PNNL-SA-130285

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

A Mathematical Methodology for Optimized, Risk-Informed Deployment of Security Countermeasures

Concealed Explosives Detection Workshop

Sarah Reehl, Robert Brigantic, and Angela Waterworth

8 November 2017

Charlottesville, VA

U.S. DEPARTMENT OF ENERGY

Abstract

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

In the security and protection of venues such as mass transit, critical infrastructure, and largescale public events, there are typically constraints or limitations to the allocation of sensors and security assets; the challenge is how to best deploy them over time to minimize risk to the venue of interest. In this presentation, we describe a mathematical methodology to formulate the risk of various threats into quantifiable subcomponents and optimize the deployment of limited security assets and countermeasures over time. This model determines the mathematically optimal strategy to ensure intelligent, risk-informed deployment of security countermeasures based on their effectiveness in mitigating threats. This presentation will focus on the early formulation and development of the Airport Risk Assessment Model (ARAM), which is currently in development for operationalization at the Seattle-Tacoma (Sea-Tac) International Airport. The method starts by decomposing risk into three core, quantifiable components: consequence, vulnerability, and threat. These subcomponents are evaluated for the given venue and potential security threats. We then assesses the effectiveness of security assets and countermeasures used to counter the security threats. A novel aspect of this methodology is quantifying these risk components as a continuous function of time. Finally, we formulate a mathematical program to determine the optimal allocation of these constrained resources to minimize the overall risk.

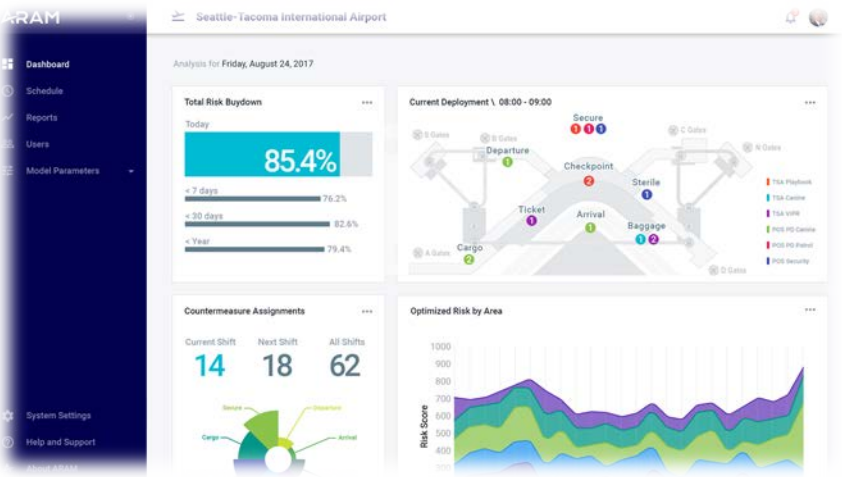
Imagine

- ... a future where:
  - quantified and apportioned **risk** is dominant driver to determine where, and when deployable countermeasures are assigned to minimize overall risk
  - this is in stark contrast to current way of doing business where risk is not quantified nor typically used to make risk informed decisions
  - rather, today assignment of deployable countermeasures is often done by gut feel, ad hoc, or reaction to other events

ARAM

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

This future is within grasp and is already being implemented as an operational risk-based, intel-driven decision platform to assess and quantify terrorism risk at Sea-Tac



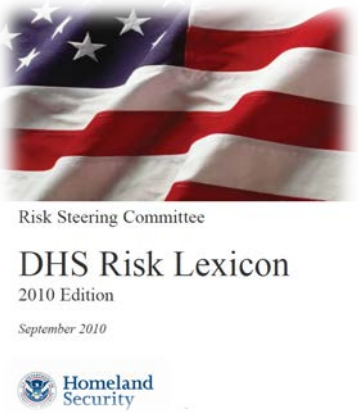
Risk Methodology

- Founded on core DHS risk doctrine and fundamental principles
- Integrates disparate information and data sources (e.g., flight schedules, passenger and airport volume, intelligence information, etc.)
- Provides an automated, end-user tool that recommends the optimal allocation of deployable countermeasures on an hourly basis for any day of the year

Notional values

Threat	Effectiveness	Deterrence	Effectiveness	Deterrence	Effectiveness	Deterrence
VBIED	6	7	6	9	9	9
PBIED	5	8	9	8	9	9
Active Shooter	4	4	2	7	3	6
Chem/Bio	2	2	2	4	1	5
Workers with Access	6	5	4	6	5	2

