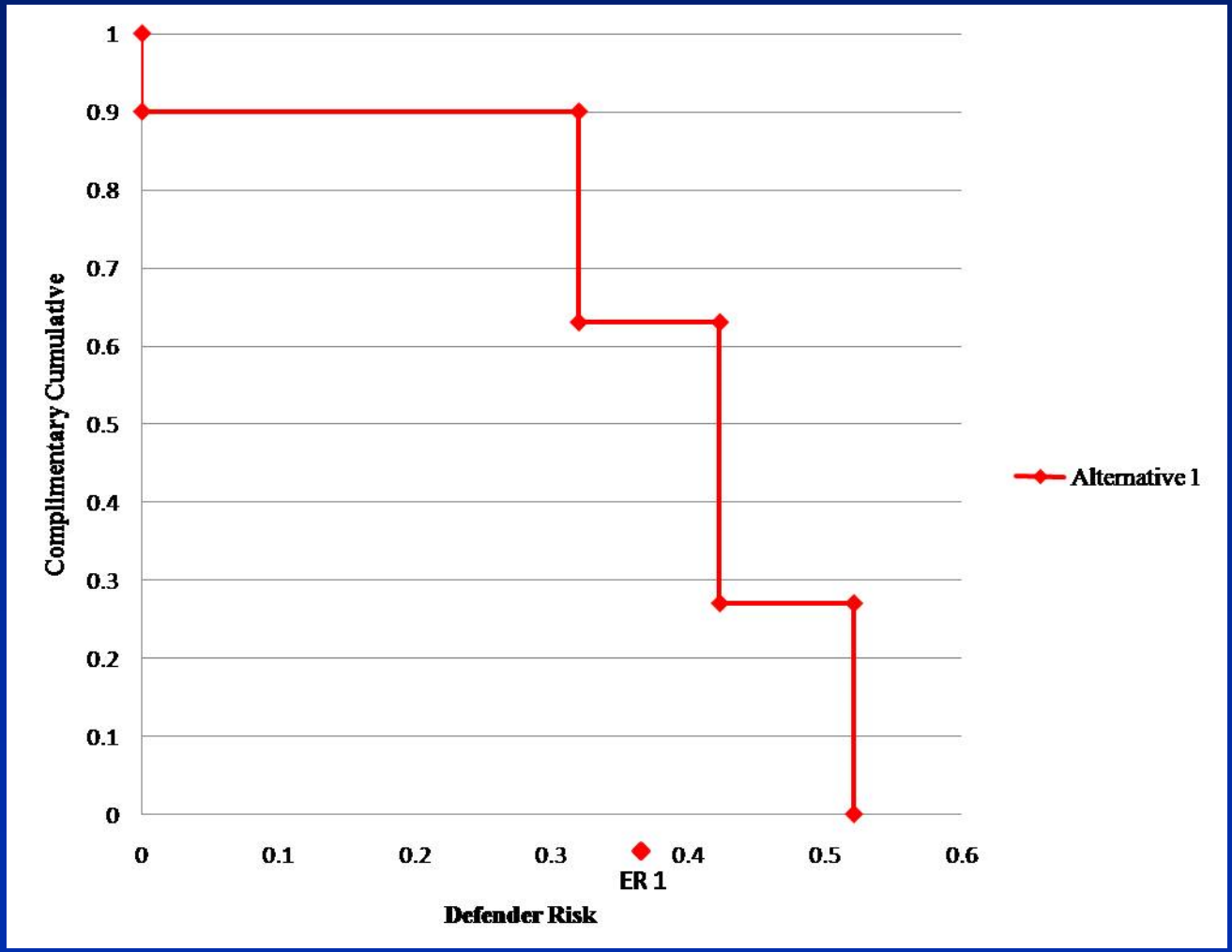
Plot of budget vs risk shows risk shifting. (Notional data)



Owner	Decisions	1 Red	2 Orange	3 Purple	4 Blue
U.S.	Bio Watch	Status Quo	Status Quo	Status Quo	Add next city
U.S.	Agent A Storage	No Reserve	50%	100%	100%
Adversary	Agent Used	Agent A	Agent A	Agent B	Agent C
Adversary	Target Population	Large	Large	Large	Large
U.S.	Deploy Agent A Storage	No	Yes	No	No
	Casualties	375,300	261,000	168,500	156,800
	Economic Impact (in $ billion)	$378	$270	$170	$160

