Game-Theoretic and Reliability Methods for Counterterrorism and Security

Vicki Bier

University of Wisconsin-Madison

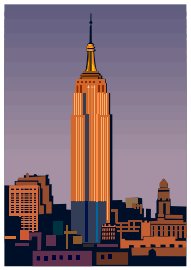
Background and Motivation

- Homeland-security funding is widely criticized:
  - "States like Wyoming…get more per capita in terrorism grants than New York"
  - "At the end of the day, blowing off New York and L.A. so that you can make sure Wyoming is safe just makes no sense" (Flynn)
- An official from one rural county stated:
  - "We're getting stuff we won't use. This equipment could have gone to Seattle"

Background and Motivation

- Skewed funding priorities of this type were widespread:
  - Federal formula “guaranteed each state 0.75% of the total amount appropriated to DHS”
  - “Many States [provided] a base amount to each county”
- Zycher uses the concept of “efficient” pork to describe situations in which such subsidies are necessary:
  - But 0.75% “is larger than most minimum amounts found in existing federal grant programs” (Brunet)

Icons



More Icons

More Icons

Alltel Stadium

Brewery

Churchill Downs

Gateway Arch

Offut AFB

“New York, You're Still No. 1”

- “…contrary to news media reports, significant landmarks like the Empire State Building and the Brooklyn Bridge were included in our deliberation over where money would go.
- “It is true that they were not classified as national monuments and icons.
  - “Why? To help New York's application.”

“New York, You're Still No. 1”

- “We purposely placed these structures into other categories:
  - the Empire State Building into the large office building category
  - and the Brooklyn Bridge into the bridges category.
- “We did so because those categories generate a higher complete risk grade for New York's financing proposal than icons like Mount Rushmore that, while important symbolically, would have fewer human and economic consequences in case of an attack.”

“New York, You're Still No. 1”

- “…the Homeland Security Department has made every effort to rely on measurable facts and to take politics out of the process.
- “State and local emergency management agencies — including those in New York — selected more than 100 local homeland security directors, fire chiefs, law enforcement officials and other experts to serve as peer reviewers of applicant-proposed solutions.”

“New York, You're Still No. 1”

- "When surveyed, 96 percent of the local and state agencies agreed that the panels that made the spending decisions included balanced representation, and 83 percent agreed that the peer review resulted in objective scores and results.”

Urban Area Security Initiative

- The Urban Area Security Initiative was initially intended to address this type of problem
- But the list of cities receiving funding grew from seven to 80:
  - Eventually scaled back to 28

Urban Areas Security Initiative

- Considers three primary variables:
  - Consequence,
  - Vulnerability, and
  - Threat

Urban Areas Security Initiative

- Also considers factors such as:
  - International borders
  - Population and population density
  - Location of critical infrastructure
  - Formal mutual aid cooperation
  - Law enforcement investigations and enforcement

What Is Risk-Based Preparedness?

- At a minimum, it should take into account attacker behavior
- Intelligent and adaptable adversaries may adopt different strategies to circumvent or destroy our protective measures:
  - Game theory provides a way of accounting for this

Game theory

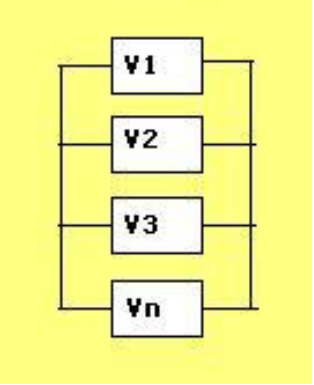
- Determine the optimal defense against an optimal attack
- Game theory is useful for security and infrastructure protection:
  - Appropriate when protecting against intelligent and adaptable adversaries
  - Recognizes that defensive strategies must account for attacker behavior

Overall goal

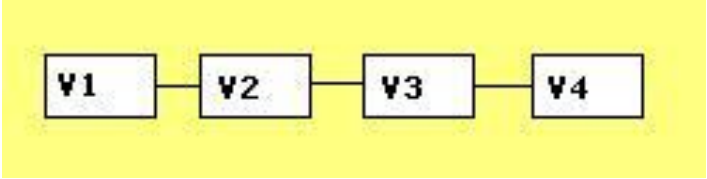
- Study optimal allocation of resources for protection of reliability systems against intentional attacks:
  - Security as a game between an attacker and a defender
  - Security as a game between defenders

Systems vs. individual assets

- **Parallel systems:**
  - Any component can perform the function
  - Attacker must disable all to succeed



- **Series systems:**
  - Attacker has a wide choice of targets
  - Defender must protect all components!



- Physically in series (pipelines, electric lines)
- Multiple failure modes (e.g., multiple points of entry to a secure facility)

Advantages

- Defending against an *optimal* attack can be *conservative*
  - In the sense of “cautious” or “prudent”
- Even if we don’t know what the adversary will do

What Is Risk-Based Preparedness?