Risk modeling considers the effectiveness and deterrence capabilities of different countermeasures in doing the math



Agenda

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Purpose
- Definitions and risk analysis introduction
- Risk analysis methodology
- Notional example
- Questions

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

From: Commander-in-Chief, United States Pacific Fleet

To: Commander Striking Force (Operation Plan 29-42)

Subject: Letter of Instruction

"In carrying out the task assigned in Operation Plan 29-42 you will be governed by the principle of calculated risk …"

Admiral C.W. Nimitz
May 28, 1942

Purpose

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Quantify national security risk and the effectiveness of different security assets so that they can be optimally deployed to minimize this risk over time

Definitions and Risk Analysis Introduction

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- *Risk*: potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences
- *Risk Analysis*: systematic examination of the components and characteristics of risk
- *Risk Score*: numerical representation that gauges the combination of ***threat***, ***vulnerability***, and ***consequence*** at a specific moment
- Basic risk equation:

$$R = f(C, V, T)$$

How much impact? How hard? How likely?

Risk Steering Committee

DHS Risk Lexicon
2010 Edition

September 2010

Homeland Security

Note: risk score is a dimensionless quantity, and therefore, it is most useful to compare the relative risk of different threats and the benefits of different mitigation options

Risk Analysis Methodology

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Given basic risk equation, how can we quantify risk from different threats and assess holistic risk to the airport of interest over time?
  - The method starts by decomposing the three core components of risk into their various subcomponents
  - Then each of these components can be evaluated against the given airport and potential threats of interest as a function of time
- Various methods can be used to decompose risk components into subcomponents, we will use those found in the *Port Security Risk Assessment Tool User Manual*