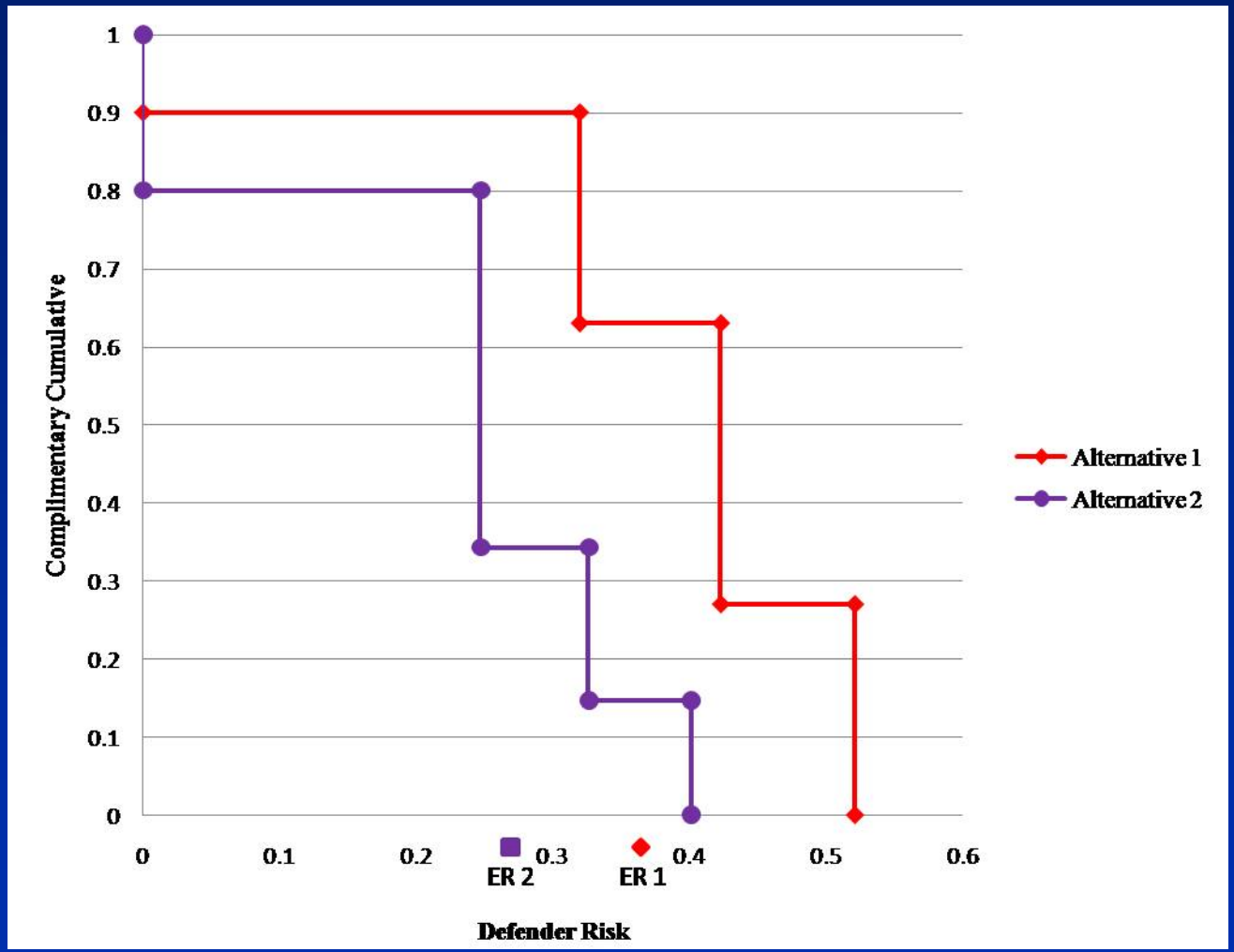
Complementary cumulative shows highest risk agent for a budget level. (Notional data)

- Displays the probability of each risk level for the defender's best decision at the a given budget level
- Expected risk noted at bottom of graph



Alternative 2 stochastically dominates alternative 1.

- Stochastic dominance when one alternative's risk is less than another alternative at every level of cumulative probability