- More realistically:
  - Real-world decision makers will want to hedge their bets
- Nobody would recommend that the U.S. invest only in defense from smallpox:
  - No matter how devastating smallpox might be
- So, a realistic method must account for uncertainty about attacker goals and motivations!

What Is Risk-Based Preparedness?

- Moreover, defenders may not have the same valuations for targets as attackers
- The value of a given target to an attacker may depend on factors such as:
  - The propaganda value of the target
  - The cost or difficulty of the attack
- Risk-based investment in preparedness must take such considerations into account too!
- Recent work addresses these considerations

Assumed Attacker Behavior

- If attackers are assumed to choose targets based on the expected value of an attack:
  - Undefended locations may not be attacked
  - It depends on the attacker's preferences!
- If the defender increases the resources allocated to one location:
  - It becomes more likely that the attacker will target some other location

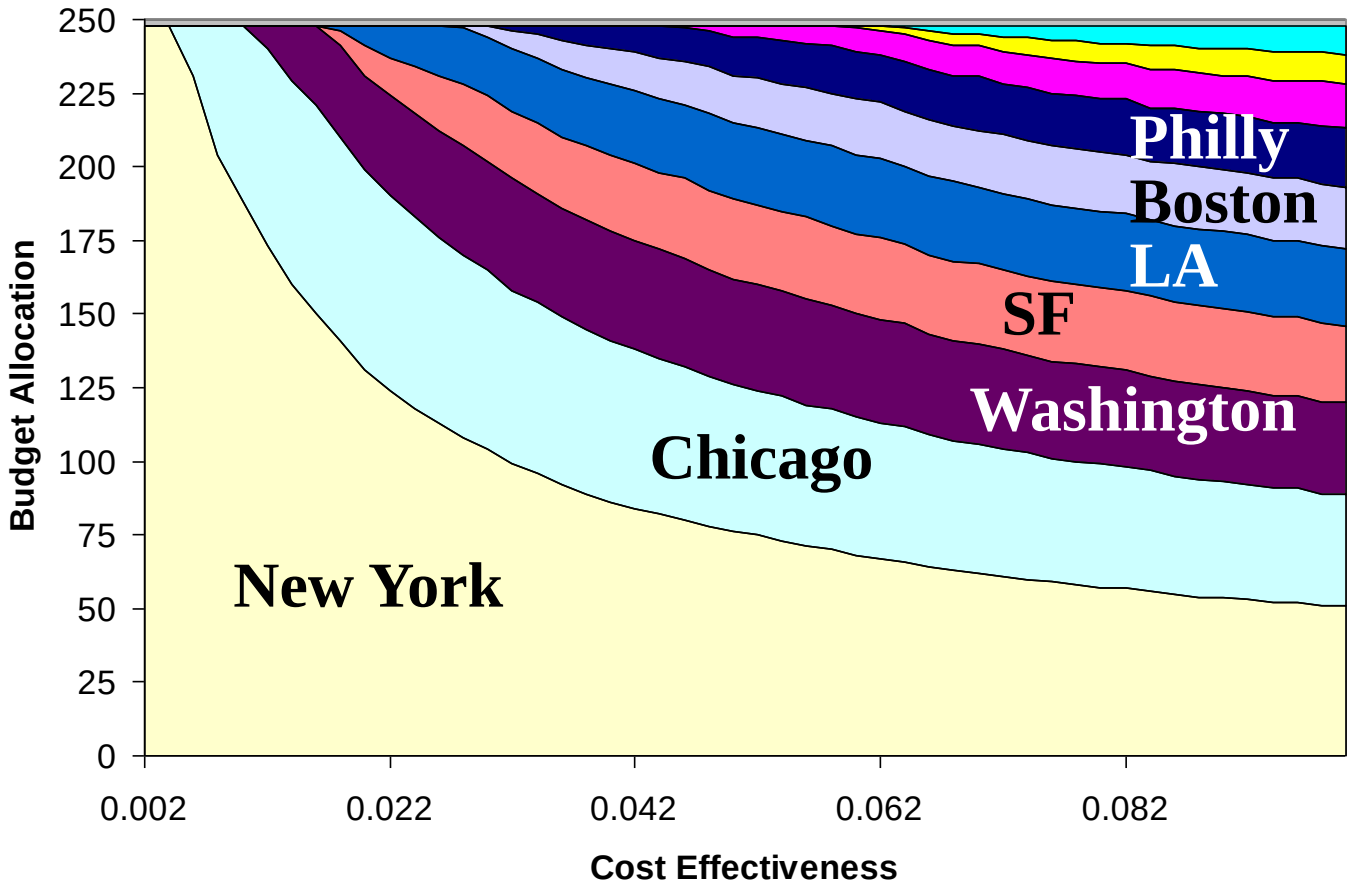
Summary of Results

- If the values of the targets are sufficiently different, low-value targets may be unlikely to be attacked:
  - Defenses should be allocated only to valuable targets
  - Even in the face of significant uncertainty!
- It can be optimal to leave some targets undefended, particularly when:
  - The defender is highly budget constrained
  - The values of the targets differ widely
- This is exactly the situation in the real world!