Risk Subcomponents

PSRAT PORT SECURITY RISK ASSESSMENT TOOL USER MANUAL

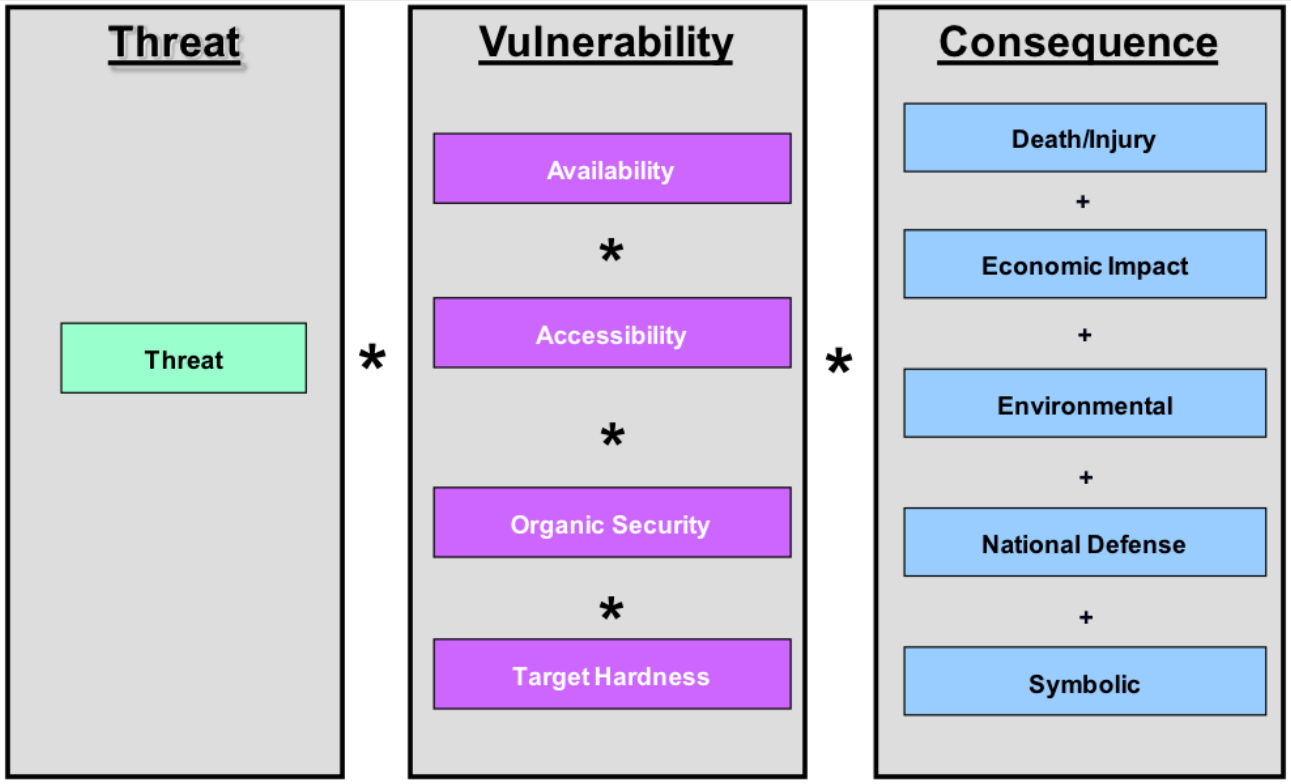


Figure 12 - PSRAT Risk Factors

Consequence

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Composed of following elements
  - Death and injury*
  - Economic impact
  - Environmental impact
  - National defense
  - Symbolic effect
  - Recoverability
  - Redundancy

First determine what consequence elements are pertinent for the airport of interest. Next, score each subcomponent for the threat being considered. Lastly, the overall consequence score is the sum of these subcomponent scores.

$$C = C_{\text{death/injury}} + C_{\text{economic}} + C_{\text{environment}} + C_{\text{defense}} + C_{\text{symbolic}} + C_{\text{recoverability}} + C_{\text{redundancy}}$$

***CONSEQUENCE**: effect of an event, incident, or occurrence*

* - Driven primarily by death/injury which can be tabulated as function of airport population as a function of time.

Vulnerability

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Composed of following elements
  - Availability
  - Accessibility
  - Organic security*
  - Target hardness

As with consequence, first determine what vulnerability elements are pertinent for the airport of interest. Next, score each subcomponent for the threat being considered. Lastly, the overall vulnerability score is the product of these subcomponent scores.

$$V = V_{\text{availability}} \times V_{\text{accessibility}} \times V_{\text{organic security}} \times V_{\text{target hardness}}$$

$$0 \leq V \leq 1$$

***VULNERABILITY**: physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard*

* - The other vulnerability elements are relatively fixed, but organic security can be flexed and optimized.

Threat

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Threat*: likelihood of threat against for the airport of interest
  - Vehicle borne improvised explosive device (VBIED)
  - Person borne improvised explosive device (PBIED)
  - Active shooter (AS)
  - Chemical or biological attack (Chem/Bio)
  - Workers with access (WWA)

First determine what threat elements are pertinent for the airport of interest. Next, score the threat being considered.

$$0 \leq T \leq 1$$

***THREAT**: natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property*

* - Can also consider deterrence effects that might reduce threat.

Holistic Risk for Airport of Interest

- Can further define risk components as a function of the type of threat (i) and specific areas (j) that that might be targeted at every hour (h) of the day for the airport of interest:

$$R_{i,j}(h) = C_{i,j}(h) \times V_{i,j}(h) \times T_{i,j}(h)$$

- Holistic hourly risk for the airport of interest:

$$\boldsymbol{R}(h) = \sum_{\forall\, i,j} R_{i,j}(h)$$

- Holistic daily risk for the airport of interest:

$$Daily\ Risk = \sum_{h=0}^{23} \boldsymbol{R}(h)$$

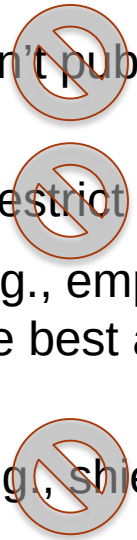
Now What?

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- The goal is to minimize holistic daily risk for the airport of interest
  - Can especially examine mitigations to reduce scores for the vulnerability subcomponents and threat

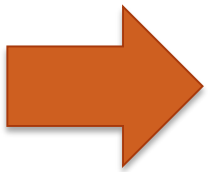
Vulnerability:

- Availability: e.g., don't publish schedule
- Accessibility: e.g., restrict access
- Organic security: e.g., employ more and determine best assets against threat
- Target hardness: e.g., shield everyone



Threat:

- Deterrence: e.g., visible security forces



Differentiate effectiveness and deterrence value of security assets (more later)

Notional Example

- Scenario:
  - Airport with 24x7 operations
  - Five areas to protect
  - Three potential threats
  - Four types of security assets
- Workflow proceeds as follows:
  - Score “baseline” consequence, vulnerability, and threat components for each area
  - Score effectiveness and deterrence value of security assets in countering each threat
  - Forecast changes to consequence as a function of time with increased/decreased volume on a given day
  - Input security asset availability for a given day
  - Produce optimal asset assignments for the day which minimizes risk