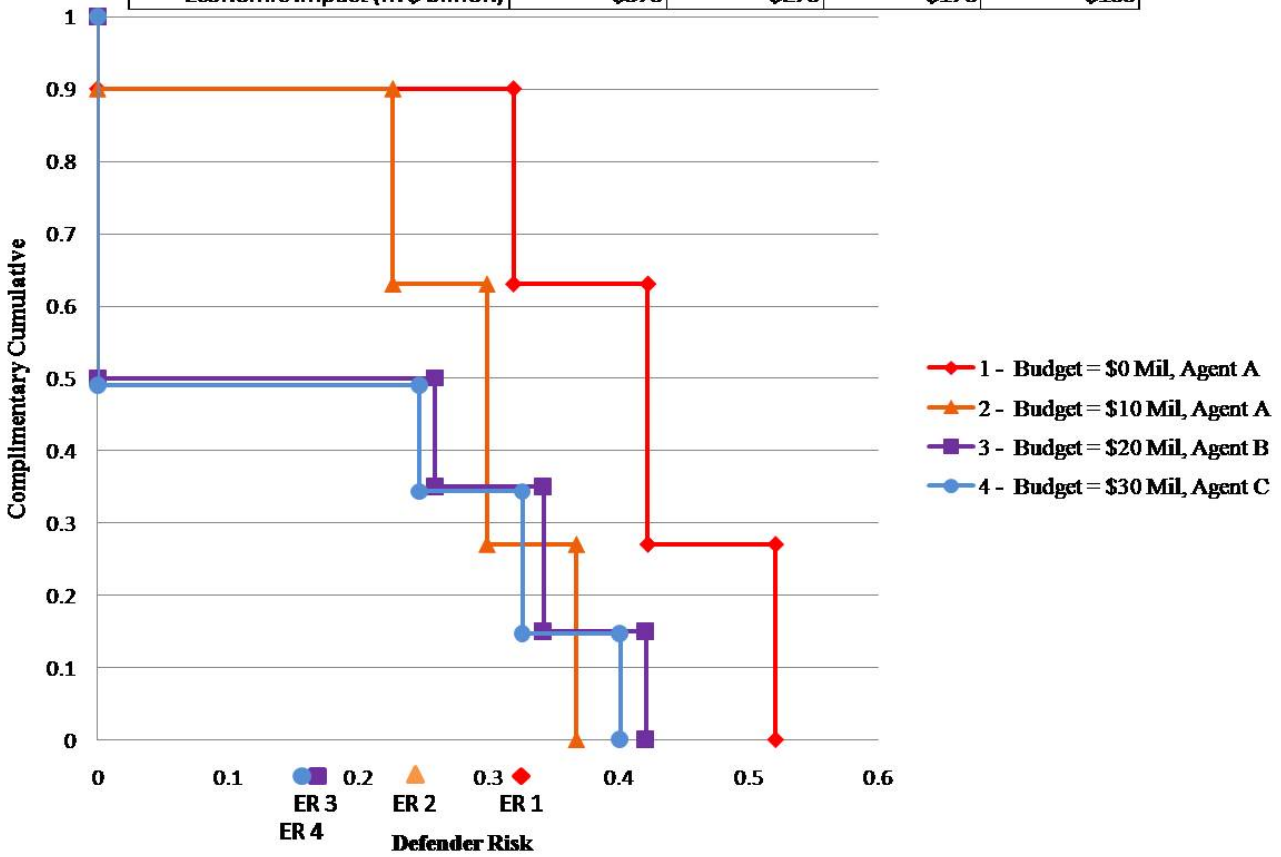


Notional data

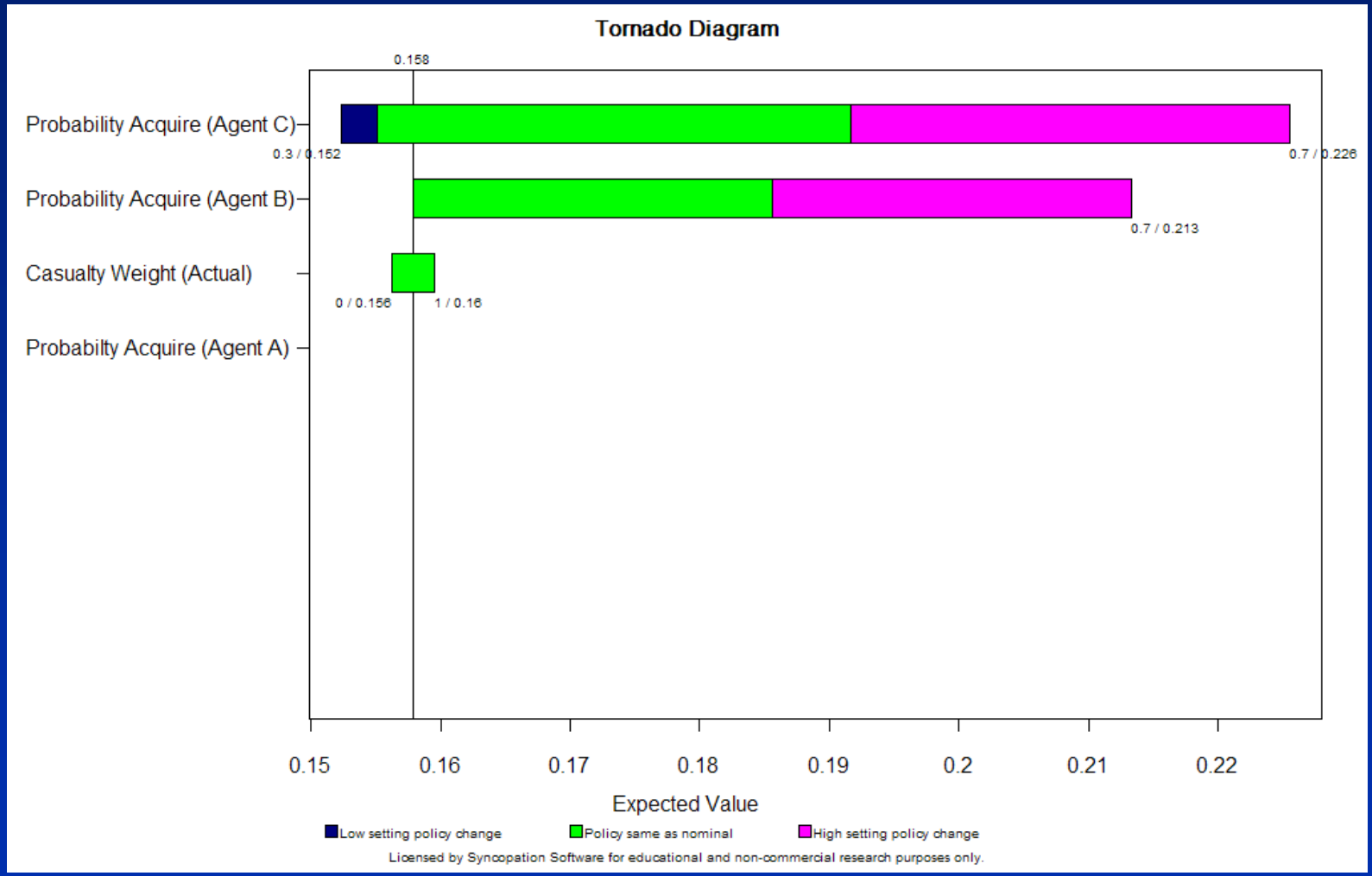
Complementary cumulative shows risk levels vs budget. (Notional data)

- Our model's complimentary cumulative curve for the different budget levels
- $10 mil budget stochastically dominates $0 mil (expected)
- Not much reduction in risk between $20 mil and $30 mil

Owner	Decisions	1 Red	2 Orange	3 Purple	4 Blue
U.S.	Bio Watch	Status Quo	Status Quo	Status Quo	Add next city
U.S.	Agent A Storage	No Reserve	50%	100%	100%
Adversary	Agent Used	Agent A	Agent A	Agent B	Agent C
Adversary	Target Population	Large	Large	Large	Large
U.S.	Deploy Agent A Storage	No	Yes	No	No
	Casualties	375,300	261,000	168,500	156,800
	Economic Impact (in $ billion)	$378	$270	$170	$160



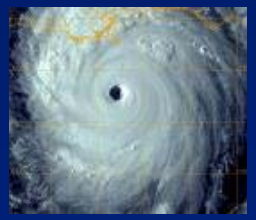
The tornado diagram shows the sensitivity to model assumptions.



Benefits of defender-attacker-defender PRA model using decision trees