Summary of Results

- The weakest-link hypothesis does not always hold!
  - Attacker preferences are relevant
- Some highly vulnerable targets may be left largely undefended:
  - If they are of little interest to attackers

Sample Results for 10 UASI Cities



Caveats

- These results are based on the assumption that the defender wants to minimize expected property losses (as estimated by Rand):
  - And the attacker preferences are based on expected property losses plus an “error term”
- Other objective functions (e.g., fatalities, infrastructure damage) would lead to slightly different resource allocations

Caveats

- Even if some cities get zero resources in a city-level analysis:
  - They may still have targets worth defending in a target-level analysis
- This is consistent with 2015 UASI allocations:
  - Ten of the highest-risk jurisdictions received 85% of the funds
  - The remaining UASI areas compete for the remaining 15% of the funds

Interpretation of Results

- Optimal investment strategies depend critically on cost effectiveness of investment:
  - High cost effectiveness allows the defender to spend more on defense of less valuable targets
  - At low cost effectiveness, the defender has to devote most resources to the more valuable targets
- However, we currently do not have a good way to measure the cost effectiveness of our investment!

Decentralization

- With decentralized decision making:
  - Some targets receive too many resources
- For instance:
  - Security measures by the Postal Service may deflect risk onto private carriers
  - Measures to make aviation more secure may deflect risk onto other modes of transportation
- Greater coordination would be preferred!

Decentralization

- Even decisions by a single agency may look decentralized:
  - "Officials [of small cities and states] talk about… the right of their citizens to get the same kind of protection that they are afforded in other places"
  - "A Congressman from Wyoming has no incentive [for] admitting that his state is not a likely target or that…the level of damages would be limited"

Large Numbers of Targets

- It is a hopeless task to defend large numbers of individual targets
- It is optimal to invest in security only if investment can be focused on a relatively small number of targets:
  - And the remainder are relatively unlikely to be attacked

Large Numbers of Targets

- The difficulty of defending extremely large numbers of assets also suggests that psychological factors may play an important role
- If the public demands protection against any possible terrorist attack:
  - Then security investment may have harm the economy
- A successful defense strategy may need to reshape public perceptions:
  - To focus defensive resources on the most serious risks

Conclusions

- When facing the threat of an intentional attack:
  - It is important to model the behavior of the attacker
- For example:
  - Concentrating on transportation security may be effective if the attacker continues to concentrate on transportation, but of little use if the attacker switches to the food supply
  - Pre-screening containers from ports shipping 80% of the containers might enhance security if attackers do not alter which ports they use, but be of little use if attackers shift to ports shipping the remaining 20%

Conclusions

- Making security funding more risk-based is difficult
- In particular, an effective terrorism defense must involve:
  - Hard choices about what not to defend,
  - Overarching protections (like border security), or
  - Changes in the incentives faced by potential terrorists
- This creates some grand challenges for security research

What are some challenging future research directions?

In the spirit of looking where we lost our keys,

Not under the lamppost!

Reframe the Problem

- **Overarching protections:**
  - **Border security**
  - **Public health**
  - **Emergency response**
  - **Intelligence**
- **Reducing terrorist recruitment:**
  - **Bruce Hoffman (Rand Corporation)**
- **New ways of thinking about security**

Terrorist Objectives

- Current models tend to be textbook or story problems
- This diminishes their realism, and also their credibility
- A couple of exceptions include:
  - Beitel et al. (Idaho National Engineering and Environmental Laboratory)
  - Richard John (CREATE)

Carrots versus Sticks

- **Current models fail to distinguish carrots from sticks**
- **At the start of the Cold War:**
  - **We were unsure of how to think about deterrence of nuclear war**
- **Results led to a Nobel prize!**
- **We are currently in the same situation with respect to terrorism**

Intelligence Community

- **We need better bridges to the intelligence experts:**
  - **More credible terrorist objective functions**
  - **More credible risk analyses**
  - **Less weight on consensus**
  - **Ways of using risk and decision analysis to inform intelligence judgments**

Acknowledgments

- **Supported in part by:**
  - **Department of Homeland Security under grant number N00014-05-0630**
  - **And lots of great students, colleagues, and researchers (too numerous to mention)**

Acknowledgments

- **Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author:**
  - **And do not necessarily reflect the views of the sponsors or others**