Notional Example – Score Consequence

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Threat

NOTE: Green (lower) is better - 5 point scale

Areas

Consequence Subcomponents

Security Area	Security Threat: 1						
	Death/Injury	Economic Impact	Environmental Impact	National Defense	Symbolic Effect	Recoverability	Redundancy
1	5	3	1	2	4	3	2
2	4	3	1	2	4	3	2
3	4	3	1	2	4	2	2
4	3	4	1	2	3	2	1
5	3	3	1	2	3	2	1

Security Area	Security Threat: 2						
	Death/Injury	Economic Impact	Environmental Impact	National Defense	Symbolic Effect	Recoverability	Redundancy
1	4	3	3	3	5	4	2
2	3	3	3	3	5	4	2
3	3	3	3	3	5	4	2
4	2	2	3	3	5	4	2
5	1	2	3	3	5	4	2

Security Area	Security Threat: 3						
	Death/Injury	Economic Impact	Environmental Impact	National Defense	Symbolic Effect	Recoverability	Redundancy
1	2	1	3	2	2	2	3
2	2	1	3	2	2	2	3
3	2	1	3	2	2	2	3
4	2	2	1	2	2	1	2
5	2	2	1	2	2	1	2

Notional Example – Score Vulnerability

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Threat

NOTE: Green (lower) is better - 5 point scale

Security Area	Security Threat: 1			
	Availability	Accessibility	Organic Security	Target Hardness
1	5	5	5	5
2	5	5	5	5
3	5	5	4	4
4	4	3	4	4
5	3	2	4	3

Areas

Vulnerability Subcomponents

Security Area	Security Threat: 1			
	Availability	Accessibility	Organic Security	Target Hardness
1	5	5	3	3
2	5	5	3	3
3	5	5	3	3
4	4	3	2	3
5	3	2	1	3

Security Area	Security Threat: 1			
	Availability	Accessibility	Organic Security	Target Hardness
1	5	5	1	2
2	5	5	1	2
3	5	5	1	1
4	4	3	1	1
5	3	2	1	1

Notional Example – Score Threat

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

NOTE: Green (lower) is better - 5 point scale

Security Area	Security Threat		
	1	2	3
1	4	2	5
2	3	2	1
3	3	2	1
4	2	2	3
5	1	3	3

Areas

Each threat has a different score for each area

Notional Example – Score Security Asset Effectiveness and Deterrence

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

NOTE: Green (higher) is better - 10 point scale

Security Threats

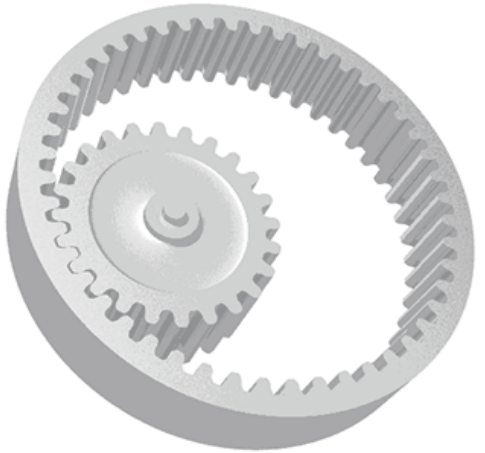
Security Threat	Security Asset Effectiveness			
	1	**2**	**3**	**4**
1	2	4	3	9
2	4	8	6	8
3	5	5	8	7

Each asset has a different effectiveness and deterrence score

Security Threat	Security Asset Deterrence			
	1	**2**	**3**	**4**
1	7	5	2	2
2	4	4	3	5
3	1	4	9	6

Notional Example – Computing Risk

- With assessment completed to score all the risk components and subcomponents, risk can now be computed
- Requires the following:
  - Consequence: each score turned into “points” and summed to determine total consequence score
  - Vulnerability: each score turned into 0-1 value and product of these determines total vulnerability score
  - Threat: each score turned into 0-1 value
  - Finally, risk for each threat type and each area is computed as product of *C*, *V*, and *T* components



Notional Example – What About Assets and Time?