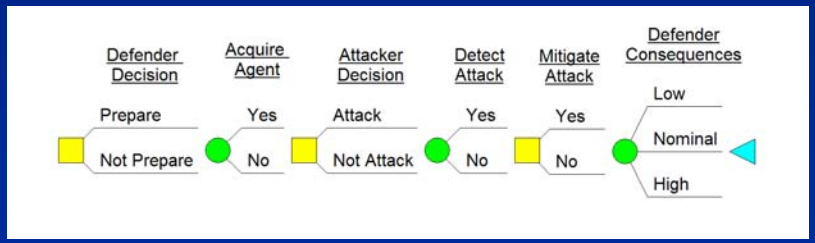
- Provides a more accurate risk assessment
  - Models intelligent adversary decision making
- Supports risk management
  - Provides tool for resource allocation for risk-informed decisions
- Enables flexible COTS software modeling environment
  - No probability assessment of attacker or defender decisions
  - Simplifies the DHS model
  - Availability of sensitivity analysis tools
- Can be run by one risk analyst
  - Understands decision analysis and optimization

Conclusions



- Intelligent adversary risk analysis is fundamentally different than natural and engineering hazard risk analysis

- Defender-attacker-defenders models capture the fundamental structure of the intelligent adversary risk analysis using probabilistic risk analysis



- Decision trees implemented in COTS software can model the defender-attacker-defender structure and provide a risk management tool (Bioterrorism risk analysis using notional data)