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Consequence (death and injury subcomponent) reduced when less people are present at airport
- Vulnerability (organic security subcomponent) reduced through assessed effectiveness value of the assets
- Threat reduced through assessed deterrence value of the assets

Notional Example – What About Assets and Time? (cont'd)

- Of course each of the above vary with time (i.e., people present changes throughout the day, as do the number and types of assets available)
  - Unmitigated risk: risk throughout the day as it ebbs and flows with people in attendance at the airport with no countermeasures
  - Mitigated risk: risk after application of assets at different airport areas
  - Optimal mitigated risk: the minimum risk after optimizing asset assignments at the airport of interest
- With all of these pieces, the daily risk function can be optimized through a traditional **mathematical programming** (MP) formulation

Notional Example – What About Assets and Time? (cont'd)

- MP:
  - Decision variables: where and when to place assets
  - Objective function: Minimize *Daily Risk*
  - Constraints: asset availability and other imposed requirements

$$\min_{X_{ijk}^t} \sum_{k,l,t} R_{kl}^t = \sum_{k,l,t} S_{kl}^t \exp\left(\sum_{i,j} K_{li} X_{ijk}^t\right)$$

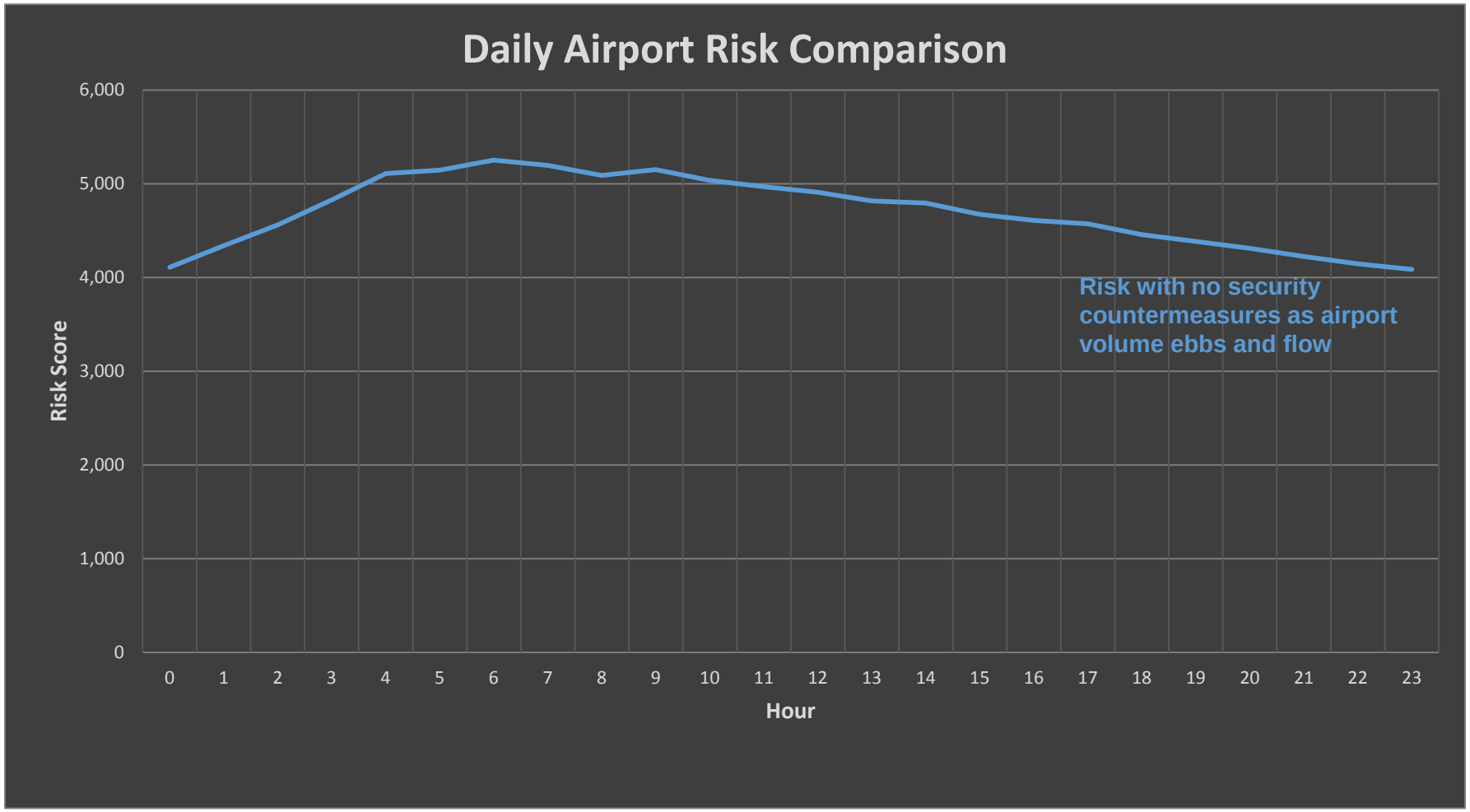
$$S_{kl}^t = \hat{C}_{kl}^t \hat{V}_{kl} \hat{T}_{kl} K_{li} = \ln E_{li} + \ln D_{li}$$

$$\sum_k X_{ijk}^t \leq a_{ij}^t, \ \forall\, i,j \in J(I), t$$

$$X_{ijk}^t \in \{0,1\}, \ \forall\, i,j \in J(I), k, t$$

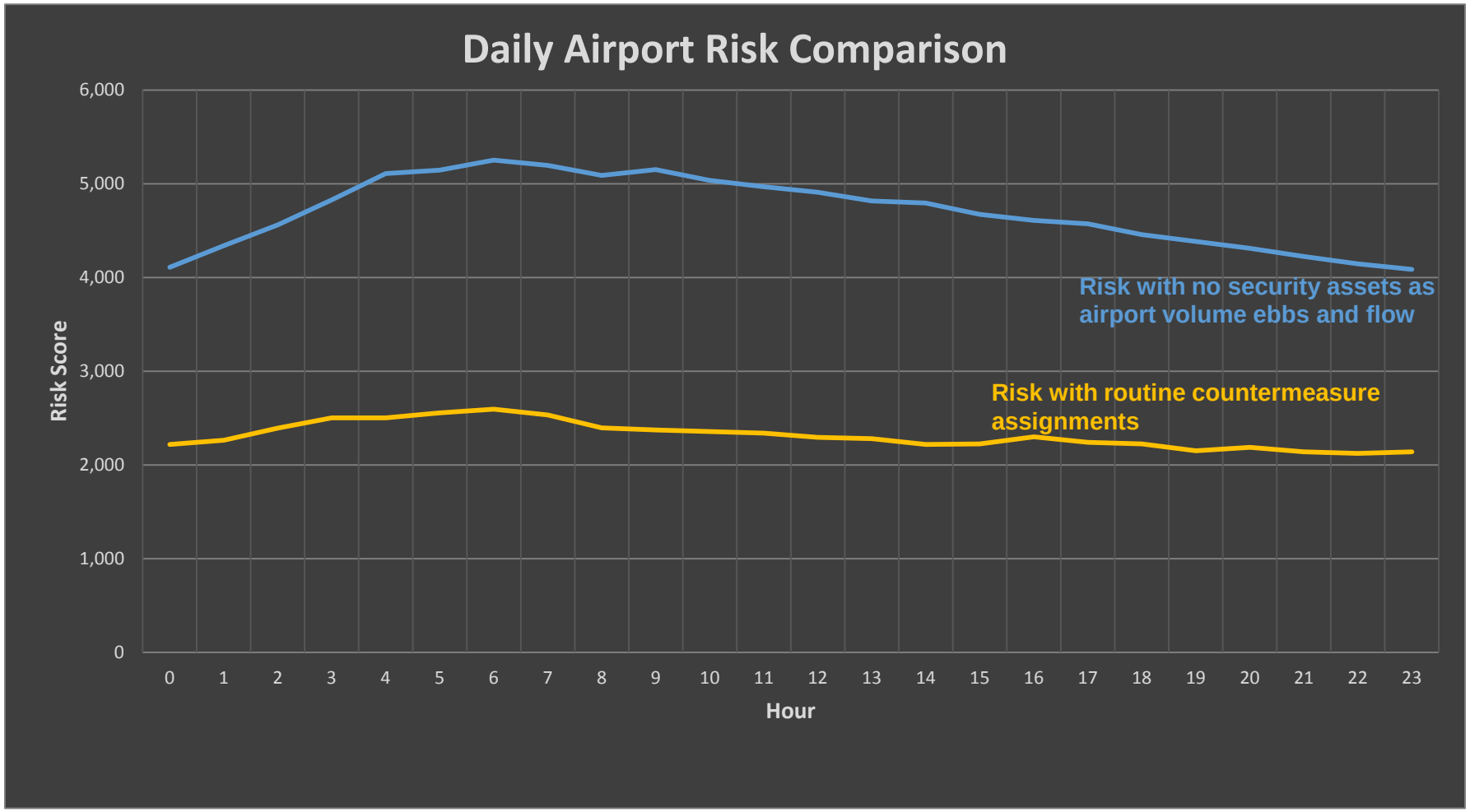
Notional Example – Risk Comparison

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965



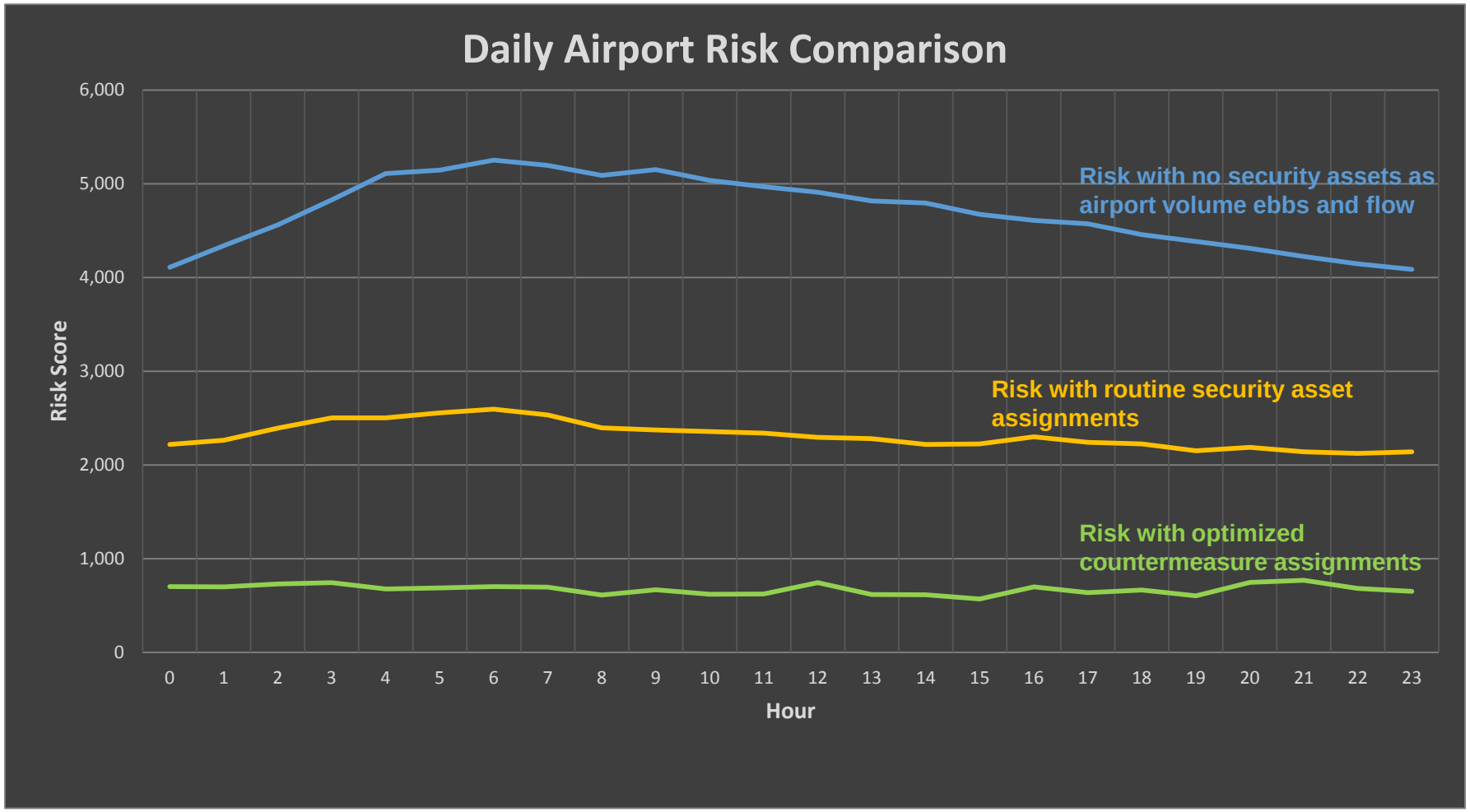
Notional Example – Risk Comparison

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965



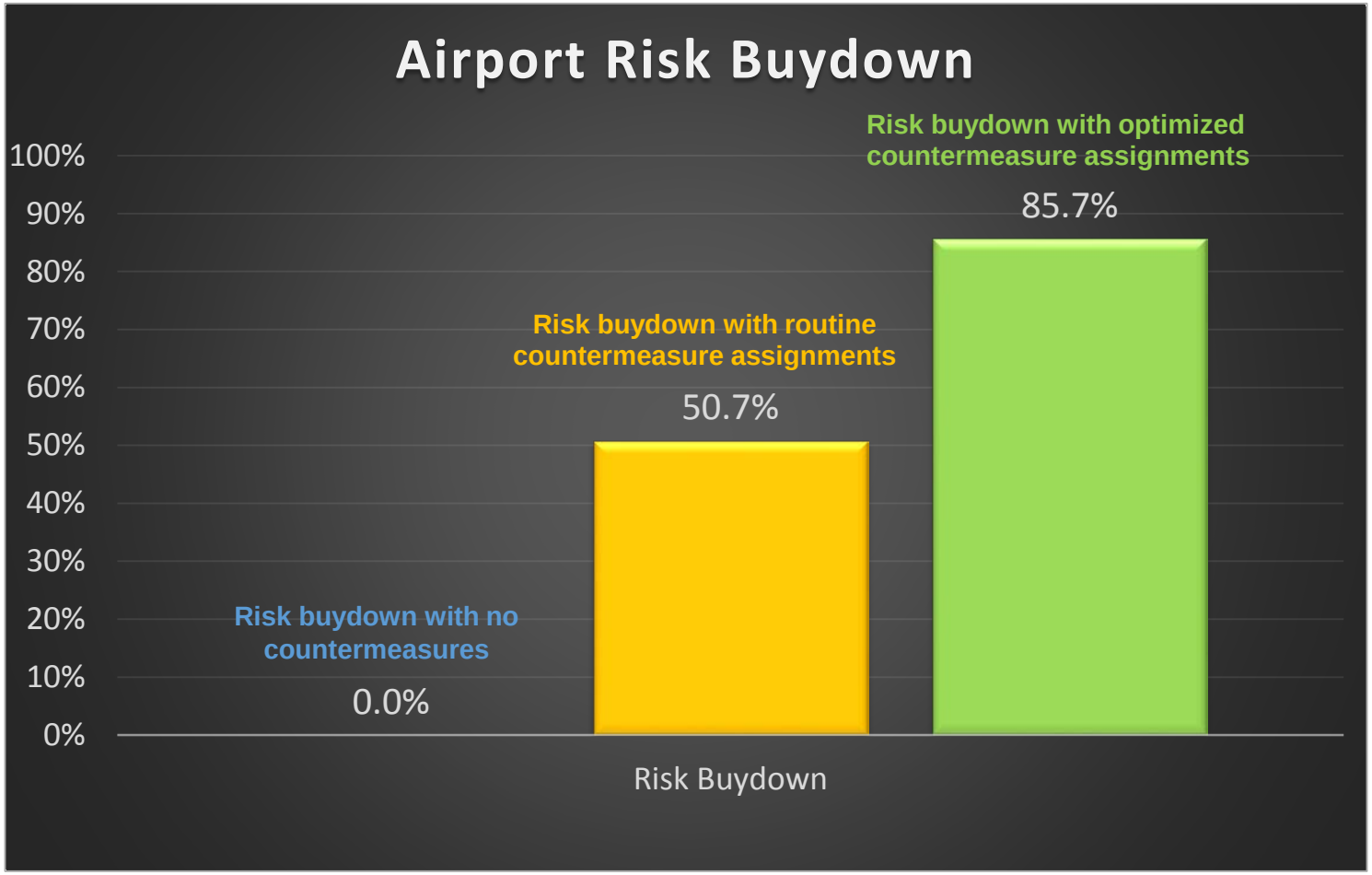
Notional Example – Risk Comparison

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965



Notional Example – Risk Buydown Comparison

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965



Summary and Benefits

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Methodology delivers an integrated, automated method to assess and minimize risk holistically across airport of interest
  - Cannot be done by hand or intuition
  - With 9 areas and only 6 different assets to assign in one hour, there are more than 500,000 combinations to choose from!
  - With more assets and the entire day to solve, the challenge becomes considerably more complex without MP
- Evaluates countermeasure effectiveness and deterrence
  - Can incorporate specific explosive threats and countermeasures
  - Resources match to threats they are most suited to defend against

Contact Information

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Sarah Reehl
Data Scientist
Pacific Northwest National Laboratory
sarah.reehl@pnnl.gov

Dr. Robert Brigantic
Chief Operations Research Scientist
Pacific Northwest National Laboratory
robert.brigantic@pnnl.gov
509-375-3675

Questions?

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965